Cryptography for Parallel RAM via Indistinguishability Obfuscation

Yu-Chi Chen∗ Sherman S. M. Chow† Kai-Min Chung‡ Russell W. F. Lai§ Wei-Kai Lin¶ Hong-Sheng Zhou∥

August 22, 2015

Abstract

Since many cryptographic schemes are about performing computation on data, it is important to consider a computation model which captures the prominent features of modern system architecture. Parallel random access machine (PRAM) is such an abstraction which not only models multiprocessor platforms, but also new frameworks supporting massive parallel computation such as MapReduce.

In this work, we explore the feasibility of designing cryptographic solutions for PRAM model of computation to achieve security while leveraging the power of parallelism and random data access. We demonstrate asymptotically optimal solutions for a wide-range of cryptographic tasks based on indistinguishability obfuscation. In particular, we construct the first publicly verifiable delegation scheme with privacy in the persistent database setting, which allows a client to privately delegate both computation and data to a server with optimal efficiency — in particular, the server can perform PRAM computation on private data with parallel efficiency preserved (up to poly-logarithmic overhead). Our results also cover succinct randomized encoding, functional encryptions, secure multiple party computations, and indistinguishability obfuscation for PRAM.

We obtain our results in a modular way through a notion of computational-trace indistinguishability obfuscation ($\text{CiO}$), which may be of independent interests.

∗ Academia Sinica, Taiwan, wycchen@iis.sinica.edu.tw
† Chinese University of Hong Kong, sherman@ie.cuhk.edu.hk
‡ Academia Sinica, Taiwan, kmchung@iis.sinica.edu.tw This work was done in part while the author was visiting the Simons Institute for the Theory of Computing, supported by the Simons Foundation and by the DIMACS/Simons Collaboration in Cryptography through NSF grant #CNS-1523467.
§ Chinese University of Hong Kong, wflai@ie.cuhk.edu.hk
¶ Academia Sinica, Taiwan, wklin@iis.sinica.edu.tw
∥ Virginia Commonwealth University, hszhou@vcu.edu
## Contents

1 Introduction .......................... 1
   1.1 The PRAM Model ............................................ 1
   1.2 Crypto for PRAM ........................................... 2
   1.3 Summary of Our Results ................................. 3
   1.4 Section Outline ........................................... 5

2 Overview of Our Constructions .......... 5

3 Highlight of Our Techniques ............ 7
   3.1 Handling Multiple Parallel Processors .................. 7
   3.2 Handling Random Memory Access .......................... 10

4 Detailed Technical Overview .......... 12
   4.1 Construction of $\text{CiO}$ ............................... 13
   4.2 From $\text{CiO}$ to Fully Succinct Randomized Encoding ($\mathcal{RE}$) .. 17

5 Computation-Trace Indistinguishable Obfuscation ($\text{CiO}$) .... 24
   5.1 Model of Distributed Computation Systems ............... 24
   5.2 Computation-trace Indistinguishability Obfuscation ....... 26

6 Starting Point: Constructing $\text{CiO}$ in the RAM Model ($\text{CiO}$-RAM) .. 26
   6.1 Building Blocks ............................................ 27
   6.2 Construction for $\text{CiO}$-RAM ............................ 27

7 Constructing $\text{CiO}$ in the PRAM Model ($\text{CiO}$-PRAM) .... 30
   7.1 Generalizing $\text{CiO}$-RAM for $\text{CiO}$-PRAM: A “Pebble Game” Illustration .... 30
   7.2 Building Blocks ............................................ 33
   7.3 Topological Iterators ...................................... 34
   7.4 Parallel Accumulator ...................................... 36
   7.5 Warm-up: Construction for $\text{CiO}$-PRAM∗ ................ 39
   7.6 $\text{CiO}$ for PRAM ........................................ 46

8 Constructing $\mathcal{RE}$ in the RAM Model ($\mathcal{RE}$-RAM) .... 50
   8.1 Building Blocks ............................................ 53
   8.2 Recap: The CP-ORAM ..................................... 54
   8.3 Construction for $\mathcal{RE}$-RAM ........................... 57

9 Constructing $\mathcal{RE}$ in the PRAM Model ($\mathcal{RE}$-PRAM) .... 59
   9.1 Recap: The BCP-OPRAM .................................. 61
   9.2 Construction for $\mathcal{RE}$-PRAM .......................... 62

10 Extensions ............................. 66
   10.1 $\text{CiO}$ with Persistent Database ......................... 66
   10.2 $\mathcal{RE}$ with Persistent Database ....................... 68
   10.3 $\mathcal{RE}$ with Output Hiding ............................. 70
   10.4 $\mathcal{RE}$ with Verifiability (Or Verifiable Encoding ($\mathcal{VE}$)) ...... 71
   10.5 $\mathcal{RE}$ and $\mathcal{VE}$ with Long Output .................. 73
   10.6 Application: Searchable Symmetric Encryption ($\mathcal{SSE}$) .......... 74
### Preliminaries

- **A.1** Models of Computation .................................................. 76
- **A.2** Randomized Encoding ($\mathcal{RE}$) .................................. 77
- **A.3** Building Blocks ............................................................... 78

### Security Proofs

- **B.1** Proof of Theorem 6.2 (Security for CiO-RAM) .................. 84
- **B.2** Proof of Lemma 7.3 (Security for Topological Iterators) ......... 113
- **B.3** Proof of Theorem 7.6 (Security for CiO-PRAM$^-$) ................. 116
- **B.4** Proof Sketch of Theorem 7.8 (Security for CiO-PRAM) ............ 128
- **B.5** Proof of Theorem 8.1 (Security for $\mathcal{RE}$-RAM) .............. 135
- **B.6** Proof Sketch of Theorem 9.1 (Security for $\mathcal{RE}$-PRAM) ....... 162
- **B.7** Proof of Theorem 10.4 (Security for $\mathcal{XE}$) ..................... 166
1 Introduction

1.1 The PRAM Model

The parallel random-access machine (PRAM) is an abstract computation or programming model of a canonical structured parallel machine. It consists of a polynomial number of synchronous processors. Each of them is similar to an individual (non-parallel) RAM with its central processing unit (CPU) performing computation locally. The difference is that CPUs in PRAM have random access of a common array of memory which is potentially unbounded, in additional to their local memory. Parallel and distributed computing community suggested many algorithms which are parallelizable in PRAM model, resulting in an exponential gap between solving the same problem in RAM and PRAM models. Examples include parallel sorting or parallel searching in a database, which have linear size input but run in polylogarithmic time.

Being an abstract model, PRAM not only models multiprocessor platforms, but also new frameworks in the big-data era such as MapReduce, GraphLab, Spark, etc. Running time is a critical factor here, especially when data is being generated in every seconds worldwide which are too big to be processed by traditional information processing technique or by a single commodity computer. For individuals, or even enterprises without in-house resource/expertise, there is an emerging demand for delegation of both data and computation to a third-party server, often called “the cloud”, a distributed computing platform with a large amount of CPUs to perform computations in parallel. We found PRAM a clean theoretical model to work with for these scenarios.

PRAM with Persistent Database. With the high volume of data uploaded to the cloud and correspondingly the potentially high volume of output data, it is natural to perform multiple computations over the “big data” in the cloud storage. Such functionality is supported by introducing the notion of persistent database on top of the PRAM model. A motivating example is a special kind of delegation formalized as searchable symmetric encryption (SSE) in the literature which features parallel search and update algorithms.

Secure and Efficient Delegation in the PRAM Model. Security concern manifests in various forms when we consider outsourcing. For a concrete discussion, we consider the delegation problem, faced by an enterprise which is outsourcing a newly-developed data analytic algorithm for uncovering market trends from the customer preferences collected. Data owners demand confidentiality. Secrecy of the algorithm is also desired, or competitors may gather the same kind of business intelligence (with their own data). The output of data analytics is also sensitive, both its confidentiality and authenticity (i.e. the correctness of the algorithm invocation) are crucial for the success of any corresponding strategy to be carried out. It is risky to place all these rather strong trust on the well-being of the cloud in different dimensions. Any client of the cloud needs to safeguard the outsourcing process by resorting to cryptography.

The next concern is about efficiency. On one hand, the client would want both storage and computation to be significantly less than the actual data and computation. On the other hand, the server, who is actually storing the data and performing the computation, would like to operate on the (private) data as a PRAM program, and not to perform too much work when compared to computation on the plaintext data. There exists verifiable delegation with privacy, but the solution is based on the circuit model, and is far from suitable for outsourcing big data. Recent work provides heuristic solution for RAM delegation with persistent database [GHRW14], but the solution is only a heuristic one based on a stronger variant of differing inputs obfuscation (dIO), which are subject to implausibility result.

More formally, we consider secure delegation of PRAM program with persistent database, as follows. A large database $x$ is firstly delegated from the client to the server. The client can make arbitrary number of PRAM program queries to the server, who performs the computation to update the database, and returns the answer with a proof. Ideally, we want the efficiency to match the “unsecured” solution. Namely, delegating database takes $O(|x|)$ cost, and for each PRAM program query, the client’s runtime depends only on the description size.
of the PRAM program, the server’s parallel runtime is linear in the parallel runtime of the program, and the client’s verification time does not depend on the complexity of the function and database size.

We pose ourselves this question: Can we outsource both data and computation, leveraging parallelism and random data access, i.e. in the PRAM model?

1.2 Crypto for PRAM

Many cryptographic schemes are about performing computation on data, which can be benefited by parallelism and persistent database. Traditionally, cryptographers worked on the circuit model of computations. For example, the celebrated result of Yao’s garbled circuit for two-party computation [Yao82]. Nowadays, we also have highly optimized solutions in the circuit model for many cryptographic tasks, including secure multiparty computation (SMC).

Secure Multiparty Computation (SMC). Oblivious PRAM [BCP14b] can be considered as a starting point of our work. A subsequent work in large-scale SMC [BCP14a] further motivates the benefits of PRAM. Consider SMC on electronic health record (EHR) for collaborative research, EHR often involves patients’ medical and genetic information which are often expensive to collect and should be kept confidential as mandated by law. Although circuit-based and RAM-based solutions of SMC exist, these solutions have inherent drawbacks: Circuit-based solutions are not feasible for big data since circuit representations are huge and the (worst case) runtime can be dependent on the input length. Consequently, it cannot represent sublinear time algorithm. Existing RAM-based solutions cannot exploit parallelism even when the program is parallelizable (which is often the case for processing big data), not to mention the large round complexity incurred by information-theoretic protocols. On the other hand, PRAM is an expressive model to capture the requirements in this case, yet a clean model to work with.

Functional Encryption (FE). Another primitive in cloud cryptography which attracts much attentions recently is functional encryption (FE), a generalized notion of attribute-based encryption (ABE), which was originally proposed for enforcing cryptographic access control. FE enables a user with the function key for \( f(\cdot) \) to learn \( f(x) \) given an encryption of \( x \). Consider \( x \) to be the encrypted cloud storage and each user can only access part of the shared storage space for obvious security reason. FE in PRAM means that the function key can be associated to a PRAM program taking the large \( x \) as an input. With PRAM program, the access control policy can be very general, and we can even embed some sort of parallel retrieval logic into it for returning the relevant part of the cloud storage expected by the cloud user. We remark that a very recent result achieved FE for Turing machines with unbounded input [AS15].

Our Goal. To summarize, current study of cryptography does not work in a model which fully leverages the important features of modern architecture to handle the computation problem nowadays, namely, massive parallel computation on big data. In this work, we address the following basic question:

“How to do Cryptography in the PRAM model — How to design cryptographic solutions that achieve security and simultaneously leverage the power of parallelism and random data access?”

Our work provides general feasibility and asymptotically optimal results for various important cryptographic primitives based on indistinguishability obfuscation.
1.3 Summary of Our Results

We develop techniques to obtain (asymptotically) optimal constructions for several cryptographic primitives in the PRAM model with persistent database. We do so in modular steps, and our results are presented below. Please also refer to Table 1 for the efficiency of our schemes.

**New notion:** Computation-trace Indistinguishability Obfuscation. First, we define a new primitive named computation-trace indistinguishability obfuscation (CiO), which obfuscates a computation instance instead of a program. A computation instance II is defined by a program P and an input x. Evaluation of II produces a computation trace, namely all CPU states, memory content, and memory access instructions throughout the computation. A CiO obfuscator takes in a computation instance II as an input, and outputs I as an obfuscated computation instance that can be evaluated to correctly output P(x). We only require a very weak indistinguishability-based security for CiO, where two obfuscations CiO(II) and CiO(II') are required to be indistinguishable only when the evaluation of II and II' produce identical computation trace (which implies the inputs need to be the same). While the security is weak, we demand stringent efficiency that the obfuscator’s runtime depends only on the instance description size, but not the evaluation runtime.

We construct CiO for RAM based on iO for circuits and one-way functions, by adopting techniques developed in a very recent result due to Koppula, Lewko, and Waters [KLW15] (hereinafter referred as KLW). We then (non-trivially, to be elaborated in the next section) extend it into CiO for PRAM. The main challenge here is to avoid linear overhead on the number of CPUs in both parallel runtime and obfuscation size — note that such overhead would obliterate the gain of parallelism for a PRAM computation. To summarize, we have:

**Theorem 1.1** (Informal). Assume that indistinguishability obfuscation (iO) and one-way functions (OWF) exist, there exists a (fully succinct) computation-trace indistinguishability obfuscation for PRAM computation.

While the notion of CiO is weak, we immediately obtain optimal publicly-verifiable delegation of PRAM computation. In particular, the program encoding has size independent of the output length.

**Corollary 1.2** (Informal). Under the assumptions of CiO and OWF, there exists a two-message publicly-verifiable delegation scheme for PRAM computation, where the delegator’s runtime depends only on the program description and input size, and the server’s complexity matches the PRAM complexity up to polynomial factor of program description size.

**Achieving privacy: fully succinct randomized encoding.** More importantly, we show how to use our (fully succinct) CiO for PRAM to construct the first fully succinct randomized encoding (RE) for PRAM computation. The notion of randomized encoding, proposed by Ishai and Kushilevitz [IK00], allows a “complex” function f on an input x to be represented by a “simpler to compute” randomized encoding $\hat{f}(x; r)$ whose output distribution encodes f(x), such that the encoding reveals nothing else regarding f and x, and one can decode by extracting f(x) from $\hat{f}(x; r)$. The circuit depth (i.e., parallel runtime) of the encoding is the original measure of simplicity [IK00]. Very recently, Bitansky, Garg, Lin, Pass, and Telang [BGL15] focus on encoding time. Bitansky et al. consider f as represented by a RAM program P, and construct (space-dependent) succinct randomized encodings where the encoding time is independent of the time complexity of P(x) (as a RAM program evaluation), but depends on the space complexity of P(x).\(^1\)

We extend the RE notion further to the PRAM model. More precisely, given a PRAM computation instance II defined by a PRAM program P and an input x, an RE for PRAM generates a randomized encoding $\hat{I} = \hat{R}E.$Encode(II) that can be decoded/evaluated to obtain P(x), but reveals nothing else regarding both P and x (except for the size/time/space bound of P(x)). Full succinctness means the encoder’s runtime (and thus the encoding size) depends on the description size of P, the input length of x, and the output length of P(x), but is

\(^1\)Canetti et al. [CHJV15] achieved a similar result in the context of garbling.
essentially independent of both time and space complexities of $P(x)$. To the best of our knowledge, there was no known fully succinct construction of $\mathcal{RE}$, even in the RAM model, before our result.

**Theorem 1.3** (Informal). Under the assumptions of iO and OWF, there exists fully succinct randomized encoding for PRAM, where the encoding time depends only on the program description and input/output size, and the server’s complexity matches the PRAM complexity of the computation up to polynomial factor of program description size.

By plugging our $\mathcal{RE}$ for PRAM into various transformations in the literature [GHRW14, BGL+15, CHJV15], we obtain the first constructions of a wide range of cryptographic primitives for PRAM (with the corresponding full succinctness), including non-interactive zero-knowledge, functional encryption, garbling, secure multi-party computation, and indistinguishability obfuscation for PRAM, and we have the following two corollaries.

**Corollary 1.4** (Informal). Under the assumptions of iO and OWF, there exist (fully) succinct non-interactive zero-knowledge, functional encryptions with succinct (PRAM) function keys, succinct reusable garbling, and secure multi-party computation for PRAM with optimal communication.

Notably, while CiO is syntactically weaker than iO, sub-exponential CiO for PRAM still implies iO for PRAM with sub-exponential security by complexity leverage argument (e.g., [BGL+15, CHJV15]).

**Corollary 1.5** (Informal). Sub-exponentially secure CiO for PRAM implies sub-exponentially secure iO for PRAM.

**Optimal outsourcing with persistent database.** Finally, we generalize to the persistent database setting where a computation consists of a database and multiple programs. The generalization is straightforward, and leads to optimal delegation with persistent database; see the theorem statement below. We remark that this immediately gives us the feasibility of optimal symmetric searchable encryption without leakage.

**Theorem 1.6** (Informal). Under the assumptions of iO and OWF, there exist fully succinct outsourcing schemes for PRAM with persistent database, where the encoding time depends on the database size and the size of each program description, and the server’s complexity matches the PRAM complexity of the computation up to polynomial factor of program description size.

**Independent and Concurrent Work.** Canetti and Holmgren [CH15] also proposed a fully succinct garbling scheme for RAM programs, based on the same assumption of the existence of iO and OWF. We note that, however, the motivation of both works are different. Specifically, we aim for developing cryptographic solutions for PRAM model of computation to capture the power of both parallelism and random data access. Achieving full succinctness in the PRAM model is a major technical novelty of our result.
On the technical level, we note that both our construction and theirs can be viewed as a natural generalization and modularization of the construction of Koppula, Lewko, and Waters (KLW) for succinct encoding for Turing machines. Both works first construct a succinct encoding that satisfies a weak indistinguishability-based security (in our case, the notion of \( \text{CiO} \)). With this encoding, both rely on encryption and ORAM to hide the content and access pattern of the RAM computation. At the core of both security proofs are approaches to “puncture” ORAM execution to switch the access pattern step by step. From here, Canetti and Holmgren [CH15] additionally introduce a novel dual-encryption mechanism with a security property of tree-based ORAM constructions, which make their security analysis more modular, at the cost of slightly increase the security loss in the hybrid. Their techniques can be generalized to provide a more modular proof of \( \mathcal{RE} \) for PRAM from CiO for PRAM.\(^2\)

1.4 Section Outline

In Section 2 and 3, we give a very high level overview of the paper. Experienced readers can jump directly to Section 4 for a more detailed overview. For a more compact presentation, we move the preliminaries to Appendix A.

The formal description of our results starts from Section 5, where we define the new notion of Computation-Trace Indistinguishability Obfuscation (CiO). The constructions of CiO in the RAM and PRAM model are described in Section 6 and 7 respectively. Next, in Section 8 and 9, we extend CiO to randomized encoding (\( \mathcal{RE} \)) in the RAM and PRAM model respectively. Various extensions of \( \mathcal{RE} \) for different delegation scenarios can be found in Section 10.

Finally, all security proofs are consolidated in Appendix B.

2 Overview of Our Constructions

This section is devoted to give a high level overview of our constructions. Koppula, Lewko, and Waters [KWL15] (KLW) constructed succinct primitives (message-hiding encodings and machine-hiding encodings) for Turing machines. At a high level, our constructions are natural generalizations of their constructions to handle PRAM with persistent database, where the major challenge is to develop new techniques to handle parallel processors and random access pattern. On a conceptual level, our constructions are modular and simple. Therefore, we focus on illustrating our constructions here first, and discuss our techniques for proving security in the next section. We start by describing the way we view (parallel) RAM model of computation.

(Parallel) RAM Model of Computation. In the RAM model, computation is done by the CPU with random access to the memory in time steps (CPU cycles). At each time step, the CPU receives the read memory content, performs one step of computation to update its CPU state, and outputs a memory access (read or write) instruction. The computation terminates when the CPU reaches a special halting state. The PRAM model is similar to the RAM model, except that there are multiple CPUs executing in parallel with random access to a shared memory (and reaching the halting state at the same time). For simplicity, here we assume that there is no conflict writes throughout the computation, though our construction can handle the general CRCW (concurrent read concurrent write) model.

We envision that the input \( x \) to a (parallel) RAM computation instance \( \Pi \) is initially stored in the memory, and the program \( P \) is encoded as a CPU next-step function with \( \text{polylog}(n) \)-sized initial CPU state. More precisely, \( P \) on input a time step \( t \), a CPU state, and a read memory content, outputs an updated CPU state and memory access instruction for time step \( t+1 \). For PRAM, we assume that the CPUs share the same CPU program \( P \), but have distinct CPU id. In this overview, we assume that the output \( y \) is short, and at the end of the computation, \( y \) is stored in the (first) CPU state (together with the special halting symbol).

\(^2\)We could include the modular proof. Yet, we decided it would be best for the readers to keep the two works separate.
Construction overview. Let us motivate our construction through the context of delegation, where a client delegates computation of a PRAM instance $\Pi = (P, x)$ to a server. Without security consideration, the client can simply send $\Pi$ in the clear to the server, who can evaluate the PRAM program and return $y = P(x)$. Our goal is to achieve publicly verifiable delegation with privacy (and asymptotically) the same client and server efficiency. Specifically, the server learns nothing except for the output $y$, whose correctness can be verified publicly.\(^3\)

At a high level, we let the client to send some obfuscated program $\tilde{P}$ and encoded input $\tilde{x}$ to the server with the hope that the obfuscation and encoding hide $P$ and $x$, yet allowing the server to perform PRAM evaluation on $\tilde{P}(\tilde{x})$ (since obfuscation preserves input/output behavior and thus allows PRAM evaluation). Note that in order to protect the privacy of $P$, we must restrict $\tilde{P}$ to evaluate only on input $x$, since $P(x')$ may leak additional information about $P$ beyond $y = P(x)$. This means that we need to have some authentication mechanism to authenticate the whole evaluation of $P$ on $x$ but nothing else. Additionally, the evaluation of $P$ on $x$ produces a long computation trace in addition to $y$. We need some hiding mechanism to hide the evaluation process. We discuss these two major ingredients in turn.

First step: authentication mechanism. The goal is to allow $\tilde{P}$ to evaluate only on $x$ but nothing else. Recall that computation involves updating CPU states and memory, where the later may be large in size. We can authenticate CPU states by signatures and memory by Merkle tree like data structure. More precisely, we obfuscate a compiled program $P_{\text{auth}}$, where at each time step, the obfuscated $\tilde{P}_{\text{auth}}$ expects to receive a signed CPU state from the previous time step, and sign the output state for the next time step.\(^4\) To authenticate the memory, a Merkle tree root is stored in the CPU state, and each memory read/write is authenticated via authentication path (i.e., the path from the root to the memory location with siblings in the Merkle tree). In other words, the server (evaluator) needs to feed $\tilde{P}_{\text{auth}}$ signed CPU states and the authentication path for the read memory content in order to evaluate $\tilde{P}_{\text{auth}}$ (otherwise, $\tilde{P}_{\text{auth}}$ outputs $\bot$). In this way, the input $x$ can simply be authenticated by signing the initial CPU state with Merkle tree root of $x$ stored inside. Indeed, intuitively (i.e., assuming security of all used primitives “works”), the server can evaluate $\tilde{P}_{\text{auth}}$ only on $x$.

We note that the above is the intuition behind the construction of message-hiding encoding of KKW [KLW15], where they use iO combined with several novel iO-friendly authentication primitives they developed to prove security. We show that their techniques can directly be used to construct GiO for RAM, and further develop new techniques to construct GiO for PRAM. We refer the readers to the next section for further details.

We also note that authentication alone already implies publicly verifiable delegation without privacy, by using a special signing key to sign the output $y$ and publishing the corresponding verification key for public verification.\(^5\)

Second step: hiding mechanism. The next goal is to hide information through the evaluation process of $\tilde{P}$ on $\tilde{x}$. A natural approach is to use encryption schemes to hide the CPU states and memory content. Namely, $\tilde{P}$ always outputs encrypted CPU states and memory, and on (authenticated) input of ciphertexts, performs decryption first before the actual computation.\(^6\) Note, however, that the memory access pattern cannot be encrypted (otherwise the server cannot evaluate), which may also leak information. A natural approach is to use oblivious (parallel) RAM (OPRAM) to hide the access pattern. Namely, we use OPRAM compiler to compile the program (and add an “encryption layer”) before obfuscating it. Again, intuitively (i.e., assuming all primitives “works”), the server cannot learn information from the evaluation process.

\(^3\)We consider other settings as well, but focus on this particular setting here.

\(^4\)While we focus on construction here, we mention that proving security is highly non-trivial since signing key is hard-wired in $\tilde{P}_{\text{auth}}$ (so unforgeability may not hold).

\(^5\)In the technical section, we do it in a modular way through GiO.

\(^6\)As above, proving security is tricky since secret key is hard-wired in.
We note that the construction of machine-hiding encoding for Turing machine [KLW15] uses public-key encryption to hide the content of TM evaluation, and hides the TM access pattern by oblivious Turning machine compiler [PF79], which is deterministic. In our case, hiding random memory access pattern for (parallel) RAM (which is necessary to capture sublinear time computation) requires new techniques, since OPRAM/OPRAM compilers are randomized, and we cannot use OPRAM/OPRAM security in a black-box way. We deal with this issue by developing “puncturing” technique for specific OPRAM construction. Our construction is also more modular than KLW [KLW15], and uses the notion of CiO in a black-box way (which in a sense captures security achieved by authentication). We refer the readers to the next section for further details.

**Extension to delegation with persistent database.** Finally, we note that our construction can be generalized readily to handle delegation with persistent database. Recall that in this setting, the client additionally delegates his database to the server at beginning, and then delegates multiple computation to evaluate and update the database in a verifiable and private way. Recall that we authenticate every step of computation by signatures. We can “connect” two programs by letting $P_i$ to sign its halting state using a spacial “termination” signing key, and letting the next program $P_{i+1}$, upon receiving a state signed by this termination key, initiate itself by signing its initial state, and inherit the Merkle tree root of the database from $P_i$ (stored in the halting CPU state).

### 3 Highlight of Our Techniques

As mentioned, our constructions are natural generalizations of the constructions of succinct primitives for Turing machines of Koppula, Lewko, and Waters (KLW) [KLW15] to handle PRAM with persistent database. In this regard, we largely inherit and build upon their novel techniques. On the other hand, we develop new techniques to handle multiple parallel processors, and random memory access in the PRAM model of computation. In this section, we highlight the technical difficulties and our techniques to resolve them.

#### 3.1 Handling Multiple Parallel Processors

Recall that our construction takes two modular steps, where we first introduce authentication mechanism to achieve a weak CiO security, and then add hiding mechanism to achieve privacy. We also mentioned that the authentication mechanism of KLW for Turing machine directly generalizes to yield CiO for RAM. However, two issues arise when we want to generalize it to handle PRAM. Let us consider a PRAM instance $\Pi = (P, x)$ with $m$ CPUs.

- **Algorithmic issue.** First note that we do not want constructions with efficiency overhead linear in $m$, since this defeat the gain of parallelism. Thus, we cannot view $m$ parallel CPUs as a single giant program taking $m$ copies of inputs (otherwise, obfuscation causes $\text{poly}(m)$ factor overhead), but need to run $m$ (obfuscated) CPU programs in parallel, each of which has small $\text{poly log}(n)$-sized state. However, recall that the (large) memory is authenticated by a Merkle tree like data structure with the root as a digest stored and updated in the CPU states. When there is a parallel write to the memory, these $m$ CPUs need to update the digest in parallel efficiently. Note that no CPU can have global update information (since each only has $\text{poly log}(n)$-sized state), so they need to do it in a distributed fashion without incurring $\Omega(m)$ efficiency overhead. We handle this issue based on the techniques in the OPRAM construction of Boyle, Chung, and Pass [BCP14b]. At a high level, we allow the CPUs to communicate with each other, and design a $O(\text{poly log } m)$-round distributed algorithm for updating the digest with oblivious communication pattern (which is important for security).\(^7\)

\(^7\)We remark that in the context of OPRAM, the CPU to CPU communication can be done through memory access (e.g., CPU $i$ writes to a specific memory address and CPU $j$ reads it). However, in our context, we cannot do so, since communication through memory again requires to update the digest, which leads to a circularity issue.
\begin{itemize}
  \item \textbf{Security proof issue.} This is a more subtle and challenging issue arises when we try to generalize the security proof for TM/RAM model to handle PRAM. At a very high level, the security proof consists of a (long) sequence of hybrids in time steps, where in the intermediate hybrids, we need to hard-wire the CPU state at some time steps to the obfuscated program. Generalizing the idea to PRAM in a naive way would require us to hard-wire the \( m \) CPU states at some time steps, which results in \( \Omega(m) \) amount of hard-wired information. This in turn requires us to pad the program to size \( \Omega(m) \) and causes \( \text{poly}(m) \) overhead in size of the obfuscated program. To see why this is the case, and pave the way for discussing our idea for resolving the issue, we must take a closer look at the technique of KLW.

\textbf{Proof Techniques of KLW.} We now provide a very high level overview of the security proof of our CiO for RAM based on the machinery of KLW. The techniques serve as a basis for the discussion of our construction of CiO for PRAM. Recall that our construction can be viewed as \( \text{CiO}(\Pi) = (i\mathcal{O}(P_{\mathit{auth}}), x_{\mathit{auth}}) \), where \( (P_{\mathit{auth}}, x_{\mathit{auth}}) \) is just \((P, x)\) augmented with \( i\mathcal{O}\)-friendly authentication mechanism of KLW. Let \( \Pi = (P, x) \) and \( \Pi' = (P', x) \) be two computation instances with identical computation trace.\(^8\) Our goal is to show \( \Pi \leftarrow \text{CiO}(\Pi) \) and \( \Pi' \leftarrow \text{CiO}(\Pi') \) are computationally indistinguishable. To prove security, we consider a sequence of hybrids starting from \( \bar{\Pi} \) that switches the program from \( P \) to \( P' \) time step by time step. However, to switch based on \( i\mathcal{O} \) security, the programs in the hybrids need to be functionally equivalent, while \( P \) to \( P' \) only behave identically during honest execution. Here is the place that the powerful \( i\mathcal{O}\)-friendly authentication primitives of KLW help. At a very high level, they allow us to switch to a hybrid program that, at a particular time step \( t \) (i.e., input with time step \( t \) stored in the CPU state), only accepts the honest input but rejects (and outputs \text{Reject}) all other inputs. This enables us to switch from \( P \) to \( P' \) at time step \( t \) using \( i\mathcal{O} \) security. More precisely, it can be viewed as introducing \textit{“check-points”} to hybrid programs as follows:\(^9\)

  \begin{itemize}
    \item We can place a check-point at the initial step of computation, and move it from a time step \( t \) to time step \((t + 1)\) through hybrids.
    \item Check-point is a piece of code that at a time step \( t \), checks if the input (or output) is the same as that in the honest computation, and forces the program to output \text{Reject} if it is different. This is an information-theoretic guarantee which enables us to switch the program at time step \( t \) based on \( i\mathcal{O} \) security.
  \end{itemize}

We can then move the check-point from the beginning to the end of the computation, and along the way switch the program from \( P \) to \( P' \). We note that this check-point technique is implicit in the security proof for message-hiding encodings [KLW15]. Our description can be viewed as an abstraction of their proof techniques.

\textbf{A “Pebble Game” illustration.} We now discuss the issue of hard-wiring \( \Omega(m) \) amount of information in intermediate hybrids when we generalize the KLW techniques to handle PRAM with \( m \) CPUs. To illustrate why, we can cast the security proof as a \textit{“pebble game”} over a graph defined by the computation, and the amount of required hardwire information in the hybrids can be captured by the \textit{“pebble complexity”} of the game. We first illustrate this pebble game abstraction for the case of RAM computation. Recall that the security proof relies on a check-point technique that allows us to place a check-point on the initial time step, and move it from a time step \( t \) to its next time step \((t + 1)\). Placing a check-point at a time step requires to hardwire information proportional to the input (or output) size of the CPU program. The goal is to travel all time steps (to switch the programs on all time steps). In this example, the RAM computation can be viewed as a line graph with each time step being a node in the graph. A check-point is a pebble that can be placed on the first node, and can be moved from node \( t \) to node \((t + 1)\). The wining condition of the pebble game is to \textit{“cover”} the graph, namely, to ever place a pebble on each node. The pebble complexity is the maximum number of pebbles needed in order

\(^8\)Recall that it means the content of both CPU states and memory are identical throughout the computation.

\(^9\)We note that the description here over-simplifies many details.
\end{itemize}
to cover the graph, which is 2 for the case of RAM (since technically we need to place a pebble at \((t + 1)\) before removing the pebble at \(t\)).

To capture the hybrids for proving our CiO for PRAM, we formulate the following pebble game:

- The graph is a layered (directed acyclic) graph with each layer corresponds to \(m\) CPUs’ at a certain time step. Namely, each node is indexed by \((t, i)\) where \(t\) is the time step and \(i\) is the CPU id. It also consists of a 0 node corresponding to the seed state. The 0 node has an outgoing edge to \((t = 1, i)\) node for every \(i \in [m]\). Each node \((t, i)\) has an outgoing edge to \((t + 1, i)\) indicating the (trivial) dependency of \(i\)-th CPU between time step \(t\) and \(t + 1\). Recall that the CPUs have communication (to jointly update the digest of the memory). If CPU \(i\) sends a message to CPU \(j\) at time step \(t\), we also put an outgoing edge from \((t, i)\) to \((t + 1, j)\) to indicate the dependency.\(^{10}\)

- The pebbling rule is defined as follows: First, we can place a pebble on the 0 node. To place a pebble on a node \(v\), all nodes of \(v\)'s incoming edges need to have a pebble on it. To remove a pebble on a node \(v\), we need to “cover” all \(v\)'s outgoing nodes, i.e., ever place a pebble on each outgoing node. This captures the conditions about when can we put a check-point to a computation step, and when can we remove it, for our generalization of the iO-friendly authentication techniques of KLW to the parallel setting.

- The goal is to cover the whole graph (i.e., ever places a pebble in every node) using a minimal number of pebbles. The pebble complexity of the game is the maximum number of pebbles we need to simultaneously use to cover the graph. Covering the graph corresponds to switching the programs for every computation step, and the pebble complexity captures the amount of hardwire information required in the intermediate hybrids.

Recall that our \(P_{auth}\) invokes a distributed protocol to update digest of the memory for every (synchronized) memory-writes. It is unfortunately unclear how to play the pebble game induced by multiple invocations of this distributed protocol with \(o(m)\) pebble complexity, and it seems likely that the pebble complexity is indeed \(\Omega(m)\). Therefore, it may seem that in the security proof hardwiring \(\Omega(m)\) amount of information in intermediate hybrids is required.

\(^{10}\)The memory accesses in general may create dependency, but we ignore it here as the pebble complexity is already high.

**A “Branch-and-Combine” Technique to Reduce Information Hardwiring.** We solve the problem by introducing a branch-and-combine approach to emulate a PRAM computation (illustrated in Figure 1), which transforms the computation graph to one that has poly \(\log(m)\) pebble complexity, and preserves the parallel run-time and obfuscation size with only a poly \(\log(m)\) overhead.

At a high level, after one parallel computation step, we combine \(m\) CPU states into one “digest” state, then we branch out from the digest state one parallel computation step, which results in \(m\) CPU states to be combined again. The PRAM computation is emulated by alternating the branch and combine steps. The combine step involves \(\log m\) rounds where we combine two states into one in parallel (which forms a complete binary tree). The branch step is done in one shot which branches out \(m\) CPUs in one step in parallel. Thus, the branch-and-combine emulation only incurs \(O(\log m)\) overhead in parallel run-time. Note that this transforms the computation graph into a sequence of complete binary trees where each time step of the original PRAM computation corresponds to a tree, and the root of a time step connects to all leaf nodes of the next time step.

Now, we observe that we can use only \(O(\log m)\) pebbles to traverse the computation graph of the branch-and-combine PRAM emulation. At a high level, this is because whenever we put two pebbles at a pair of sibling nodes in the complete binary tree of the combine step, we can merge them into a single one at their parent node. This means that we only need to use one pebble for each height level of the tree. More precisely, we can move pebbles from one root to the next one by simply putting pebbles at its branched out nodes one by one in order, and merge the pebbles greedily whenever it is possible.
We refer the readers to Section 7 for the construction of the branch and combine steps. Very roughly (and in an oversimplified manner), the combine step corresponds to constructing an accumulator tree for CPU states, and the branch step verifies an input CPU state using the accumulator and performs one computation step.

### 3.2 Handling Random Memory Access

Recall that our construction to achieve privacy is very natural: We hide CPU states and memory content using public-key encryption (PKE) and use oblivious (parallel) RAM to hide access pattern. Also recall that KLW already showed how to use PKE to hide the content of Turing machine evaluation. Roughly speaking, the security proof is done by a sequence of hybrid that “erases” the computation step by step *backward* in time. Finally, recall that hiding access pattern for Turning machine is simple since oblivious Turning machine compiler [PF79] is deterministic.

In contrast, ORAM and OPRAM compilers are randomized, and they only hide the access pattern statistically when the adversary learns only the access pattern, but not the content of CPU states and memory. However, since the obfuscated program has the secret key of PKE hard-wired in, we can only argue that the content is hidden by puncturing argument with the cost of hard-wiring information. In other words, we can only afford to argue hiding holds “locally” but not “globally”. This is the reason that the work of KLW requires a sequence of hybrids to erase the computation step by step. More importantly, this prevents us from using ORAM/OPRAM security in a black-box way.

We remark that the seminal work of Canetti et al. [CHJV15] encountered this technical problem in the context of one-time RAM garbling scheme, where they resolve the issue by identifying stronger security of a specific ORAM construction [CP13]. However, this approach requires to “erase” the computation *forward* in time in the security hybrids, which in turn requires to hard-wire information proportional to the space complexity of the RAM computation. We instead resolve this question by a puncturing ORAM/OPRAM technique that also relies on specific ORAM/OPRAM constructions [CP13, BCP14b]. We elaborate the idea below for the case of RAM computation.

#### A Puncturing ORAM Technique for Simulation.

We develop a puncturing ORAM technique to reason about the simulation for a specific ORAM construction [CP13] (referred to as CP ORAM hereafter). Our high level strategy is to switch the ORAM access pattern from a real one to a simulated one step by step (backward in time). To enable switching at time step $i$ (i.e., for the $i$-th memory access), we “puncture” the real execution in a way that ensures that the $i$-th memory access is information theoretically hidden even given the content of the first $i-1$ steps execution. Since we do hybrids backward in time, the computation after $i$-th step is already erased, and so once the ORAM is “punctured”, we can replace the real $i$-th step access pattern by a simulated one (both of which are random given full information of the punctured real ORAM execution). To further explain how this is done, we first review the CP ORAM Construction.

#### Review of the CP ORAM Construction.

In a tree-based ORAM such as the CP ORAM, the memory is stored in a complete binary tree (called ORAM tree), where each node is associated with a bucket. A bucket is a vector with $K$ elements, where each element is either a memory block, or an unique symbol dummy stands for an empty slot. A position map $pos$ records where each memory block is stored in the tree, i.e., a node somewhere along a path from the root to the leaf indexed by $pos[i]$. Each memory block $\ell$ in the ORAM tree also stores its index $\ell$ and position map value $pos[\ell]$ as meta data. Each memory access to block $\ell$ is performed by OACCESS, which (i) reads the position map value $p = pos[\ell]$ and refreshes $pos[\ell]$ to a random value, (ii) fetches and removes the block $\ell$ (i.e., replace it by dummy) from the path, (iii) updates the block content and puts it back to...

---

11We believe that our puncturing technique works for any tree-based ORAM, but we work with CP ORAM for concreteness.

12A memory block is the smallest unit of operation in CP ORAM, which consists of a fixed small number of memory cells.
the root (i.e., replace a dummy block by the updated memory block), and (iv) performs a flush operation along another random path $p'$ to move the blocks down along $p'$ (subject to the condition that each block is stored in the path specified by their position map value). At a high level, the security follows by the fact that the position map values are uniformly random and hidden from the adversary, and thus the access pattern of each OACCESS is simply two uniformly random paths, which is trivial to simulate.

The position map is large in the above construction, and is recursively outsourced to lower level ORAM structures to reduce its size. For illustration, we consider non-recursive version of the CP ORAM, where the large position map is stored in the CPU state. We handle the full-fledged recursive version in the technical section.

**Key Observation for “Puncturing” CP ORAM.** Consider the execution of an CP ORAM\(^\text{13}\) compiled program which accesses memory block $\ell$ in the $i$-th time step (corresponds to the $i$-th OACCESS call), the access pattern at this time step is determined by the position map value $p = pos[\ell]$ at the time.\(^\text{14}\) So, as long as this value $p$ is information-theoretically hidden from the adversary, we can simulate the access pattern by a random path even if everything else is leaked to the adversary. On the other hand, the value is generated at the last access time $t'$ of this block, which can be much smaller than $i$, stored in both the position map and the block $\ell$ (as part of the meta data), and can be touched multiple times from time step $t'$ to $i$. Thus, the value can appear many times in the computation trace of the evaluation. Nevertheless, by a sequence of carefully defined hybrids (which we refer to as partially punctured hybrids), we can erase the information of $p$ step by step without hardwiring too much information, which allows us to carry through the puncturing ORAM argument. We refer the reader to Section 4 for further details.

![Figure 1: Illustrating an evaluation of “branch and combine” program: each node is a step computation of either $F_{\text{branch}}$ or $F_{\text{combine}}$ with its CPU id denoted in a binary string, each arrow denotes dispatching an output to the input of another node; dummy computations are omitted, and dispatching is performed in the evaluator.](image)

\(^\text{13}\)Ideally, it is desirable to formalize a “puncturable” property for ORAM or the CP ORAM construction, and use the property in the security proof. Unfortunately, we do not know how to formalize such a property without referring to our actual construction, since it is difficult to quantify what an adversary can learn from the GiO obfuscation. Yet, in an independent work [CH15] which also construct succinct randomized encoding for RAM (but not for PRAM), a more modular and cleaner technique is developed to prove security.

\(^\text{14}\)We ignore the uniformly random path used in the flush operation here, which is trivial to simulate.
4 Detailed Technical Overview

This section provides a detailed technical overview of our constructions of CiO and randomized encodings for PRAM computation. The presentation here aims to provide more comprehensive and technical overview, and thereby repeats some key points mentioned in Section 2 and 3.

Before getting into details, we present a high level outline and highlight our techniques.

(Parallel) RAM Model of Computation. In the RAM model, computation is done by the CPU with random access to the memory in time steps (CPU cycles). At each time step, the CPU receives the read memory content, performs one step of computation to update its CPU state, and outputs a memory access (read or write) instruction. The computation terminates when the CPU reaches a special halting state. A RAM computation instance $\Pi$ is defined by a CPU next-step program $P$, and an input $x$ stored in the memory as initial memory content (and a default initial CPU state). At the end of the computation, the output $y$ is stored in the CPU state (together with the special halting symbol). The CPU program $P$ is represented as a next-step circuit that takes previous CPU state and read memory content, and outputs next CPU state and memory access instruction.

The PRAM model is similar to the RAM model, except that there are multiple CPUs executing in parallel with random access to a shared memory. The CPUs share the same CPU program $P$, but have distinct CPU id.

CiO for RAM. Our starting point is a construction of CiO for RAM computation based on iO for circuits and the novel iO-friendly authentication techniques of Koppula, Lewko, and Waters (KLW) [KLW15], for their construction of message-hiding encodings (MHE). While the primitives are different, our CiO construction is closely related to their construction, and CiO can be used to construct MHE readily. In fact, our CiO notion is heavily inspired by their work, and can be viewed as an abstraction of what is achieved by their techniques.

CiO for PRAM. We then extend the above approach to handle PRAM computation with some care of efficiency issues in the parallel setting. Yet, a natural generalization does not yield a fully succinct construction. This is because the hybrids in the (generalized) security proof needs to hardwire $\Omega(m)$ amount of information in the iO-ed program, where $m$ is the number of CPUs in the PRAM program, and thus the obfuscated computation instance has size dependent on $m$. We address this issue by developing a “branch-and-combine” technique to emulate PRAM computation, which enables us to reduce the amount of hardwired information in the hybrids to $O(\log m)$. See Section 4.1.2 for a more detailed discussion.

From CiO for RAM to RE for RAM — the case without hiding access pattern. We then discuss how to construct fully succinct randomized encoding from CiO for RAM computation. At a high level, this requires to hide both the content and the access pattern of the computation. We first consider the simpler case where the computation has oblivious access pattern (so we only need to hide the content), which we can again rely on techniques from [KLW15] to hide the content using public-key encryption. In fact, if the access pattern is not required to be hidden, the construction of machine-hiding encoding for TM [KLW15] can be modified in a straightforward way to yield RE for RAM (based on iO for circuits). Our construction can be viewed as a modularization and simplification of their construction through our CiO notion.

From CiO for RAM to RE for RAM — the full-fledged case. We next discuss how to hide access pattern, which is the major challenge for the construction of fully succinct RE for RAM. We follow a natural approach to use oblivious RAM (ORAM) compiler to hide it. However, the main difficulty is that ORAM only hides the access pattern when the CPU state and memory contents are hidden from the adversary, which is hard to argue
for unless the obfuscation is virtual-black-box (VBB) secure \([\text{BGI}+01]\), while \(\text{CiO}\) (just like \(i\text{O}\)) does not hide anything explicitly.

We develop a puncturable ORAM technique to tackle this issue. We rely on a simple ORAM construction \([\text{CP13}]\) (referred to as CP ORAM) and show that it can be “punctured” at time step \(i\) so that the access pattern at the \(i\)-th time step of \(P(x)\) can be simulated even given the punctured program. Armed with this technique, we can simulate the access pattern at time step \(i\) by puncturing the ORAM compiled program at step \(i\) (through hybrids), replacing the access pattern at this step, and then unpuncturing the program. However, the computation traces of a punctured program can differ from the original ones in many steps. Therefore, arguing the indistinguishability of a hybrid using a punctured program is non-trivial. We do so by defining a sequence of “partially punctured” hybrids that gradually modifies the program step by step. See Section 4.2.2 for a more detailed discussion.

**From \(\text{CiO for PRAM to \(\mathcal{RE}\) for PRAM.}** Finally, we extend the above construction to handle PRAM computation, where we simply replace the CP ORAM compiler by the oblivious PRAM compiler of Boyle et al. \([\text{BCP14b}]\). The security proof also generalizes in a natural way, except that we need to take care of some issues aroused in the parallel setting. The main issue here is to generalize the puncturing argument to puncture ORAM in a way that avoids dependency on the number of CPU \(m\) to maintain full succinctness. This can be done by puncturing the ORAM CPU by CPU. See Section 4.2.3 for a more detailed discussion.

### 4.1 Construction of \(\text{CiO}\)

Our construction of \(\text{CiO}\) for (parallel) RAM computation is based on \(i\text{O}\) for circuits and the novel \(i\text{O}\)-friendly authentication techniques developed originally to build \(i\text{O}\) for TM \([\text{K LW15}]\). Let \(\Pi\) be a computation instance for (parallel) RAM computation defined by \((P, x)\), where \(P\) is represented as next-step circuit for the CPU program and \(x\) is the input.\(^{15}\) At a high level, our \(\text{CiO}\) construction outputs \(i\text{O}\) of a compiled version of \(P\) together with a compiled input. We proceed to discuss the intuition behinds our construction.

Recall that the security of \(\text{CiO}\) requires that if two computation instances \(\Pi\) and \(\Pi'\), defined by \((P, x)\) and \((P', x')\) respectively, have identical computation trace (which implies \(x = x'\)), then their \(\text{CiO}\)-ed computation instances should be computationally indistinguishable, i.e., \(\text{CiO}(\Pi) \approx \text{CiO}(\Pi')\). Note that the two programs \(P\) and \(P'\) may behave differently on other inputs \(x'' \neq x\). So, for \(\text{CiO}(\Pi)\) and \(\text{CiO}(\Pi')\) to be indistinguishable, we must restrict the obfuscation to only be able to evaluate the program on the specific input \(x\), but not other inputs.

A natural approach to do so is via authentication. Specifically, we consider a \(\text{CiO}\) obfuscator which outputs \(\tilde{\Pi}\) defined by \((i\text{O}(P_{\text{auth}}), x_{\text{auth}})\), where \(P_{\text{auth}}\) is just \(P\) augmented with some authentication mechanism and \(x_{\text{auth}}\) is an authenticated input. The hope is that the authentication mechanism, together with \(i\text{O}\) security, can ensure that an adversary receiving \(\tilde{\Pi}\) can only generate the honest computation trace of \(\Pi\), and further imply \(\text{CiO}\) security.

We discuss how this can be done in the following subsections. We first focus on the simpler case of RAM computation, which can be viewed as an abstraction of the existing techniques for TM. In Section 4.1.2, we handle the full-fledged PRAM computation by introducing several new techniques to handle new challenges in the parallel setting, in particular, to achieve full succinctness without dependency on the number of CPUs.

#### 4.1.1 \(\text{CiO for RAM computation}\)

Recall that a RAM computation instance \(\Pi\) is specified by a next-step circuit \(P\) for the CPU program and an input \(x\) stored in the memory. At each time step of the RAM computation, \(P\) takes as input the previous CPU state and the memory cell it reads in the previous time step, and outputs the next CPU state and memory access

\(^{15}\)Note that for uniform programs, the circuit size is polylogarithmic.
instruction (read or write) of this time step. For convenience, we assume that \( P \) only writes to the memory cell it reads in the previous time step.\(^{16}\) We also assume that the CPU state stores the time step \( t \).

As mentioned, we want to authenticate the computation. The CPU state can be authenticated simply by signatures, but the entire memory is large. Here we use a structure similar to the Merkle-tree\(^ {17}\)\). To authenticate the whole memory, we can store the tree root as the digest in the CPU state. The CPU program can then verify and update a memory cell locally by receiving the authentication path of the cell.

More precisely, our \( \text{CiO} \) construction outputs \( \tilde{\Pi} \) defined by \((iO(P_{\text{auth}}), x_{\text{auth}})\), where the compiled program \( P_{\text{auth}} \) expects to receive as input a signed CPU state, the read memory cell \( \ell \), and its authentication path. If the authentication path and the signature pass verification, then \( P_{\text{auth}} \) outputs a signed next CPU state and memory access instruction. Additionally, if the memory access is a write to the memory cell \( \ell \), it also updates the digest stored in the CPU state using the authentication path. The authenticated input \( x_{\text{auth}} \) consists of the initial memory content \( x \), and a signed initial CPU state that contains the Merkle tree digest of \( x \).

Let \( \Pi \) and \( \Pi' \) be two computation instances defined by \((P, x)\) and \((P', x)\) respectively with identical computation trace. To prove security, we consider a sequence of hybrids starting from \( \tilde{\Pi} \) that switches the program from \( P \) to \( P' \) time step by time step. However, to switch based on \( iO \) security, the programs in the hybrids need to be functionally equivalent, while \( P \) to \( P' \) only behave identically during honest execution. Note that normal signatures and Merkle-tree cannot guarantee functional equivalence as forgeries exist (information-theoretically). Here is the place we rely on the powerful \( iO \)-friendly authentication primitives [KLW15]. At a very high level, they allow us to switch to a hybrid program that, at a particular time step \( t \) (i.e., input with time step \( t \) stored in the CPU state), only accepts the honest input but rejects (and outputs \( \text{Reject} \)) all other inputs, which enables us to switch from \( P \) to \( P' \) at time step \( t \) using \( iO \) security.

More precisely, our \( \text{CiO} \) construction uses splittable signatures and accumulators [KLW15] instead of normal signatures and Merkle trees, respectively. Additionally, a primitive called iterators is introduced [KLW15] to facilitate the above hybrids. We refer the reader to [KLW15] for details. We can carry through the above hybrids by introducing “check-points” to hybrid programs as follows:\(^ {19}\)

- We can place a check-point at the initial step of computation, and move it from a time step \( t \) to time step \((t + 1)\) through hybrids.

- A check-point is a piece of code that, at a time step \( t \), checks if the input (or output) is the same as that in the honest computation, and forces the program to output \( \text{Reject} \) if it is different. This is an information-theoretic guarantee which enables us to switch the program at time step \( t \) based on \( iO \) security.

We can then move the check-point from the beginning to the end of the computation, and along the way switch the program from \( P \) to \( P' \). We note that this check-point technique is implicit in the security proof for message-hiding encodings [KLW15]. Our description can be viewed as an abstraction of their proof techniques.

### 4.1.2 CiO for PRAM computation

Recall that a PRAM computation instance \( \Pi \) is also specified by a next-step circuit \( P \) for the CPU program and an input \( x \) stored in the memory. However, instead of a single CPU, there are \( m \) CPUs, specified by the same program \( P \) but with different CPU id’s, performing the computation in parallel with shared random access to the memory. We assume that there are no conflict writes throughout the computation, all CPUs have synchronized read/write memory access, and all terminate at the same time step.\(^ {20}\)

---

\(^{16}\)Note that this convention can be imposed without loss of generality.

\(^{17}\)Namely, we build a Merkle tree with each memory cell being a leaf node of the tree.

\(^{18}\)Namely, the nodes along the path from the root to the cell and their neighboring nodes.

\(^{19}\)We note that the description here over-simplifies many details.

\(^{20}\)We note that the later two conventions can be imposed with \( O(\log m) \) blow up in the parallel run-time.
From parallelism, $m$ CPUs gains a factor of $m$ in the parallel run-time. A naive construction would introduce a linear overhead in $m$ in the obfuscation size, which obliterates all such gains. We thus discuss how to avoid the dependency on $m$ in CiO for PRAM computation.

**A Naive Attempt.** We can view the $m$ copies of next-step circuit as a single giant next-step circuit $P^m$ that accesses $m$ memory locations at each CPU time step. We can then compile $P^m$ to $P^m_{\text{auth}}$ and output $\tilde{\Pi}$ defined by $(\text{iO}(P^m_{\text{auth}}), x_{\text{auth}})$ in a similar way as before. This approach indeed works in terms of security and correctness. However, as $P^m$ has description size $\Omega(m)$ (since it operates on $\Omega(m)$-size input), the obfuscated computation will have description size $\text{poly}(m)$, which incurs $\text{poly}(m)$ overhead in the evaluation time.\(^{21}\)

**A Second Attempt.** Now we can only $\text{iO}$ a single (compiled) CPU program $P_{\text{auth}}$, and run $m$ copies of $\text{iO}(P_{\text{auth}})$ in the evaluation of obfuscated instance with different CPU id’s (as in the evaluation of the original $\Pi$).

Recall that we use accumulator to authenticate the (shared) memory. That is a Merkle-tree like structure with the tree root as the (shared) accumulator value $w$ stored in the CPU state, which needs to be updated when the memory content is changed. Specifically, consider a time step where $m$ CPUs perform parallel write to distinct memory cells. The CPUs need to update the shared accumulator value $w$ to reflect the $m$ writes in some way. Note that we cannot let a single CPU perform the update in one time step, because it involves processing $\Omega(m)$-size data, which makes the size of the next-step circuit dependent on $\Omega(m)$ again. Also, we cannot afford to update sequentially (i.e., each CPU takes turns to update the digest), since this blows up the parallel run-time of the evaluation algorithm by $m$ and obliterates the gains of parallelism.

To deal with this problem, we allow the instances of the (compiled) CPU program $P_{\text{auth}}$ to communicate with each other. Namely, each CPU can send a message to other CPUs at each time step. Such CPU-to-CPU communications can be emulated readily by storing the messages in the memory for the evaluator of the obfuscation. Recall that $P_{\text{auth}}$ needs to authenticate the computation, so the program needs to authenticate the communication as well. Fortunately, this can be done using splittable signatures in a natural way. We can now formulate the problem of updating the accumulator value as a distributed computing problem as follows:

There are $m$ CPUs, each holding an accumulator value $w$, memory cell index $\ell_i$, write value $\text{val}_i$, and an authentication path $\text{ap}_i$ for $\ell_i$ (received from the evaluation algorithm) as its inputs. Their common goal is to compute the updated accumulator value $w'$ with respect to the write instructions $\{(\ell_i, \text{val}_i)\}_{i \in [m]}$. Our task is to design a distributed algorithm for this problem with oblivious communication pattern\(^ {22}\), in $\text{poly} \log(m)$ rounds, and with per-CPU space complexity $\text{poly} \log(m)$. If this is achieved, the blow-up in both the parallel run-time and obfuscation size can be reduced from $\Omega(m)$ to $\text{poly} \log(m)$.

We construct an oblivious update protocol with desired complexity based on two oblivious protocols by Boyle et al. \cite{BCP14b}: an aggregation protocol that allows $m$ CPUs to aggregate information they need in parallel, and a multi-casting protocol that allows $m$ CPUs to receive messages from other CPUs in parallel. Both protocols have run-time poly-logarithmic in $m$. Roughly, our oblivious update protocol updates the Merkle-tree layer-by-layer from leaves to root. For each layer, the CPUs engage in the oblivious aggregation protocol to aggregate information for updating their local branches of the tree. They then distribute their results using the oblivious multi-casting protocol.

Back to explaining our CiO construction, we output $\tilde{\Pi}$ defined by $(\text{iO}(P_{\text{auth}}), x_{\text{auth}})$, where $P_{\text{auth}}$ is a compiled CPU program that can communicate with other CPUs and authenticate the communication by splittable signatures. The evaluation of $\tilde{\Pi}$ runs $m$ copies of $\text{iO}(P_{\text{auth}})$ and emulates the communication by routing the messages. After each memory-write time step, $P_{\text{auth}}$ maintains the accumulator value by invoking the oblivious

\(^{21}\)Note that while $P^m$ has low depth (independent of $m$), we cannot hope its obfuscated version to have low depth, as the security of $\text{iO}$ needs to hide the circuit depth. Thus, the parallel run-time is not preserved.

\(^{22}\)We mention that the oblivious communication pattern property may not be essential, but a useful feature to make the construction simple, since the CPUs do not need to decide who to send/receive messages.
update protocol. Finally, for the authenticated input $x_{\text{auth}}$, it consists of the initial memory content $x$, and the accumulator value of $x$ stored in signed CPU states as before. However, it cannot contain $m$ (signed) initial CPU states for each CPU, as otherwise the obfuscation has size dependent on $m$. This can be solved by a simple trick: we let $x_{\text{auth}}$ only consists of a single signed “seed” CPU state $s_{\text{seed}}$, and when $P_{\text{auth}}$ takes $s_{\text{seed}}$ and a CPU id $i$ as input, $P_{\text{auth}}$ outputs a signed initial state of CPU $i$.

**Does it Work? A “Pebble Game” Illustration.** Although it seems that we now have the desired efficiency, if we generalize the previous security argument (including generalization of both accumulators and iterators) directly, it would require hardwiring $\Omega(m)$ amount of information in some intermediate hybrids. As a result, $P_{\text{auth}}$ needs to be padded to size $\Omega(m)$, and $\tilde{I}$ has $\text{poly}(m)$ overhead again.

To illustrate why, we can cast the security proof as a “pebble game” over a graph defined by the computation. The amount of information that needs to be hardwired in the hybrids can be captured by the “pebble complexity” of the game. We first illustrate this pebble game abstraction for the case of RAM computation. Recall that the security proof relies on a check-point placing technique that allows us to place a check-point on the initial time step, and move it from a time step $t$ to its next time step $(t+1)$. Placing a check-point at a time step requires us to hardwire information proportional to the input (or output) size of the CPU program. The goal is to travel all time steps (to switch the programs on all time steps). In this example, the RAM computation can be viewed as a line graph with each time step being a node in the graph. A check-point is a pebble that can be placed on the first node, and can be moved from node $t$ to node $(t+1)$. The winning condition of the pebble game is to “cover” the graph, namely, to ever place a pebble on each node. The pebble complexity is the maximum number of pebbles needed in order to cover the graph, which is $2$ for the case of RAM (since technically we need to place a pebble at $(t+1)$ before removing the pebble at $t$).

To capture the hybrids for proving our CiO for PRAM, we formulate the following pebble game:

- The graph is a layered (directed acyclic) graph where each layer corresponds to $m$ CPUs’ at a certain time step. Namely, each node is indexed by $(t, i)$ where $t$ is the time step and $i$ is the CPU id. It also consists of a 0 node corresponding to the seed state. The 0 node has an outgoing edge to $(t = 1, i)$ node for every $i \in [m]$. Each node $(t, i)$ has an outgoing edge to $(t + 1, i)$ indicating the (trivial) dependency of $i$-th CPU between time step $t$ and $t + 1$. Recall that the CPUs communicate. If CPU $i$ sends a message to CPU $j$ at time step $t$, we also put an outgoing edge from $(t, i)$ to $(t + 1, j)$ to indicate the dependency.\(^{23}\)

- The pebbling rule is defined as follows: First, we can place a pebble on the 0 node. To place a pebble on a node $v$, all nodes of $v$'s incoming edges need to have a pebble on it. To remove a pebble on a node $v$, we need to “cover” all $v$’s outgoing nodes, i.e., ever place a pebble on each outgoing node. This captures the conditions about when can we put a check-point to a computation step, and when can we remove it, for our generalization of the CiO-friendly authentication techniques of KLW to the parallel setting.

- The goal is to cover the whole graph (i.e., ever places a pebble in every node) using a minimal number of pebbles. The pebble complexity of the game is the maximum number of pebbles we need to simultaneously use to cover the graph. Covering the graph corresponds to switching the programs for every computation step, and the pebble complexity captures the amount of hardwired information required in the intermediate hybrids.

Recall that our $P_{\text{auth}}$ invokes the oblivious update protocol for every (synchronized) memory-writes. It is unfortunately unclear how to play the pebble game induced by multiple invocations of the oblivious update protocol with $o(m)$ pebble complexity, and it seems likely that the pebble complexity is indeed $\Omega(m)$. Therefore, it means that the security proof requires us to hardwire $\Omega(m)$ amount of information in some intermediate hybrids.

\(^{23}\)The memory accesses in general may create dependency, but we ignore it here as the pebble complexity is already high.
A “Branch-and-Combine” Technique to Reduce Information Hardwiring. We solve the problem by introducing a branch-and-combine approach to emulate a PRAM computation (illustrated in Figure 1), which transforms the computation graph to one that has poly \(\log(m)\) pebble complexity, and preserves the parallel run-time and obfuscation size with only a poly \(\log(m)\) overhead.

At a high level, after one parallel computation step, we combine \(m\) CPU states into one “digest” state, then we branch out from the digest state one parallel computation step, which results in \(m\) CPU states to be combined again. The PRAM computation is emulated by alternating the branch and combine steps. The combine step involves \(\log m\) rounds where we combine two states into one in parallel (which forms a complete binary tree). The branch step is done in one shot which branches out \(m\) CPUs in one step in parallel. Thus, the branch-and-combine emulation only incurs \(O(\log m)\) overhead in parallel run-time. Note that this transforms the computation graph into a sequence of complete binary trees where each time step of the original PRAM computation corresponds to a tree, and the root of a time step connects to all leaf nodes of the next time step.

Now, we observe that we can use only \(O(\log m)\) pebbles to traverse the computation graph of the branch-and-combine PRAM emulation. At a high level, this is because whenever we put two pebbles at a pair of sibling nodes in the complete binary tree of the combine step, we can merge them into a single one at their parent node. This means that we only need to use one pebble for each height level of the tree. More precisely, we can move pebbles from one root to the next one by simply putting pebbles at its branched out nodes one by one in order, and merge the pebbles greedily whenever it is possible.

We refer the readers to Section 7 for the construction of the branch and combine steps. Very roughly (and oversimplifying), the combine step corresponds to constructing an accumulator tree for CPU states, and the branch step verifies an input CPU state using the accumulator and performs one computation step.

4.2 From CiO to Fully Succinct Randomized Encoding (\(\mathcal{RE}\))

In this section, we discuss how to construct fully succinct randomized encoding (\(\mathcal{RE}\)) from CiO. Recall that a randomized encoding of a computation instance \(\Pi = (P, x)\) hides everything about \(\Pi\) except its output \(y = P(x)\) and runtime \(t^*\). This requires both the content and the access pattern of the computation to be hidden.

Our construction is a fairly intuitive one: we use public-key encryption to hide the content (including the input), oblivious (parallel) RAM to hide the access pattern, then CiO to obfuscate the \(\mathcal{PKE}\) and ORAM/OPRAM compiled program. Namely, our \(\mathcal{RE}\) encoder outputs \(\hat{\Pi} = \text{CiO}(P_{\text{hide}}, x_{\text{hide}})\), where \(P_{\text{hide}}\) is a \(\mathcal{PKE}\) and ORAM/OPRAM compiled version of \(P\), and \(x_{\text{hide}}\) is an encrypted version of \(x\). At each time step, \(P_{\text{hide}}\) outputs encrypted CPU states and memory contents, and uses ORAM/OPRAM to compile its memory access (with randomness supplied by puncturable PRF for succinctness).

Note that for this to work, the decryption keys need to be hardwired in \(P_{\text{hide}}\) to evaluate \(P(x)\), so semantic security may not hold. Further note that ORAM/OPRAM only hides the access pattern when the CPU state and memory contents are hidden from the adversary. This way of arguing is hard unless the obfuscation is virtual black-box (VBB) secure [BGI+01], while CiO (just like iO) does not hide anything by itself. Indeed, hiding the access pattern is the major technical challenge.

4.2.1 \(\mathcal{RE}\) for Oblivious RAM Computation

We first focus on the simpler case of \(\mathcal{RE}\) for oblivious RAM computation where the given RAM computation instance \(\Pi = (P, x)\) has oblivious access pattern. Namely, we assume that there is a public function \(ap(t)\) that predicts the memory access at each time step \(t\), to be given to the simulator.

For this simpler case, we do not need to use oblivious RAM to hide the access pattern. We can directly use existing techniques [KLUW15] to hide the content of CPU state and memory using \(\mathcal{PKE}\). In fact, their machine-hiding encoding for TM [KLUW15] based on iO for circuits can be modified in a straightforward way to yield \(\mathcal{RE}\) for oblivious RAM computation. Our construction presented below can be viewed as a modularization and
simplification of their construction through our CiO notion.

Recall that our construction is of the form $\mathcal{R}E.\text{Encode}(\Pi) = \text{CiO}(P_{\text{hide}}, x_{\text{hide}})$, where $P_{\text{hide}}$ is a compiled version of $P$, and $x_{\text{hide}}$ is an encrypted version of $x$. Here, we only use $\mathcal{P}E$ to compile $P$, and denote the compiled program as $P_{\mathcal{P}E}$ instead of $P_{\text{hide}}$. We also denote the encrypted input by $x_{\mathcal{P}E}$ instead of $x_{\text{hide}}$.

At a high level, $P_{\mathcal{P}E}$ emulates $P$ step by step. Instead of outputting the CPU state and memory content in the clear, $P_{\mathcal{P}E}$ outputs encrypted versions of them. $P_{\mathcal{P}E}$ also expects encrypted CPU states and memory contents as input, and emulates $P$ by first decrypting these inputs. A key idea here (following [KLW15]) is to encrypt each message (either a CPU state or a memory cell) using a different key, and generate these keys (as well as encryption randomness) using puncturable PRF (PPRF), which allows us to use a standard puncturing argument (extended to work with CiO instead of iO) to move to a hybrid where semantic security holds for a particular message so that we can “erase” the message.

To make sure that each key is used to encrypt a single message, at time step $t$, $P_{\mathcal{P}E}$ encrypts the output state and memory content using the “$t$-th” keys, which are generated by PPRF with input $t$ (and some additional information to distinguish between state and memory). Likewise $x_{\mathcal{P}E}$ contains the encryption of the initial memory $x$ with different keys for each memory cell. To decrypt the input memory, $P_{\mathcal{P}E}$ needs to know which secret key to use. This can be addressed by simply storing the time tag $t$ with the encrypted memory (as a single memory cell). Namely, each memory cell for $P_{\mathcal{P}E}$ contains a ciphertext $c_{\text{mem}}$ together with a time tag $t$. We remark that no additional authentication mechanisms are needed, as authentication is taken care of by CiO as a black box.

We now turn to discuss security proof of the above construction. At a high level, we prove the security by defining a sequence of hybrids that “erase” the computation backward in time, which leads to a simulated encoding $\text{CiO}(P_{\text{Sim}}, x_{\text{Sim}})$ where all ciphertexts generated by $P_{\text{Sim}}$ as well as in $x_{\text{Sim}}$ are replaced by some encrypted special dummy symbols. More precisely, $P_{\text{Sim}}$ simulates the access pattern using the public access function $\mathcal{A}p$. For each time step $t < t^*$, $P_{\text{Sim}}$ simply ignores the input and outputs encrypted dummy symbols (for both CPU state and memory content), and outputs $y$ at time step $t = t^*$.

By erasing the computation backward in time, we consider the intermediate hybrids $\text{Hyb}_i$ where the computations of the first $i$ time steps are real, and those of the remaining time steps are simulated. Namely, $\text{Hyb}_i$ is a hybrid encoding $\text{CiO}(P_{\text{Hyb}_i}, x_{\mathcal{P}E})$, where $P_{\text{Hyb}_i}$ acts as $P_{\mathcal{P}E}$ in the first $i$ time steps, and acts as $P_{\text{Sim}}$ in the remaining time steps. To argue for the indistinguishability between $\text{Hyb}_i$ and $\text{Hyb}_{i-1}$, which corresponds to erasing the computation at the $i$-th time step, the key observation is that the $i$-th decryption key is not used in the honest evaluation, which allows us to replace the output of the $i$-th time step by an encryption of dummy through a puncturing argument. We can then further remove the computation at the $i$-th time step readily by CiO security.

In more details, to move from $\text{Hyb}_i$ to $\text{Hyb}_{i-1}$, we further consider an intermediate hybrid $\text{Hyb}'_i$ where the output of the $i$-th time step is replaced by an encryption of dummy, but the real computation is still performed. Namely, at the $i$-th time step, $P_{\text{Hyb}'_i}$ in $\text{Hyb}'_i$ still decrypts the input and emulates $P$, but replaces the output by an encryption of dummy. Note that indistinguishability between $\text{Hyb}'_i$ and $\text{Hyb}_{i-1}$ follows immediately from CiO security by observing that $(P_{\text{Hyb}'_i}, x_{\mathcal{P}E})$ and $(P_{\text{Hyb}_{i-1}}, x_{\mathcal{P}E})$ have identical computation trace.

To argue for the indistinguishability between $\text{Hyb}_i$ and $\text{Hyb}'_i$, we note that the $i$-th decryption key is not used in the honest evaluation, since the computation after time step $i$ is erased. Thus, we can puncture the randomness and erase the decryption key from the program (which uses CiO security as well), and (from $\text{Hyb}_i$) reach a hybrid where semantic security holds for the output ciphertext at time step $i$. We can then replace the ciphertext by an encryption of dummy and undo the puncturing to reach $\text{Hyb}'_i$.

There remains some details to complete the proof. First, the real encoding $\text{CiO}(P_{\mathcal{P}E}, x_{\mathcal{P}E})$ and $\text{Hyb}_{t^*-1}$ have identical computation trace, so indistinguishability follows by CiO security. Second, moving from $\text{Hyb}_0$

\footnotesize
24We remind the reader that here we only consider honest evaluation of $P_{\text{Sim}}$ on $x_{\text{Sim}}$. Any “dishonest” evaluation is “taken care of” by CiO security.

\normalsize
to the simulated encoding $\text{CiO}(P_{\text{Sim}}, x_{\text{Sim}})$ requires us to replace $x_{\mathcal{PKE}}$ by $x_{\text{Sim}}$, which can be done by a similar puncturing argument.

### 4.2.2 RE for General RAM Computation

We now deal with the main challenge of hiding access pattern by using oblivious RAM (ORAM). Recall that an ORAM compiler compiles a RAM program by replacing each memory access by a randomized procedure \texttt{OAccess} that implements memory access in a way that hides the access pattern.\(^{25}\) Given a computation instance $\Pi = (P, x)$, we first compile $P$ using an ORAM compiler with randomness supplied by puncturable PRF. Let $P_{\text{ORAM}}$ denote the compiled program. We also initiate the ORAM memory by inserting the input $x$. Let $x_{\text{ORAM}}$ denote the resulting memory. We then compile $(P_{\text{ORAM}}, x_{\text{ORAM}})$ using \texttt{PKE} in the same way as in Section 4.2.1. Namely, we use PPRF to generate multiple keys, and use each key to encrypt a single message, including the initial memory $x_{\text{ORAM}}$. Denote the resulting instance by $(P_{\text{hide}}, x_{\text{hide}})$. Our randomized encoding of $\Pi$ is $\text{CiO}(P_{\text{hide}}, x_{\text{hide}})$. However, as we discussed in the beginning of Section 4.2, it is unlikely that we can use the security of ORAM in a black-box way, since ORAM security only holds when the adversary does not learn any content of the computation. Indeed, recall in the previous section, we can only use puncturing argument to argue that semantic security holds locally for some encryption at a time.

We remark that the seminal work of Canetti et al. [CHJV15] encountered a similar technical problem in their construction of one-time RAM garbling scheme. Their construction has similar high level structure as ours, but based on a quite different machinery called asymmetrically constricted encapsulation (ACE) they built from iO for circuits. Canetti et al. provide a novel solution to this problem, but their garbling incurs dependency on the space complexity of the RAM program, and thus is not fully succinct.

In more details, their security proof established the indistinguishability of hybrids \textit{forwards in time}: At a certain hybrid $\text{Hyb}_i$, they information-theoretically erase computation before time step $i$, simulate the memory access pattern, and hardwire the configuration of the $(i+1)$-th step into the program, so as to faithfully perform the correct computation in the later steps. Moving to the $(i + 1)$-th hybrid relies on their \textit{new} strong ORAM simulatability (which is satisfied by a specific ORAM construction [CP13] they use), which enables them to replace the actual memory access at time step $(i + 1)$ by a simulated one. However, the ORAM security relies on the fact that the first $i$ steps of computation are information-theoretically hidden, and thus the hybrids need to hardwire in an intermediate configuration of size proportion to the space complexity of the program. This memory content hardwiring forces their garbling scheme to be padded to a size depending on the space complexity of the program, making the scheme non-succinct in space.

Back to our construction, a natural approach to avoid dependency on space complexity is to establish indistinguishability of hybrids \textit{backwards in time}, as in the previous section. Namely, we consider intermediate hybrids $\text{Hyb}_i$ where the computations of the first $i$ time steps are real, and those of the remaining time steps are simulated (appropriately). However, since the computation trace of the first $(i - 1)$ time steps is real, it contains enough information to carry out the rest of the (deterministic) computation. In particular, the access pattern at time step $i$ is deterministic, which means that we cannot replace it by a simulated access pattern.

**Our Solution — A Puncturing ORAM Technique for Simulation.** To solve this problem, we develop a \textit{puncturing ORAM} technique to reason about the simulation for a specific ORAM construction [CP13] (referred to as CP ORAM hereafter).\(^{26}\) At a very high level, to move from $\text{Hyb}_i$ to $\text{Hyb}_{i-1}$ (i.e., erase the computation at $i$-th time step), we “puncture” ORAM at time step $i$ (i.e., the $i$-th memory access), which enables us to replace

\(^{25}\)We remark that in contrast, for Turning machines (TM), one can make the access pattern oblivious by a deterministic oblivious TM compiler. This is the reason that [KLW15] does not need to address the issue of hiding access pattern for TM computation.

\(^{26}\)We believe that our puncturing technique works for any tree-based ORAM constructions, but we work with CP ORAM for concreteness.
the access pattern by a simulated one at this time step. We can then move (from $\text{Hyb}_i$) to $\text{Hyb}_{i-1}$ by replacing the access pattern, erasing the content and computation, and undoing the “puncturing.”

Roughly speaking, “puncturing” CP ORAM at $i$-th time step can be viewed as injecting a piece of “puncturing” code in $\text{OACCESS}$ to erase the information about access pattern at time step $i$ information-theoretically. In a bit more detail (but still at a very high level), the access pattern at time step $i$ is generated at the latest time step $t'$ that accesses the same memory location as time step $i$. The puncturing code simply removes the generation of this information at time step $t'$.

However, note that the last access time $t'$ can be much smaller than $i$, so the puncturing may cause global changes in the computation. Thus, moving to the punctured mode requires a sequence of hybrids that modifies the computation step by step. We do so by further introducing an auxiliary “partially puncturing” code that punctures the information from certain threshold time step $j \geq t'$. The sequence of hybrids to move to the punctured code corresponds to moving the threshold $j \leq i$ backwards from $i$ to $t'$.

This completes the overview of our technique. We now proceed with more details. As we rely on CP ORAM, we start by a brief review of this construction and state our key observation for puncturing CP ORAM.

**Review of the CP ORAM Construction.** In a tree-based ORAM like CP ORAM, the memory is stored in a complete binary tree (called ORAM tree), where each node is associated with a bucket. A bucket is a vector with $K$ elements, where each element is either a memory block, or an unique symbol $\text{dummy}$ stands for an empty slot. A position map $\text{pos}$ records where each memory block is stored in the tree, i.e., a node somewhere along a path from the root to the leaf indexed by $\text{pos}[\ell]$. Each memory block $\ell$ in the ORAM tree also stores its index $\ell$ and position map value $\text{pos}[\ell]$ as meta data. Each memory access to block $\ell$ is performed by $\text{OACCESS}$, which (i) reads the position map value $p = \text{pos}[\ell]$ and refreshes $\text{pos}[\ell]$ to a random value, (ii) fetches and removes the block $\ell$ (i.e., replace it by $\text{dummy}$) from the path, (iii) updates the block content and puts it back to the root (i.e., replace a $\text{dummy}$ block by the updated memory block), and (iv) performs a flush operation along another random path $p'$ to move the blocks down along $p'$ (subject to the condition that each block is stored in the path specified by their position map value). At a high level, the security follows by the fact that the position map values are uniformly random and hidden from the adversary, and thus the access pattern of each $\text{OACCESS}$ is simply two uniformly random paths, which is trivial to simulate.

The position map is large in the above construction, and is recursively outsourced to lower level ORAM structures to reduce its size. For illustration, we consider non-recursive version of the CP ORAM, where the large position map is stored in the CPU state. We handle the full-fledged recursive version in the technical section.

**Key Observation for “Puncturing” CP ORAM.** Consider the execution of an CP ORAM compiled program which accesses memory block $\ell$ in the $i$-th time step (corresponds to the $i$-th $\text{OACCESS}$ call), the access pattern at this time step is determined by the position map value $p = \text{pos}[\ell]$ at the time. So, as long as this value $p$ is information-theoretically hidden from the adversary, we can simulate the access pattern by a random path even if everything else is leaked to the adversary. On the other hand, the value is generated at the last access time $t'$ of this block, which can be much smaller than $i$, stored in both the position map and the block $\ell$ (as part of the meta data), and can be touched multiple times from time step $t'$ to $i$. Thus, the value can appear many times in the computation trace of the evaluation.

Below is a more detailed sketch of the security proof to illustrate the puncturing ORAM technique in depth.

---

27 A memory block is the smallest unit in CP ORAM, which consists of a fixed small number of memory cells.

28 Ideally, it is desirable to formalize a “puncturable” property for ORAM or the CP ORAM construction, and use the property in the security proof. Unfortunately, it is unclear how to formalize such a property without referring to our actual $\text{RE}$ construction, since it is difficult to quantify what an adversary can learn from the $\text{CIO}$ obfuscation.

29 We ignore the uniformly random path used in the flush operation here, which is trivial to simulate.
**RE Simulator and Backward-in-time Hybrids.** Our construction is $\mathcal{RE}.\text{Encode}(\Pi) = \mathcal{C}i\mathcal{O}(P_{\text{hide}}, x_{\text{hide}})$, where $P_{\text{hide}}$ is $\mathcal{P}\mathcal{K}\mathcal{E}$ and CP ORAM compiled version of $P$. We construct simulated encoding $\mathcal{C}i\mathcal{O}(P_{\text{Sim}}, x_{\text{Sim}})$ where $P_{\text{Sim}}$ simulates $P_{\text{hide}}$ for each time step of $P(x)$ (corresponding to each OACCESS call), and it simulates the access pattern by two (pseudo-)random paths supplied by PPRF (with a (different) key used in simulation). For each access, it ignores the input and outputs encryptions of dummy (as before). Note that in the rest of this section, a time step refers to a time step of $P(x)$, as opposed to a time step of $P_{\text{hide}}(x_{\text{hide}})$.

We prove the security by a sequence of hybrids that erases the computation backward in time. Namely, we consider intermediate hybrids $\text{Hyb}_i$, a hybrid encoding $\mathcal{C}i\mathcal{O}(\hat{P}_{\text{Hyb}_i}, x_{\text{hide}})$ where $\hat{P}_{\text{Hyb}_i}$ acts as $P_{\text{hide}}$ for the first $i$ time steps, and acts as $P_{\text{Sim}}$ in the remaining time steps. A main step in the proof is to show indistinguishability of $\text{Hyb}_i$ and $\text{Hyb}_{i-1}$, which corresponds to erasing the computation at the $i$-th time step. It is not hard to see that the outputs can be replaced by an encryption of dummy by a similar puncturing argument as in Section 4.2.1.

To replace the access pattern, we define a punctured hybrid $\text{Hyb}_i^{\text{punct}}$ that punctures ORAM at time step $i$.

**A Punctured Hybrid $\text{Hyb}_i^{\text{punct}}$.** Let $\ell$ be the memory block accessed at the $i$-th time step of $P(x)$, $p = \text{pos}[\ell]$ be the position map value at the time, and $t'$ be the last access time of block $\ell$ before time step $i$. Following the above key observation, our goal is to move to a hybrid where the value $p$ is information-theoretically erased. We do so by injecting a “puncturing” code that removes the generation of the value $p$ at time step $t'$. More precisely, we define a punctured hybrid $\text{Hyb}_i^{\text{punct}}$ with a hybrid encoding $\mathcal{C}i\mathcal{O}(P_{\text{Hyb}_i^{\text{punct}}}, x_{\text{hide}})$ where $P_{\text{Hyb}_i^{\text{punct}}}$ is $\hat{P}_{\text{Hyb}_i}$ with the following puncturing code added:

**Puncturing Code:** At time step $t = t'$, do not generate the value $p$, and instead of putting back the (encrypted) fetched block $\ell$ to the root of the ORAM tree, an encryption of a dummy block is put back. Moreover, the position map value $\text{pos}[\ell]$ is not updated. Additionally, the value $p$ is hardwired, and is used to emulate the memory access at the $i$-th time step.

In other words, block $\ell$ is deleted at time step $t'$ and $\text{pos}[\ell]$ remains to store the old value (used to fetch the block at time step $t'$). So, in $\text{Hyb}_i^{\text{punct}}$, the value $p$ is information-theoretically hidden in the computation trace of the first $i-1$ time steps and is only used to determine the access pattern at time step $i$. We can then use puncturing arguments for PPRF to replace $p$ by one generated by the simulation (as opposed to real) PPRF key.

We also note that since block $\ell$ is not accessed before time step $i$, the computation trace of $P_{\text{Hyb}_i^{\text{punct}}}$ before time step $i$ is identical to that of $P_{\text{Hyb}_i}$, except that each time when $P_{\text{Hyb}_i}$ touches the block $\ell$ (resp., $\text{pos}[\ell]$), it is replaced by a dummy block (resp., the old value) instead (though this can occur many times).

To complete the argument, we should argue indistinguishability between $\text{Hyb}_i$ and $\text{Hyb}_i^{\text{punct}}$. However, for simplicity of exposition, we consider a simplified goal as follows.

**A Simplified Version $\text{Hyb}_i^{\text{punct}}$ of Puncturing Hybrid.** Here we consider a simplified version of $\text{Hyb}_i^{\text{punct}}$, denoted by $\text{Hyb}_i^{\text{punct}}$, where only the block $\ell$ is removed but the $\text{pos}[\ell]$ value is still updated at time step $t'$. Namely, the puncturing code is replaced by the following simplified version.

**Puncturing Code (Simplified):** At time step $t = t'$, instead of putting back (an encryption of) the fetched block $\ell$ to the root of the ORAM tree, (an encryption of) a dummy block is put back.

We focus on indistinguishability between $\text{Hyb}_i$ and $\text{Hyb}_i^{\text{punct}}$ (i.e., “deleting” the block $\ell$) to simplify the exposition. The $\text{pos}[\ell]$ part can be addressed in a similar way to be detailed in the technical section.

**Moving from $\text{Hyb}_i$ to $\text{Hyb}_i^{\text{punct}}$.** As discussed above, the computation traces of $P_{\text{Hyb}_i}$ and $P_{\text{Hyb}_i^{\text{punct}}}$ can differ in many time steps, where each occurrence of the (encrypted) block $\ell$ is replaced by a dummy (encrypted) block. Thus, we cannot move from $\text{Hyb}_i$ to $\text{Hyb}_i^{\text{punct}}$ in one step, but requires a sequence of hybrids that
gradually modifies the computation trace of \( P_{\text{Hyb}} \) to that of \( P_{\text{Hyb}^{\text{punct}}} \) step by step, using puncturing arguments for PPRF and (local) semantic security of \( \mathcal{PKE} \) (as in Section 4.2.1). One natural approach is to keep track of the differing places in the computation trace, and replace the (encrypted) block \( \ell \) by a (encrypted) dummy block one by one. This can indeed be done carefully by a sequence of hybrids backwards in time. However, when we consider parallel RAM computation, the difference of computation traces in the corresponding hybrids is more complicated, and it becomes tedious to keep track of the differences and modify them through hybrids.

We instead introduce an auxiliary “partially puncturing” code that punctures the information of \( p \) from certain threshold time step \( j \geq t' \), and move from \( \text{Hyb}_i \) to \( \text{Hyb}^{\text{punct}}_i \) by a sequence of hybrids that moves the threshold \( j \) from \( i \geq j \) backwards to \( t' \). Such a code modification technique can be generalized to handle corresponding hybrids in the PRAM setting.

**Partially Punctured Hybrids \( \text{Hyb}^{\text{punct}}_{i,j} \).** We define partially punctured hybrids \( \text{Hyb}^{\text{punct}}_{i,j} \) indexed by a threshold time step \( j \), where the underlying \( P_{\text{Hyb}^{\text{punct}}} \) is \( P_{\text{Hyb}} \) with the partially puncturing code below added:

**Partially Puncturing Code \([j]\):** At any time step \( t > j \), if the input CPU state or memory contains the block \( \ell \), then replace it by a dummy block before performing the computation.

In other words, \( P_{\text{Hyb}^{\text{punct}}_{i,j}} \) punctures the block \( \ell \) after threshold time step \( j \) by deleting the block from its input. We will see it is important that the code removes block \( \ell \) by deleting it from the input (as opposed to output).

**Moving from \( \text{Hyb}^{\text{punct}}_{i,j} \) to \( \text{Hyb}^{\text{punct}}_{i,j-1} \).** We show indistinguishability between \( \text{Hyb}_i \) and \( \text{Hyb}^{\text{punct}}_i \) by moving the threshold \( j \) from \( i \) to \( t' \). As the main step, we prove indistinguishability between \( \text{Hyb}^{\text{punct}}_{i,j} \) to \( \text{Hyb}^{\text{punct}}_{i,j-1} \), which corresponds to deleting the block \( \ell \) from the input at time step \( j \). Now there are two cases. If the input at the \( j \)-th time step does not contain the block \( \ell \), then \( P_{\text{Hyb}^{\text{punct}}_{i,j}} \) and \( P_{\text{Hyb}^{\text{punct}}_{i,j-1}} \) have identical computation trace, and thus indistinguishability follows by CIT security. If the input contains the block \( \ell \), then the computation traces can be different. We observe that, since the block \( \ell \) is not accessed at time step \( j \), the difference is to correspondingly replace the (encrypted) block \( \ell \) by a dummy block in the output. Thus, to show indistinguishability, we use the puncturing PRF argument and semantic security of \( \mathcal{PKE} \) to modify the output.

However, the situation here is more complicated. Previously, we only modify an encryption whose corresponding decryption key is not used in the honest computation, since the computation afterward is erased. Here, the encrypted output block can later be accessed by \( P_{\text{Hyb}^{\text{punct}}_{i,j}} \) at some time step \( j < t < i \), where the encryption is not erased and thus the decryption key is still in use. Let \( \text{ct} \) be the encrypted output block \( \ell \) at the \( j \)-th time step, and \( \text{sk} \) be the corresponding decryption key. In order to replace the content of \( \text{ct} \), we proceed in the following steps, which use the property that the partially puncturing code deletes the block \( \ell \) from the input:

- We first move to a hybrid where the block \( \ell \) is hardwired, and the decryption of \( \text{ct} \) is set to the hardwired value instead of decryption using \( \text{sk} \) so that the decryption key \( \text{sk} \) is not used.
- We then replace \( \text{ct} \) by an encryption of a dummy block using puncturing PRF argument and semantic security of \( \mathcal{PKE} \). Note that this creates inconsistency in that the decryption of \( \text{ct} \) is still set to the hardwired block \( \ell \), as opposed to the dummy block.
- We now undo the hardwiring and use \( \text{sk} \) to decrypt \( \text{ct} \) again to reach \( \text{Hyb}^{\text{punct}}_{i,j-1} \). This fixes the inconsistency from the previous step. On the other hand, the decryption of \( \text{ct} \) is changed from the block \( \ell \) to dummy, so when \( \text{ct} \) is accessed in later time steps (after \( j \)), the input block \( \ell \) is replaced by a dummy block. Here is the place we use the property of partially punctured code: after time step \( j \), the input block
ℓ is replaced by a dummy block before the computation anyways. Thus, this change does not effect the computation trace, and indistinguishability follows by CiO security.

We can now argue indistinguishability of \( \text{Hyb}_i \) to \( \text{Hyb}_{i,\text{punct}} \). Indistinguishability of \( \text{Hyb}_{i,\text{punct}} \) and \( \text{Hyb}_{i,i} \) follows from CiO security by observing that they have identical computation trace. The above argument allows us to move from \( \text{Hyb}_{i,i} \) to \( \text{Hyb}_{i,i}^{\text{punct}} \). Now, note that the difference between \( \text{Hyb}_{i,i}^{\text{punct}} \) and \( \text{Hyb}_{i}^{\text{punct}} \) is that the output block \( \ell \) at time step \( t' \) is replaced by a dummy block in the later hybrid. The indistinguishability follows by the same argument using PPRF, \( \mathcal{PK}_E \), and the property of partially punctured code as above.

Recall that \( \text{Hyb}_{i}^{\text{punct}} \) is a simplified version of punctured hybrid. To move to the actual punctured hybrid \( \text{Hyb}_{i}^{\text{punct}} \), we can apply the same argument to handle the value stored in \( \text{pos}[\ell] \).

**Summarizing the Hybrids.** We summarize the long (nested) sequences of hybrids we discussed so far. Above we showed how to move from \( \text{Hyb}_i \) to \( \text{Hyb}_i^{\text{punct}} \), which corresponds to puncturing ORAM at time step \( i \). From \( \text{Hyb}_i^{\text{punct}} \), we can replace the output by encryption of dummy and replace the access pattern by a simulated one. We can then reach \( \text{Hyb}_{i-1} \) by undo the puncturing.

Finally, we can complete the proof in a similar way as the previous section, where we move from the real encoding to \( \text{Hyb}_{i-1} \) by CiO security, then move to \( \text{Hyb}_0 \) by the above puncturing ORAM technique, and then replace \( x_{\text{hide}} \) by \( x_{\text{Sim}} \) using puncturable PRF and semantic security of \( \mathcal{PK}_E \).

### 4.2.3 \( \mathcal{RE} \) for PRAM Computation

Our construction of \( \mathcal{RE} \) for PRAM is the same as our construction of \( \mathcal{RE} \) for RAM, except that we replace the CP ORAM compiler by the OPRAM compiler of Boyle et al. [BCP14b] (referred to as BCP OPRAM hereafter), a generalization of tree-based ORAM to the parallel setting. Namely, given a PRAM computation instance \( \Pi \) defined by \( (P, x) \), we first compile \( P \) into \( P_{\text{OPRAM}} \) using the BCP OPRAM compiler with randomness supplied by puncturable PRF. We also initiate the OPRAM memory by inserting the input \( x \). Let \( x_{\text{OPRAM}} \) be the resulting memory. We then compile \( (P_{\text{OPRAM}}, x_{\text{OPRAM}}) \) using \( \mathcal{PK}_E \) in the same way as in Section 4.2.1. A small difference here is that we also need to include CPU id as PPRF input to ensure single usage of each key. Denote the resulting instance by \( (P_{\text{hide}}, x_{\text{hide}}) \). Our randomized encoding of \( \Pi \) is CiO\((P_{\text{hide}}, x_{\text{hide}})\).

The security proof also follows identical steps, where we prove the security by a sequence of hybrids that erases the computation backward in time, and argue simulation of access patterns by generalizing the puncturing ORAM argument to puncturing BCP OPRAM. At a high level, the arguments generalize naturally with the following two differences: First, as the OPAccess algorithm of BCP OPRAM is more complicated, we need to be slightly careful in defining the simulated encoding CiO\((P_{\text{Sim}}, x_{\text{Sim}})\). Second, to avoid dependency on the number \( m \) of CPUs, we need to handle a single CPU at a time in the hybrids to puncture OPRAM.

**Review of BCP OPRAM Construction.** BCP OPRAM is a natural generalization of tree-based ORAM. Consider that each CPU \( j \) wants to access memory block \( \ell_j \) in a (parallel) memory access. At a high level\(^{30}\), the CPUs first communicate with each other to resolve the conflicts, and recursively invoke OPAccess to fetch and refresh the position map values. They then fetch the memory blocks from the path, put the blocks back, and flush the tree in parallel. Since the \( m \) CPUs want to access \( m \) paths \( p_j \) of the tree in parallel, they need to communicate with each other to avoid write conflicts. In the BCP OPRAM construction, the CPUs access the tree level by level, and in each level, they aggregate the access instructions, select representative to perform the access, and then distribute the answers via oblivious aggregation and oblivious multi-casting protocols.

\(^{30}\)We refer the reader to [BCP14b] for further details.
Simulated Encoding $\text{CiO}(P_{\text{Sim}}, \tau_{\text{Sim}})$. As before, $P_{\text{Sim}}$ simulates $P_{\text{hide}}$ for each (parallel) time step of $P(x)$, and at each step $P_{\text{Sim}}$ uses simulated access pattern and erases the computation by ignoring the input and outputs encryptions of dummy. Here, we need to simulate the parallel access pattern of OPAccess, which is more complicated and involves polylogarithmic time steps. In particular, the access pattern of the OPAccess depends on the paths $p_j$’s each CPU wants to access. If we still erase all the content step by step, we would not have enough information to simulate the second half access pattern of OPAccess once the content in the first half is erased. Nevertheless, the key observation here is that the access pattern is fully determined by the paths $p_j$’s each CPU wants to access, which are public information revealed in the execution. So, we can view these $p_j$’s as public states of OPAccess, and do not erase its content in the hybrids. In other words, we generate simulated path $p_j$ for each CPU, and store them as public states to simulate the access pattern of OPAccess.

Puncturing BCP OPRAM CPU by CPU. As BCP OPRAM is a generalization of tree-based ORAM, it is not hard to see that the puncturing argument generalized to work for BCP OPRAM as well. Namely, it suffices to information-theoretically hide the values of the paths $p_j$’s to simulate the access pattern, and this can be done by injecting a puncturing code. Additionally, we observe that this can be done CPU by CPU. Namely, for each $p_j$ accessed by CPU $j$, we can inject a puncturing code at the corresponding time step $t'_j$ that the value $p_j$ is generated, to remove the generation of $p_j$. Also, we can move to this punctured hybrid by a sequence of partially punctured hybrids as before, by gradually puncturing the value of $p_j$ backwards in time, per time-step and per CPU. Upon reaching this punctured hybrid, we can switch $p_j$ to a simulated one, undo the puncturing, and move to the next CPU. In this way, we switch the paths $p_j$’s to simulated version one by one, and never need to hardwire information of size depending on $m$ throughout the hybrids, which maintain full succinctness.

5 Computation-Trace Indistinguishable Obfuscation (CiO)

We define a new primitive called Computation-Trace Indistinguishable Obfuscation (CiO), which produces indistinguishable obfuscated computations as long as the input computations give identical computation trace. For this, we need to define a formal notion of computation trace, and before that, a formal notion of (distributed) computation systems.

We define a distributed computation system $\Pi$ as a tuple consisting of a collection initial states $\{s_k^0\}$, a shared initial memory $\text{mem}^0$, and a collection of stateful algorithms $\{F_k\}$. The entity which executes the stateful algorithm $F_k$, named agent $A_k$, takes as input the state in the previous time step, an access command received from the memory, and some communication messages received from the other agents. It outputs a new state, an access command to be sent to the memory, and some communication messages to be sent to the other agents. The memory which receives access commands from all the agents processes these commands and outputs some new access commands to be returned to all the agents. Having specified these, the computation trace of a distributed computation system is simply defined as the collection of the states, access commands and communication messages at all time steps.

The philosophy behind such a definition is to decouple the functionality of a program and its computation trace. On one hand, programs with the same functionality can still produce different computation traces. On the other hand, we wish to only focus at one particular instance of a program-input pair $(P, x)$ rather than the entire functionality of $P$.

5.1 Model of Distributed Computation Systems

Definition 5.1. We define a distributed computation system $\Pi$ with an evaluation algorithm $\text{evaluate}$ as follows.
Description of the Computation. A computation \( \Pi \) consists of \( m \) agents \( A_1, \ldots, A_m \) and a shared memory component \( M \). Each agent \( A_k \) where \( k \in [m] \) is associated with: (i) a stateful algorithm \( F_k \); (ii) a register for storing its local state \( st_k \); (iii) an incoming communication buffer which allows any other agents \( A_j \) where \( j \in [m] \setminus \{k\} \) to send communication messages \( c_{k_{j-1}} \) to agent \( A_k \); (iv) an incoming memory access buffer which stores value \( a_{k_{k-1}} \) that read from the shared memory.

Memory component \( M \) is a distinguished component in the computation system, associated with: (i) a memory \( \text{mem} \); (ii) an incoming memory access buffer which allow any agents \( A_j \) where \( j \in [m] \) to write the memory with value \( a_{M_{k-1}} \).

For all \( k \in [m] \), for all \( j \in [m] \setminus \{k\} \), \( \Pi \) is set to be \((st_k, c_{k_{j-1}}, a_{k_{k-1}}, a_{M_{k-1}}, \text{mem})\) with the initialized values \((st_k^0, c_{k_{j-1}}^0, a_{k_{k-1}}^0, a_{M_{k-1}}^0, \text{mem}^0)\) given externally.

We denote the computation system as \( \Pi = (\{\text{mem}^0, \{st_k^0, \{c_{k_{j-1}}^0\}_{j \in [m] \setminus \{k\}}, a_{k_{k-1}}^0, a_{M_{k-1}}^0, \text{mem}^0\}_{k \in [m]}\}, \{F_k^m\}_{k \in [m]}) \).

Computation System Evaluation Procedure. The procedure \( \text{evaluate}() \) will evaluate the system \( \Pi \) by rounds. For each round \( t > 0 \),

- Each agent \( A_k \) where \( k \in [m] \) operates as follows:
  - Reads its incoming communication buffers and memory access buffer, and obtains \( c_{k_{j-1}}^{t-1} = \{c_{k_{j-1}}^{t-1}\}_{j \in [m] \setminus \{k\}} \) and \( a_{k_{k-1}}^{t-1} \) respectively.
  - Computes \((st_k^t, a_{k_{k-1}}^t, c_{k_{j-1}}^t) \leftarrow F_k(st_k^{t-1}, a_{k_{k-1}}^{t-1}, c_{k_{j-1}}^{t-1})\), where \( c_{k_{j-1}}^t = \{c_{k_{j-1}}^t\}_{j \in [m] \setminus \{k\}} \).
  - If \( st_k^t = (\text{halt}, \cdot) \) or Reject then \( a_{M_{k-1}}^t = \perp, c_{k_{j-1}}^t = \perp \) for \( j \in [m] \setminus \{k\} \), \( st_k^t = st_k^{t-1} \).
  - Writes the value \( a_{M_{k-1}}^t \) to the incoming memory access buffers, and sends the messages \( e_{j_{j-1}}^t \) to the incoming communication buffer of agent \( j \in [m] \setminus \{k\} \).

- The memory component \( M \) operates as follows:
  - Reads its incoming memory access buffers, and obtains \( a_{M_{k-1}}^t, \ldots, a_{M_{k-1}}^t \).
  - Computes \((\text{mem}^t, a_{k_{k-1}}^t, \ldots, a_{M_{k-1}}^t) \leftarrow \text{access}(\text{mem}^{t-1}, a_{k_{k-1}}^{t-1}, \ldots, a_{M_{k-1}}^{t-1})\), where access performs the memory access command \( a_{M_{k-1}}^{t-1} \) on memory \( \text{mem}^{t-1} \) and output its corresponding read value \( a_{k_{k-1}}^{t-1} \) and update memory \( \text{mem}^t \) for each \( k \in [m] \).
  - Returns value \( a_{k_{k-1}}^t \) to each agent \( k \)'s memory access buffer, where \( k \in [m] \).

Terminologies. To facilitate presentation, we introduce the following terminologies.

- The terminating time \( t^* \), if it exists, is the smallest \( t \) such that \( st_k^t = (\text{halt}, \cdot) \) for all \( k \in [m] \).
- The computation configuration at any time \( t \geq 0 \), defined as \( \text{Conf}(\Pi, t) = \{\{st_k^t, a_{k_{k-1}}^t, a_{M_{k-1}}^t, c_{k_{j-1}}^t\}_{k \in [m]}, \text{mem}^t\} \), is the output of the evaluation at time \( t \).
- The computation trace is defined as \( \text{Trace}(\Pi) = \{\text{Conf}(\Pi, t)\}_{t \geq 0} \).
- The next step function \( F \) is another representation of all \( F_k \) such that \( F(k, st, a, c) = F_k(st, a, c) \) for all \( st, a, c \).

Remark 5.2. For specific computation systems, we can restrict the initial states, access commands and communication messages to some default values. Such initial values can thus be dropped from the tuple \( \Pi \), and we use the simplified form \( \Pi = ((\text{mem}^0, st_1^0, st_2^0, \ldots, st_m^0), (F_1, F_2, \ldots, F_m)) \).

Remark 5.3. For easier presentation, the model of computation system defined here is for PRAM. We can easily generalize the definition to support richer syntax for even more fine-grained models of computation.
5.2 Computation-trace Indistinguishability Obfuscation

In this subsection, we introduce a new security notion named Computation-trace Indistinguishability Obfuscation (CiO for short). The original iO captures the security intuition that if the functionalities of the computations are identical, then the complied / obfuscated versions are indistinguishable. Here, we want to capture even milder security property that if the computation traces are identical, then the obfuscated versions are indistinguishable.

A CiO scheme consists two parts, a randomized compilation procedure \( \text{Obf} \) which transforms a computation system to an “obfuscated” computation system, and a deterministic evaluation algorithm \( \text{Eval} \) which evaluates the obfuscated system to return the output.

**Definition 5.4.** Let \( \mathcal{P} \) be a collection of computation systems. A computation-trace indistinguishability obfuscation scheme w.r.t \( \mathcal{P} \), denoted as \( \text{CiO} = \{\text{Obf}, \text{Eval}\} \), is defined as follows:

**Compilation algorithm** \( \tilde{\Pi} := \text{Obf}(1^\lambda, \Pi; \rho) \): \( \text{Obf}() \) is a probabilistic algorithm which takes as input the security parameter \( \lambda \), the computation system \( \Pi \in \mathcal{P} \) and some randomness \( \rho \), and returns a complied / obfuscated system \( \tilde{\Pi} \) as output.

**Evaluation algorithm** \( \text{conf} := \text{Eval}(\tilde{\Pi}) \): \( \text{Eval}() \) is a deterministic algorithm which takes as input the obfuscated system \( \tilde{\Pi} \), and returns a configuration of the original computation system \( \Pi \) as output.

**Correctness.** For all \( \Pi \in \mathcal{P} \) with termination time \( t^* \) and all randomness \( \rho \), let \( \tilde{\Pi} := \text{Obf}(1^\lambda, \Pi; \rho) \). It holds that \( \text{Eval}(\tilde{\Pi}) = \text{Conf}(\Pi, t^*) \).

**Security.** For any (not necessarily uniform) PPT distinguisher \( D \), there exists a negligible function \( \text{negl}(\cdot) \) such that, for all security parameters \( \lambda \in \mathbb{N} \), \( \Pi^0, \Pi^1 \in \mathcal{P} \) where \( \text{Trace}(\Pi^0) = \text{Trace}(\Pi^1) \), it holds that

\[
| \Pr[D(\text{Obf}(1^\lambda, \Pi^0))] = 1] - \Pr[D(\text{Obf}(1^\lambda, \Pi^1))] = 1 | \leq \text{negl}(\lambda).
\]

**Efficiency.** We require \( \text{Obf} \) runs in time \( \tilde{O}(\text{poly}(|\Pi|)) \), and efficient \( \text{Eval} \) runs in time \( \tilde{O}(t^*) \). That is, a client can efficiently compile \( \Pi \), and a server carries out evaluation in time comparable to the insecure computation.

Note that a trivial construction is to perform all computations in the \( \text{Obf} \) algorithm. However, this trivial case does not work because we require \( \text{Obf} \) should be efficient and cannot depend on computation time \( T \).

6 Starting Point: Constructing CiO in the RAM Model (CiO-RAM)

As introduced in Section 5, CiO is a type of obfuscation which guarantees the indistinguishability of the obfuscation of computations which give identical computation trace. Viewing in another perspective, CiO in some sense forces the evaluator to evaluate the obfuscated computation as intended, so as to only produce the intended computation trace.

To construct CiO, a natural idea is therefore to authenticate the output of a time step and verify the integrity of the input in the next time step. Straightforwardly, the output state (which is small in size) will be signed using a signature scheme. On the other hand, the memory has a much larger size and is controlled by the evaluator outside the obfuscated program. For authenticating the memory, a Merkle-tree like structure is used to produce a digest which is then stored in the CPU state. Having a similar construction but a more vigorous and ambitious security goal, our CiO can be referred to as an abstraction of KLW.

In this section, we first tackle the simpler task of constructing CiO for RAM computation. For this, we compile the underlying function \( F \) into the following function \( \tilde{F} \) which verifies and authenticates its inputs and
outputs respectively. Concretely, upon receiving as input a time \( t \), a CPU state, and a bit read from the memory, \( \tilde{F} \) verifies the signature of the input CPU states and the memory digest, before executing the underlying function \( F \). \( \tilde{F} \) then signs the resulting CPU state, updates the Merkle-tree-like structure to obtain an updated memory digest, and eventually outputs the time \( (t + 1) \), a new CPU state, and an access command. We then convert \( \tilde{st}^0 \) and \( \tilde{mem}^0 \) to an authenticated form \( (\tilde{st}^0, \tilde{mem}^0) \), and compute \( \tilde{CiO}(\Pi) = ((\tilde{mem}^0, \tilde{st}^0), \tilde{F}) \) where \( \tilde{F} = iO(\tilde{F}) \).

6.1 Building Blocks

In our \( CiO \) construction in Section 6.2, we will use several building blocks: accumulator, iterator, splittable signature, puncturable PRF, and indistinguishability obfuscation. The formal definitions of these primitives can be found in Section A. We next define the parameters for the building blocks we will use in our \( CiO \) construction.

- Accumulator scheme \( Acc = \{\text{Setup, SetupEnforceRead, SetupEnforceWrite, PrepRead, PrepWrite, VerifyRead, WriteStore, Update}\} \) with message space \( \{0, 1\}^{\ell_{msg}} \) and accumulated value space \( \{0, 1\}^{\ell_{acc}} \).
- Iterator scheme \( ltr = \{\text{Setup, SetupEnforceIterate, Iterate}\} \) with message space \( \{0, 1\}^{\ell_{itr} + \ell_{acc} + \ell_{msg}} \) and iterated value space \( \{0, 1\}^{\ell_{itr}} \).
- Splittable signature scheme \( Spl = \{\text{Setup, Sign, Verify, Split, AboSign}\} \) with message space \( \{0, 1\}^{\ell_{itr} + \ell_{acc} + \ell_{msg}} \). We will assume \( Spl.\text{Setup} \) uses \( \ell_{rnd} \) bits of randomness.
- Puncturable PRF scheme \( PPRF = \{\text{Setup, Puncture, Eval}\} \) with key space \( K \), punctured key space \( K_{\text{punct}} \), domain \([T]\), and range \( \{0, 1\}^{\ell_{msg}} \).
- Indistinguishability obfuscation scheme \( iO \).

6.2 Construction for \( CiO\text{-}RAM \)

We construct \( CiO \) in the RAM model. Informally, a RAM consists of a single CPU, with random access to an external memory, executing a next-step circuit \( F \) step by step until reaching the termination state, which embeds the computation result \( P(x) \) for some program \( P \) evaluated on some input \( x \). A RAM computation \( \Pi \) can hence be specified by a program \( P \) and an initial input \( x \). The evaluator interprets the input \( x \) so as to prepare the initial state \( \tilde{st}^0 \) and the initial memory \( \tilde{mem}^0 \), to which it has random access ability. \( P \) is converted to the stateful algorithm \( F \). At each time step, \( F \) is executed with the state in the previous time step and a bit read from the memory as input. \( F \) outputs a new state for the next step, and a memory access command.

Formally, the class of distributed computation for RAM, denoted by \( \mathcal{P}_{\text{RAM}} \), is defined as follows:

**Definition 6.1 (RAM Computation Class).** We define \( \mathcal{P}_{\text{RAM}} \) as a class of distributed computation systems for RAM computation with a single agent \( k \) (a.k.a. CPU) and a memory \( M \) where

- the terminating time \( t^* \) is bounded by \( 2^\lambda \),
- the memory size \( |\text{mem}| \) is bounded by \( \text{poly}(\lambda) \),
- the state size \( |\tilde{st}| \) and the communication buffers size \( |a_{A \leftarrow M}| \) and \( |a_{M \leftarrow A}| \) are bounded by \( \text{poly log}(\lambda) \),
- the initial access commands are empty, i.e. \( a^0_{A \leftarrow M} := \bot \) and \( a^0_{M \leftarrow A} := \bot \).

In this subsection, we describe our scheme \( \tilde{CiO} = \tilde{CiO}\{\text{Obf, Eval}\} \) where \( \tilde{CiO}.\text{Obf} \) can transform a given computation system \( \Pi \in \mathcal{P}_{\text{RAM}} \) into an obfuscated computation system \( \tilde{\Pi} \). Here

\[
\Pi = ((\text{mem}^0, \tilde{st}^0), F),
\]

\[
\tilde{\Pi} = ((\tilde{\text{mem}}^0, \tilde{st}^0), \tilde{F}).
\]
Compilation algorithm \( \tilde{\Pi} \leftarrow \text{CiO.Obf}(1^\lambda, \Pi) \). The compilation algorithm \( \text{Obf}(\cdot) \) consists of several steps.

**Step 1: Generating parameters.** The compilation algorithm computes the following parameters for the obfuscated computation system:

\[
K_A \leftarrow \text{PPRF.Setup}(1^\lambda) \\
(\text{pp}_{\text{Acc}}, \hat{w}_0, \text{store}_0) \leftarrow \text{Acc.Setup}(T) \\
(\text{pp}_{\text{itr}}, v^0) \leftarrow \text{itr.Setup}(T)
\]

**Step 2: Generating stateful algorithms \( \tilde{F} \).** Based on the parameters \( T, \text{pp}_{\text{Acc}}, \text{pp}_{\text{itr}}, K_A \) generated above, as well as program \( F \), we define the program \( \tilde{F} \) in Algorithm 1.

**Algorithm 1: \( \tilde{F} \)**

<table>
<thead>
<tr>
<th>Input</th>
<th>( \hat{\sigma} \in (t, \hat{\sigma}<em>{\hat{\text{M}}</em>{\hat{\lambda}}} \in (\sigma_{\hat{\text{M}}<em>{\hat{\lambda}}}, \pi</em>{\text{in}})) ) where ( \sigma_{\hat{\text{M}}<em>{\hat{\lambda}}} = (\hat{\text{I}}, \text{B}</em>{\text{in}}) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data:</td>
<td>( T, \text{pp}<em>{\text{Acc}}, \text{pp}</em>{\text{itr}}, K_A )</td>
</tr>
</tbody>
</table>

1. If \( \text{Acc.VerifyRead}(\text{pp}_{\text{Acc}}, w_{\text{in}}, \text{I}_{\text{in}}, \text{B}_{\text{in}}, \pi_{\text{in}}) = 0 \) output \( \text{Reject} \);
2. Compute \( r_A = \text{PRF}(K_A, t - 1) \);
3. Compute \( (\text{sk}_A, \text{vk}_A, \text{vk}_A,\text{rej}) = \text{Spl.Setup}(1^\lambda; r_A) \);
4. Set \( m_{\text{in}} = (v_{\text{in}}, \hat{\sigma}_{\hat{\text{in}}}, \hat{\text{I}}_{\text{in}}) \);
5. If \( \text{Spl.Verify}(\text{vk}_A, m_{\text{in}}, \sigma_{\text{in}}) = 0 \) output \( \text{Reject} \);
6. Compute \( (\text{st}_{\text{out}}, \hat{\sigma}_{\hat{\text{M}}_{\hat{\lambda}}} | \hat{\text{I}}_{\text{in}}) \leftarrow F(\text{st}_{\text{in}}, \hat{\sigma}_{\hat{\text{M}}_{\hat{\lambda}}}) \) where \( \hat{\sigma}_{\hat{\text{M}}_{\hat{\lambda}}} = (\text{I}_{\text{out}}, \text{B}_{\text{out}}) \);
7. If \( \text{st}_{\text{out}} = \text{Reject} \) output \( \text{Reject} \);
8. Set \( w_{\text{out}} = \text{Acc.Update}(\text{pp}_{\text{Acc}}, w_{\text{in}}, \text{B}_{\text{out}}, \pi_{\text{in}}) \);
9. If \( w_{\text{out}} = \text{Reject} \) output \( \text{Reject} \);
10. Compute \( v_{\text{out}} = \text{itr.Iterate}(\text{pp}_{\text{itr}}, v_{\text{in}}, (\text{st}_{\text{in}}, w_{\text{in}}, \text{I}_{\text{in}})) \);
11. If \( v_{\text{out}} = \text{Reject} \) output \( \text{Reject} \);
12. Compute \( r_A' = \text{PRF}(K_A, t) \);
13. Compute \( (\text{sk}_A', \text{vk}_A', \text{vk}_A',\text{rej}) = \text{Spl.Setup}(1^\lambda; r_A') \);
14. Set \( m_{\text{out}} = (v_{\text{out}}, \text{st}_{\text{out}}, w_{\text{out}}, \text{I}_{\text{out}}) \);
15. Compute \( \sigma_{\text{out}} = \text{Spl.Sign}(\text{sk}_A', m_{\text{out}}) \);

Output \( \tilde{\text{st}}_{\text{out}} = (t + 1, \text{st}_{\text{out}}, v_{\text{out}}, w_{\text{out}}, \sigma_{\text{out}}) \), \( \hat{\sigma}_{\hat{\text{M}}_{\hat{\lambda}}} = \hat{\sigma}_{\hat{\text{M}}_{\hat{\lambda}}} \).

The compilation procedure then computes an obfuscation of the program \( \tilde{F} \). That is, \( \tilde{F} \leftarrow \text{iO.Gen}(\tilde{F}) \).

**Step 3: Generating the initial configuration \( (\tilde{\text{mem}}, \tilde{\text{st}}^0) \).** Recall that \( \hat{\sigma}_{\hat{\text{M}}_{\hat{\lambda}}} = \bot, \hat{\sigma}_{\hat{\text{M}}_{\hat{\lambda}}} = \bot \). Based on given \( \text{mem}^0, \text{st}^0 \), the compilation procedure computes the initial configuration for the complied computation system as follows.

- For each \( j \in \{1, \ldots, |\text{mem}^0|\} \), it computes iteratively:

\[
\pi_j \leftarrow \text{Acc.CreateWrite}(\text{pp}_{\text{Acc}}, \text{store}_{j-1}, j) \\
\hat{w}_j \leftarrow \text{Acc.Write}(\text{pp}_{\text{Acc}}, \hat{w}_{j-1}, j, x_j, \pi_j) \\
\text{store}_{j} \leftarrow \text{Acc.WriteStore}(\text{pp}_{\text{Acc}}, \text{store}_{j-1}, j, \text{mem}^0[j])
\]

Set \( w^0 := \hat{w}_{\text{mem}^0} \), and \( \text{store}^0 := \text{store}_{\text{mem}^0} \).
Compute $\sigma^0$ as follows:

$$r_A \leftarrow \text{PRF}(K_A, 0)$$

$$(sk^0, vk^0) \leftarrow \text{Spl.Setup}(1^\lambda; r_A)$$

$$\sigma^0 \leftarrow \text{Spl.Sign}(sk^0, (0, w^0, v^0))$$

Now we can define the initial configuration as

$$\tilde{\text{mem}}^0 = \text{store}^0$$

$$\tilde{st}^0 = (0, st^0, v^0, w^0, \sigma^0)$$

**Final step.** The compilation procedure returns $\tilde{\Pi} = ((\tilde{\text{mem}}^0, \tilde{st}^0), \tilde{F})$ as output.

**Evaluation algorithm** $\text{conf} := \text{Eval}(\tilde{\Pi})$. Upon receiving an obfuscated system $\tilde{\Pi}$, the evaluation algorithm carries out the following:

1. Set $\tilde{a}^0_{k-M} = \perp$. For $t = 1$ to $T$, perform following procedures until $\tilde{F}$ outputs a halting state $\tilde{st}^*$ at that halting time $t^*$:
   - Compute $(\tilde{st}^t, \tilde{a}^{t}_{k-M}) \leftarrow \tilde{F}(\tilde{st}^{t-1}, \tilde{a}^{t-1}_{k-M})$;
   - Run $(\tilde{\text{mem}}^t, \tilde{a}^{t}_{k-M}) \leftarrow \text{access}(\tilde{\text{mem}}^{t-1}, \tilde{a}^{t-1}_{k-M})$, where access is defined in Algorithm 2.

2. Parse $\tilde{\text{mem}}^{t*} = \text{mem}^{t*}$ and $\tilde{st}^* = (t^*, st^{t*}, v^{t*}, w^{t*}, \sigma^{t*})$. Output $\text{conf} = (\text{mem}^{t*}, st^{t*}, a_{k-M}^{t*}, a_{k-M}^{t*})$ where $a_{k-M}^{t*} = a_{k-M}^{t*} = \perp$.

**Algorithm 2:** access

```
Input : \text{mem}^{in}, a_{k-M}^{in} = (I^{in}, B^{in})
1 If \tilde{a}_{k-M}^{in} = \perp, output \text{mem}^{out} = \tilde{\text{mem}}^{in}.
2 Compute \tilde{\text{mem}}^{out} \leftarrow \text{WriteStore}(pp_{\text{Acc}}, \tilde{\text{mem}}^{in}, (I^{in}, B^{in}));
3 Compute ((I^{out}, B^{out}), \pi^{out}) \leftarrow \text{PrepRead}(pp_{\text{Acc}}, \tilde{\text{mem}}^{out}, I^{in});
4 Output (\tilde{\text{mem}}^{out}, \tilde{a}_{k-M}^{out} = ((I^{out}, B^{out}), \pi^{out}));
```

**Efficiency.** Let $|F|$ be the description size of program $F$, $n$ be the description size of initial memory $\text{mem}^0$, computation system $\Pi$ proceeds with time and space bound $T$ and $S$. Assuming iO is a circuit obfuscator with circuit size $|iO(C)| \leq \text{poly}|C|$ for given circuit $C$. Our GiO for RAM has following complexity:

- Compilation time and is $\tilde{O}(\text{poly}(|F|) + n)$.
- Compilation size is $\tilde{O}(\text{poly}(|F|) + n)$.
- Evaluation time is $\tilde{O}(T \cdot \text{poly}(|F|))$.
- Evaluation space is $\tilde{O}(S)$, where $S$ term is needed by $F$ intrinsically.

**Theorem 6.2.** Assume iO is a secure indistinguishability obfuscation for circuits scheme, PPRF is a secure puncturable PRF scheme, ltr is a secure iterator, Acc is secure positional accumulator scheme, and Spl is a secure splittable signature scheme. Then construction GiO is a computation-trace indistinguishability obfuscation scheme with respect to class $\mathcal{P}_{\text{RAM}}$.

The proof can be found in Section B.1.
7 Constructing CiO in the PRAM Model (CiO-PRAM)

In this section we construct a computation-trace indistinguishability obfuscation scheme CiO in the PRAM model. Our final scheme CiO-PRAM is quite technical, and thus for facilitating presentation, we will illustrate our main ideas gradually via three attempts.

First, as a naive attempt, we directly extend our CiO-RAM scheme into that in the PRAM model. However, we face two technical challenges: (i) In our CiO-RAM construction, memory accumulator has been used. We therefore need a new strategy to efficiently compute the memory accumulator digest in the parallel setting. (ii) In the PRAM model, for each CPU step, its output depends on all previous CPU steps (and further depends on their own previous steps). We therefore need to track these dependencies in the security proof. This is a significant challenge since we are not able to hardwire too much information for efficiency. In Section 7.1, we will formalize the dependency problem.

In our second attempt, we focus on the dependency problem that raised in the naive attempt above. Instead of directly providing a solution in the standard PRAM model, we here consider a special model, memoryless PRAM model PRAM− which has no memory component but allows communications between CPUs. We remark that to construct CiO in the PRAM− model, there exists the dependency issue in this model. To solve the issue, we introduce “branch-and-combine” technique, which allows us to maintain an accumulator that stores m CPU states and messages, without scarifying efficiency too much. In Section 7.5, we will present this technique.

Finally, in our full-fledged attempt, we extend the above PRAM− model solution to construct CiO in the standard PRAM model. In addition to adopting the branch-and-combine technique, we here also use parallel accumulator to compute accumulator digest in the standard PRAM model. See Section 7.6 for more details.

Section Outline. In the next subsection (Section 7.1), we will describe the naive attempt based on CiO for RAM and briefly discuss the reason why it fails. In addition, we show that there exists the dependency problem in parallel setting. The remainder of this section will be organized as follows. For completeness we list the building blocks for our constructions in Section 7.2. Among the building blocks, we will introduce in Section 7.3, a new primitive named Topological Iterators, which will replace the (ordinary) iterator in our construction. Then, we will present parallel accumulator as the solution to the first challenge (i) in Section 7.4. Next, as a warm-up to overcome the second challenge (ii), a construction of CiO for memoryless model PRAM− is shown by using a new branch-and-combine technique in Section 7.5, with its security proof in Section B.3. Finally, in Section 7.6, we will show the full-fledged construction of CiO for (standard) PRAM, with its security proof sketched in Section B.4.

7.1 Generalizing CiO-RAM for CiO-PRAM: A “Pebble Game” Illustration

To construct CiO for PRAM, a trivial solution is to convert PRAM computation Π to RAM computation Π′ and to obfuscate Π′ with CiO for RAM in a black-box manner. However, this convert-to-RAM solution is not acceptable because it has \(O(m)\) parallel time overhead multiplicatively, which does not benefit from parallelization. To utilize the benefits of parallel computation, our goal is to construct an efficient CiO for PRAM such that minimize the parallel time overhead. In general, we require the parallel time overhead to be \(\omega(m)\).

An attempt to build efficient CiO for PRAM is through the generalization of CiO for RAM directly. Let Π be a PRAM computation composed of an m-CPU PRAM program \(P\) and an input \(x\). The program \(P\) takes CPU id \(i\) as input and emulates the \(i\)-th CPU. Then we can obfuscate \(P\) associated with \(i\) and the input \(x\) by the same way of CiO for RAM. Finally, the evaluation algorithm runs \(m\) copies of the obfuscated program in parallel with different CPU id to emulate the PRAM computation. It preserves the parallel runtime of the evaluation algorithm.
The construction of CiO for RAM (presented in Section 6) follows KLW construction, which utilizes splittable signature, iterator, and accumulator. To realize CiO for PRAM, we need to address the issue of updating accumulator digest in the parallel setting. \( m \) CPUs can perform parallel writes to different memory cells, and they need to obtain updated accumulator digest in some way. However, we face the following distributed algorithm problem for updating the accumulator digest: There are \( m \) CPU agents, where each CPU \( i \) holds the same accumulator digest \( w \), memory cell index \( \ell_i \), write value \( val_i \), and an authentication path \( \pi_i \) for \( \ell_i \) (received from the evaluation algorithm) as its inputs, with the goal of computing the updated accumulator digest \( w' \) with respect to write instructions \( \{(\ell_i, val_i)\}_{i \in [m]} \). We need a distributed algorithm to solve this problem with oblivious communication pattern, \( \text{poly} \log(m) \) rounds, and per-CPU space complexity \( \text{poly} \log(m) \), where oblivious communication requires the sender and receiver of any message be public information and independent from the input. With oblivious communication, a message can be signed and verified with a fixed pair of signature keys, which authenticates this message just by signatures to CPU states. This is a non-trivial problem, but not too difficult. Our solution (the parallel accumulator) is to rely on an oblivious update protocol with desired complexity based on oblivious aggregation and oblivious multicasting protocols constructed in [BCP14b]. For more details, we will introduce the parallel accumulator in Section 7.4.

With the above update protocol, each CPU can concurrently obtain the correct accumulator digest, and then we have a construction that emulates the PRAM execution with \( \text{poly} \log(m) \) overhead in both CPU program size and parallel time complexity. Then, it seems that we can directly generalize the proof techniques of CiO for RAM to prove the security of CiO for PRAM. However, if we were to prove the security of the above construction, in the proof, we will still need to hardwire all \( m \) CPU states (at some time step \( t \)) in some intermediate hybrids. As a result, the obfuscated program must be padded to size \( \Omega(m) \), which leads to inefficient constructions because each step takes time \( \Omega(m) \) and the total parallel time is multiplied by a factor of \( \Omega(m) \). The reason why hardwiring \( \Omega(m) \) information in the program is necessary is illustrated in the following “pebble game”.

**Pebble Game Illustration.** A pebble game is a type of mathematical game played by moving pebbles on a directed graph. The pebble game that involves placing pebbles on the nodes of a directed acyclic graph \( DAG \) according to certain rules which are given as follows.

- A step of the game is either placing a pebble on an empty node of \( DAG \) or removing a pebble from a previously pebbled node.
- A pebble can be added to node \( v \) only if either (1) all its predecessors \( u \), such that \( u \rightarrow v \), have pebbles, or (2) \( v \) is a source node.
- The pebble on a node \( v \) can be removed only if all its successors \( u' \), such that \( v \rightarrow u' \), had been traversed by some other pebbles.
- The winning condition of the game is to successively put pebbles each node to traverse the whole graph (in any order) while minimizing the number of pebbles that are ever on the graph simultaneously.

We rely on an (oversimplified) interpretation of the security proof as a pebble game, to show why hardwiring \( m \) CPU states is necessary. Firstly, we show that the pebble game illustration is applicable to the KLW proof techniques in proving the security of CiO for RAM, where a formal proof has already presented in Section B.1. Conceptually, we can interpret each time step \( t \) as a node and the connection of two time steps as an edge. The computation will be transformed into a line path, and thus the KLW proof techniques (Hyb\(_{0,2,i}\) and Hyb\(_{0,2',i}\)) can be viewed as a way to put and move a check point (pebble) on the nodes. When the pebble is placed on a node \( t \), we obtain an information theoretical guarantee of the correctness of the input/output of the \( t \)-th step computation, such that the input/output values from an honest evaluation must pass the verification. This allows us to locally change the program code at time step \( t \), so that the pebble can be moved forward or backward along the computation path. Very interestingly, although the computation path is long, moving a pebble corresponds to hardwiring only \( O(1) \) information in the hybrids, independent to the time bound \( T \). In
Section B.1, the security proof of CiO for RAM has shown how to replace program \( P_0 \) to \( P_1 \) gradually in this way.

However, in the PRAM setting, the computation trace becomes a directed layered graph with width \( m \), where each layer corresponds to a time step and
- each node is indexed by a time \( t \) and a CPU id \( i \),
- there is a directed edge \((u, v)\) if node \( u \) outputs either a CPU state or a communication message as input to node \( v \).

Note that an edge only exists between the nodes in neighboring layers, which means that an edge denotes some dependency between the two nodes in the actual computation. In particular, nodes \( u \) and \( v \) can be either the same CPU depends on its previous state or different CPUs such that \( v \) receives a message from \( u \). \(^{31}\)

Suppose that we generalize the proof techniques of KLW to this setting in a straightforward manner, which is analogous to putting and moving check points along the graph. By moving check points, we have the check condition to check the output \( m^{\text{out}}_u \) of a computation step \( u \) against the hardwired value \( m^u \). The general pebble game rules bring a constraint that we can only put one pebble on a node \( v \) if, for every \( u \) such that \((u, v) \in E\), the pebbles are put on all nodes \( u \), which is analogous to adding another hardwired value \( m^v \) must depends on all its input. As such, we can only remove a check point after we have put check points on all its outgoing neighbors, which is analogous to the hybrid removing the hardwired signing key and CPU output state \( m^u \). In general, placing (or removing) a pebble on node \( u \) is analogous to hardwiring (or un-hardwiring) the output of computation step \( u \) in a intermediate hybrid program. Let the security proof correspond to the pebble game. Our goal of the security proof is to traverse all computation steps and to locally change the program with minimizing the total number of hardwired values for any intermediate hybrid. Accordingly, in the corresponding pebble game abstraction, the goal is to traverse the whole graph with minimizing the total number of pebbles (a.k.a. pebble complexity) on the graph.

Using this pebble game, the graph of \( \text{OUpdate} \) is partially depicted in Figure 2. To win this pebble game, the straightforward solution is to put \( m \) pebbles on all \( m \) CPUs of the first column, and then placing pebbles to the next column while removing from the first greedily whenever possible. We can remove all pebbles on the first column when its next is filled with pebbles, since any column only depends on its previous one. The pebble complexity is at most \( 2m \). Unfortunately, we have not found a solution yet to winning this pebble game with pebble complexity less than the number of CPUs \( m \). The straightforward solution implies an inefficient CiO scheme with encoding of size \( \Omega(m) \). However, we provide a generic transformation that converts any PRAM program with oblivious communication to a special class of PRAM program with \( \log m \) pebble complexity (with \( \log m \) parallel time overhead in addition). Such transformation allows us to construct efficient CiO for PRAM programs.

**Branch and Combine Transformation** Here we very briefly describe the transformation. It is motivated by the observation that a hardwired value (and thus a pebble) is corresponding to the signature signing and verifying a CPU state or communication, and in a sense we can replace such verification with an additional accumulation structure. Furthermore, computing the digest of the CPU accumulator is much simpler than that of memory accumulator, since each CPU computes directly with its fixed neighbor without additional communication. We divide it into two stages: branch and combine.

At the beginning, all \( m \) input CPU states and messages are stored in a random access buffer \( \text{buff} \), and then the evaluator is required to provide each state \( s_t \) and message \( m_i \) with a proof \( \pi_i \) to each CPU. All CPUs receive as input the same signed accumulator digest \( w_{\text{buff}} \) of the \( \text{buff} \), their corresponding states and messages with proofs. Each CPU then verifies accumulator digest with signature, verifies state and message.

\(^{31}\) We assume here we have the protocol to update the memory accumulator digest (Section 7.4) in the parallel setting. Although memory accesses lead to dependencies between two steps, they are verified by memory accumulators, and thus are not hardwired in hybrid programs. Therefore we do not consider memory accesses in this pebble game.
with accumulator digest and proof, computes its output state and message, and sign the output with signature scheme. In this branch stage, these procedures have one signature as input but \( m \) different signatures as output.

Now the evaluator has \( m \) new signed states and messages, but CPU steps at the next branch stage require a new signed accumulator digest \( w'_{\text{buff}} \). Our next goal is to design a series of CPU steps to compute such digest and its signature, which should be verifiable at the next stage by CPUs but unforgeable for the evaluator. Intuitively, we construct a CPU program follows the Merkle-tree-like structure, which takes a pair of signed inputs and output one signed output in each step (Figure 1). From a leaf to the root, the program indeed computes the whole tree structure of \( \text{buff}' \) including the tree root, which is exactly the accumulator digest \( w'_{\text{buff}} \), and each step has output signed with signature. Now we have this new signed accumulator digest, and the evaluator can start the next branch stage iteratively. In this combine stage, there are \( m \) leaf signatures at the beginning but only one root signature as final output.

To analyze our branch and combine technique, we observe those states and communications in the original program are transformed into \( \text{buff} \), and dependencies are simple. In the pebble game abstraction, it is easy to traverse from a root in a combine stage to the next root via post order, where its pebble complexity is \( \log m \). Specifically, our strategy is to merge two sibling pebbles to their parent node as soon as possible. There is an invariant that each layer in the binary tree has at most 2 pebbles. Multiplying \( \log m \) overhead of branch and combine transformation with \( \log m \) pebble complexity, the overall overhead is \( O(\log^2 m) \) in parallel time. As a result, it significantly improves the naive solution. Also note that the evaluation of branch and combine program is parallel, but the pebble game (and thus the series of hybrids) is sequential because it is not possible to traverse \( Tm \) nodes with only \( \log m \) pebbles in \( T \) moves. We will describe branch-and-combine construction in Section 7.5, and then prove its security in Section B.3 for more details.

### 7.2 Building Blocks

In our Ci\(\hat{O}\) construction in Section 7.5, we will use several building blocks: accumulator, topological iterator, splittable signature, puncturable PRF, and indistinguishability obfuscation. Topological iterator is a new building block and we will investigate it in detail in next subsection. The formal definitions for other building blocks can be found in Section A. We next define the parameters for the building blocks we will use in our Ci\(\hat{O}\) construction.

- Accumulator scheme \( \text{Acc} = \text{Acc.}\{\text{Setup, SetupEnforceRead, SetupEnforceWrite, PrepRead, PrepWrite, VerifyRead, WriteStore, Update}\} \) with message space \( \{0, 1\}^{\ell_{\text{msg}}} \) and accumulated value space \( \{0, 1\}^{\ell_{\text{acc}}} \).
- Topological Iterator scheme $TiTr = TiTr.\{\text{Setup, SetupEnforceIterate, Iterate}\}$ with message space \(\{0, 1\}^{\ell_{\text{Acc}} + \ell_{\text{msg}}}\) and iterated value space \(\{0, 1\}^{\ell_{\text{itr}}}\) bits. (Section 7.3)
- Splittable signature scheme $Spl = Spl.\{\text{Setup, Sign, Verify, Split, AboSign}\}$ with message space \(\{0, 1\}^{\ell_{\text{itr}} + \ell_{\text{Acc}} + \ell_{\text{msg}}}\), we will assume $Spl.\text{Setup}$ uses $\ell_{\text{rand}}$ bits of randomness.
- Puncturable PRF scheme $PPRF = PPRF.\{\text{Setup, Puncture, Eval}\}$ with key space $K$, punctured key space $K_{\text{punct}}$, domain \([T]\), and range \(\{0, 1\}^{\ell_{\text{rand}}}\).
- Indistinguishability obfuscation scheme $\text{iO}$.
- Parallel Accumulator scheme. (Section 7.4)

### 7.3 Topological Iterators

In this section, we will define a primitive named *Topological Iterators* based on the original KLW Iterator (Section A.3.1). We will demonstrate a construction for this new primitive by using $\mathcal{PKE}$, puncturable PRF and $\text{iO}$, and then prove its security. The main difference between our Topological Iterators and KLW Iterator is that, we allow iterating two states, instead of one, into a new state.

**Syntax.** Let poly be any polynomial. An iterator $TiTr$ with message space $\mathcal{M}_\lambda = \{0, 1\}^{\text{poly}(\lambda)}$ and state space $\mathcal{S}_\lambda$ consists of three algorithms - $TiTr.\text{Setup}$, $TiTr.\text{SetupEnf}$, $TiTr.\text{Iterate}$, and $TiTr.\text{Iterate2to1}$ defined below.

- $TiTr.\text{Setup}(1^\lambda, N)$: The setup algorithm takes as input the security parameter $\lambda$ (in unary), and an integer bound $N$ (in binary) on the number of iterations. It outputs public parameters $pp_{\text{itr}}$ and an initial state $v \in \mathcal{S}_\lambda$.

- $TiTr.\text{SetupEnf}(1^\lambda, N, \text{DAG})$: The enforced setup algorithm takes as input the security parameter $\lambda$ (in unary), an integer bound $T$ (in binary) and messages in $\text{DAG}$, which has following properties:
  1. $\text{DAG} = (N, E, \text{source}, \text{sink})$ is a directed acyclic graph with $|N| < N$, and
  2. Single “source” node and single “sink” node, and
  3. Each node (expect source) has in-degree 1 or 2, and
  4. Each node $n$ has a unique message value $m_n \in \mathcal{M}_\lambda$. This property is important in the security of enforcing.

It outputs public parameters $pp_{\text{itr}}$ and an initial state $v \in \mathcal{S}_\lambda$.

- $TiTr.\text{Iterate}(pp_{\text{itr}}, v, m)$: The iterate algorithm takes as input the public parameters $pp_{\text{itr}}$, a state $v$, and a message $m \in \mathcal{M}_\lambda$. It outputs a state $v_{\text{out}} \in \mathcal{S}_\lambda$.

- $TiTr.\text{Iterate2to1}(pp_{\text{itr}}, v_l, v_r, m)$: The iterate algorithm takes as input the public parameters $pp_{\text{itr}}$, two states $(v_l, v_r)$, and a unique message $m \in \mathcal{M}_\lambda$. It outputs a state $v_{\text{out}} \in \mathcal{S}_\lambda$.

**Security.** Let $TiTr = TiTr.\{\text{Setup, SetupEnforceIterate, Iterate, Iterate2to1}\}$ be an iterator with message space $\mathcal{M}_\lambda$ and state space $\mathcal{S}_\lambda$. We require the following notions of security.

**Definition 7.1** (Indistinguishability of Setup). An iterator $TiTr$ is said to satisfy indistinguishability of Setup phase if any PPT adversary $A$’s advantage in the security game $\text{Exp-Setup-Itr}(1^\lambda, TiTr, A)$ is at most negligible in $\lambda$, where $\text{Exp-Setup-Itr}$ is defined as follows.

$\text{Exp-Setup-Itr}(1^\lambda, TiTr, A)$

- The adversary $A$ chooses a bound $N \in \Theta(2^\lambda)$ and sends it to challenger.
- $A$ sends $\text{DAG} = (N, E, \text{source}, \text{sink})$ to the challenger.
- The challenger chooses a bit $b$. If $b = 0$, the challenger outputs $(pp_{\text{itr}}, v) \leftarrow TiTr.\text{Setup}(1^\lambda, N)$. Else, it outputs $(pp_{\text{itr}}, v) \leftarrow TiTr.\text{SetupEnf}(1^\lambda, N, \text{DAG})$. 

34
A sends a bit $b'$.

A wins the security game if $b = b'$.

**Definition 7.2 (Enforcing).** Consider any $\lambda \in \mathbb{N}, N \in \Theta(2^\lambda)$, $\text{DAG} = (\mathcal{N}, \mathcal{E}, \text{source}, \text{sink})$. Let $(\text{pp}_\text{ltr}, v) \leftarrow \text{Tltr.Setup}\text{Enf}(1^\lambda, N, \text{DAG})$ and $v_n = \text{Tltr.Iterate2to1}(\text{pp}_\text{ltr}, v(l(n), v(r(n), m_n))$ for all $n \in \mathcal{N} \setminus \{\text{source}\}$.

Then, $\text{Tltr} = (\text{Tltr.Setup}, \text{Tltr.SetupEnf}, \text{Tltr.Iterate2to1})$ is said to be enforcing if

$$v_{\text{sink}} = \text{Tltr.Iterate2to1}(\text{pp}_\text{ltr}, v_l, v_r, m) \Rightarrow (v_l, v_r, m) = (v_{l, \text{sink}}, v_{r, \text{sink}}, m_{\text{sink}})$$

Note that this is an information-theoretic property.

### 7.3.1 Construction

- $\text{Tltr.Setup}(1^\lambda, T)$: The setup algorithm chooses $(PK, SK) \leftarrow \mathcal{PK}\mathcal{E}.\text{Gen}(1^\lambda)$ and puncturable PRF key $K \leftarrow \text{PRF}\cdot\text{Setup}(1^\lambda)$. It sets $\text{pp}_\text{ltr} \leftarrow i\mathcal{O}(\text{prog}\{K, PK\})$, where prog is defined in Algorithm 3. Let $ct \leftarrow \mathcal{PK}\mathcal{E}.\text{Encrypt}(PK, 0)$. The initial state $v = ct$. It outputs $(\text{pp}_\text{ltr}, v)$.

**Algorithm 3: prog\text{Enf}**

<table>
<thead>
<tr>
<th>Line</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td><strong>Input</strong>: $v_l, v_r, m \in \mathcal{M}_\lambda$</td>
</tr>
<tr>
<td>1</td>
<td><strong>Data</strong>: Puncturable PRF key $K$, $\mathcal{PK}\mathcal{E}$ public key $PK$</td>
</tr>
<tr>
<td>2</td>
<td>Compute $r \leftarrow \text{PRF}(K, (v_l, v_r, m))$;</td>
</tr>
<tr>
<td>3</td>
<td>Let $ct \leftarrow \mathcal{PK}\mathcal{E}.\text{Encrypt}(PK, 0; r)$;</td>
</tr>
<tr>
<td>4</td>
<td>Output $v_{\text{out}} = ct$;</td>
</tr>
</tbody>
</table>

- $\text{Tltr.SetupEnf}(1^\lambda, T, \text{DAG})$: The setup algorithm chooses $(PK, SK) \leftarrow \mathcal{PK}\mathcal{E}.\text{Gen}(1^\lambda)$ and puncturable PRF key $K \leftarrow \text{PRF}\cdot\text{Setup}(1^\lambda)$. Let $\text{DAG} = (\mathcal{N}, \mathcal{E}, \text{source}, \text{sink})$. $\forall n \in \mathcal{N}$, compute $v_n$ by following steps.

  1. $\forall n \in \mathcal{N}$, $v_n \leftarrow \bot$.
  2. The initial state $v_{\text{source}} = \mathcal{PK}\mathcal{E}.\text{Encrypt}(PK, 0)$.
  3. $\forall n \in \mathcal{N}$ such that has definite in-edge, compute $v_n$. That is,

     $$\forall n \in \mathcal{N}, (v_n = \bot) \land (\exists (l, n), (r, n) \in \mathcal{E}) \land (v_l \neq \bot) \land (v_r \neq \bot)$$

     $$r_n \leftarrow \text{PRF}(K, (v_l, v_r, m_n))$$

     and $v_n \leftarrow \mathcal{PK}\mathcal{E}.\text{Encrypt}(PK, 0; r_n)$.

  4. Repeat previous step until $\forall n \in \mathcal{N}, v_n \neq \bot$.

Let $(l_{\text{sink}}, \text{sink}), (r_{\text{sink}}, \text{sink}) \in \mathcal{E}$ be the two edges that direct to sink. It computes a punctured key $K' \leftarrow \text{PRF} \cdot \text{Puncture}(K, (v_{l, \text{sink}}, v_{r, \text{sink}}, m_{\text{sink}}))$, chooses $r \leftarrow \{0, 1\}^\lambda$ and sets $ct_{\text{sink}} = \mathcal{PK}\mathcal{E}.\text{Encrypt}(PK, 1; r)$. Finally, it computes the public parameters $pp_{\text{ltr}} \leftarrow i\mathcal{O}(\text{prog}\text{Enf}\{\text{sink}, (v_{l, \text{sink}}, v_{r, \text{sink}}, m_{\text{sink}}), ct_{\text{sink}}, K', PK\})$, where prog\text{Enf} is defined in Algorithm 4. It outputs $(pp_{\text{ltr}}, v_{\text{source}})$.

**Algorithm 4: prog\text{Enf}**

<table>
<thead>
<tr>
<th>Line</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td><strong>Input</strong>: $v_l, v_r, m \in \mathcal{M}_\lambda$</td>
</tr>
<tr>
<td>1</td>
<td><strong>Data</strong>: sink, states $m_{\text{sink}}, ct_{\text{sink}}$, Puncturable PRF key $K'$, $\mathcal{PK}\mathcal{E}$ public key $PK$</td>
</tr>
<tr>
<td>2</td>
<td>if $(v_l, v_r, m) = (v_{l, \text{sink}}, v_{r, \text{sink}}, m_{\text{sink}})$ then</td>
</tr>
<tr>
<td>3</td>
<td>Output $ct_{\text{sink}}$;</td>
</tr>
<tr>
<td>4</td>
<td>Compute $r \leftarrow \text{PRF}(K, (v_l, v_r, m))$;</td>
</tr>
<tr>
<td>5</td>
<td>Let $ct \leftarrow \mathcal{PK}\mathcal{E}.\text{Encrypt}(PK, 0; r)$;</td>
</tr>
<tr>
<td>6</td>
<td>Output $v_{\text{out}} = ct$;</td>
</tr>
</tbody>
</table>

- $\text{Tltr.Iterate}(pp_{\text{ltr}}, v, m)$: simply outputs $pp_{\text{ltr}}(v, \bot, m)$.
- $\text{Tltr.Iterate2to1}(pp_{\text{ltr}}, v_l, v_r, m)$: simply outputs $pp_{\text{ltr}}(v_l, v_r, m)$.
7.3.2 Security

We show that the construction described in Section 7.3.1 satisfies Indistinguishability of Setup (Definition 7.1) and Enforcing (Definition 7.2).

**Lemma 7.3** (Indistinguishability of Setup). Assuming \( iO \) is a secure indistinguishable obfuscator, PRF is a selectively secure puncturable PRF, and \( \mathcal{PKE} \) is a semantically-secure public key encryption scheme, any PPT adversary \( A \) has only negligible advantage in the Exp-Setup-Itr game.

The proof can be found in Section B.2.

**Lemma 7.4** (Enforcing). Assuming \( \mathcal{PKE} \) is a perfectly correct public key encryption scheme, then \( \mathcal{Tltr} = (\mathcal{Tltr.Setup, Tltr.SetupEnf, Tltr.Itrate, Tltr.Itrate2to1}) \) is enforcing.

**Proof.** This follows directly from the correctness of \( \mathcal{PKE} \) because the sink node has \( v_{\text{sink}} \) be an encryption of 1 but all other nodes are encryption of 0.

7.4 Parallel Accumulator

Consider the (standard) PRAM model in which \( m \) CPUs have random access to a shared memory at \( m \) locations at each time step. An intuitive approach is to extend the construction of \( CiO \) for RAM into the PRAM model, where each bit read by each CPU is verified against the accumulator value (a.k.a. digest) \( w \). The verification is straightforward and can be run in parallel. The problem, however, is that the digest \( w \) must be correctly verified after each bit written by each CPU (in order to verify the next bit to be read). Therefore, as long as \( m \) writes the new digest \( w \) depends on all \( m \) newly written bits, which may take roughly \( m \) (total) steps to update \( w \). The trivial solution which sequentially update \( w \) with each \( m \) bits obviously introduces an unacceptable \( O(m) \) multiplicative parallel time overhead. To retain the benefits of using \( m \) CPUs, we must design a clever update mechanism with \( O(\log m) \) overhead at most.

Recall that by our assumption the \( m \) CPUs read and write synchronously and alternatively. Consider a time step when \( m \) synchronized writes occur. Our goal here is to let each CPU, with their own bits to be written, exchange information with each others and concurrently compute the same digest \( w \). Ignoring the steps where the bits are actually written to the memory, the procedures for computing the digest alone form a memory-less PRAM computation, which can be obfuscated using techniques in the construction of \( CiO \) for memory-less PRAM.

To argue the security of this approach, we observe that the whole accumulator tree structure is accessible to the malicious evaluator/adversary, and thus it is not necessary to hide any intermediates while updating. In fact, the CPUs compute and communicate with their sequences forming a binary tree bottom-up, and leak a partially updated memory to the decoder at each level of the tree. However, any partially updated memory does not give the adversarial decoder additional information because it can always compute these values from the previous memory contents and the newly written bits. For correctness, as long as the CPU states and messages are authenticated by \( CiO \), any adversary is not able to forge a malicious message or digest, and hence the CPUs will eventually agree on the same digest \( w \) correctly.

The construction of \( CiO \) for memory-less PRAM requires the communication pattern between CPUs to be oblivious, which means the receiver of each communication is uniquely determined by the iteration counter \( t \) and the sender CPU id. In the following Section 7.4.1, we recall the oblivious aggregation and oblivious multicasting protocols from [BCP14b] to build oblivious communication between the CPUs. We then use these protocols to construct the mechanism for computing the digest \( w \) in Section 7.4.2.

### 7.4.1 Oblivious Aggregation and Multicasting

To simplify the “updating” algorithm, we apply two PRAM primitives, namely oblivious aggregation and oblivious multicasting, which are introduced in [BCP14b] and described below for completeness. Both primitive are
deterministic PRAM algorithms that run with only CPU states and oblivious communication. By oblivious communication, we say that the source and destination of all messages are specified by algorithm but not depended on the input. The functionality and complexity are specified in the following definitions.

**Oblivious Aggregation.** OblivAgg is a procedure satisfying the following aggregation goal with communication patterns independent of the input, using only $O(poly\log(m))$ local memory and communication per CPU, in only $O(poly\log(m))$ sequential time steps.

**Input:** Each CPU $i \in [m]$ holds $(key_i, data_i)$. Let $\mathcal{K} = \bigcup\{key_i\}$ denote the set of distinct keys. We assume that any (subset of) data associated with the same key can be aggregated by an aggregation function $Agg$ to a short digest of size at most $poly(|data_i|, \log m)$.

**Goal:** Each CPU $i$ outputs $out_i$ such that the following holds.

- for every key $\in \mathcal{K}$, there exists unique agent $i$ with key $i = key$ such that $out_i = (rep, key, agg_{key})$, where $agg_{key} = Agg\{data_j : key_j = key\}$.
- for every remaining agent $i$, $out_i = (\text{dummy}, \bot, \bot)$.

**Oblivious Multicasting.** OblivMCast is a procedure satisfying the following multicasting goal with communication patterns independent of the inputs, using only $O(poly\log(m))$ local memory and communication per CPU, in only $O(poly\log(m))$ sequential time steps. Namely, a subset of CPUs must deliver information to (unknown) collections of other CPUs who request it. This is abstractly modelled as follows, where key $i$ denotes which data item is requested by each CPU $i$.

**Input:** Each CPU $i$ holds $(key_i, data_i)$ with the following promise. Let $\mathcal{K} = \bigcup\{key_i\}$ denote the set of distinct keys. For every key $\in \mathcal{K}$, there exists a unique agent $i$ with key $i = key$ such that $data_i \neq \bot$; let $data_{key}$ denote such $data_i$.

**Goal:** Each agent $i$ outputs $out_i = (key_i, data_{key_i})$.

### 7.4.2 OUpdate Algorithm

In the following, we construct a distributed Acc.OUpdate algorithm (Algorithm 5) to be run with $m$ CPUs. Each CPU $i$ takes $i$, loc$_i$, $b_i$, $\pi_i$ as input, communicates with other CPUs obliviously using OblivAgg and OblivMCast defined above, and outputs the same digest $w$ of the whole updated memory, where for CPU $i$

- loc$_i$, $b_i$ are the writing location and value, and
- $\pi_i$ is the authentication path (proof) of the writing location loc$_i$.

Acc.OUpdate introduces a multiplicative $O(\log S)$ parallel time overhead in the worst case where all CPUs write $m$ different values at distinct locations of the memory with size $S$ in parallel. Acc.OUpdate traverses each authentication path $\pi_i$ in a bottom-up approach. For each node in $\pi_i$, it checks if another CPU possesses a fresh sibling node by the OblivAgg protocol, which exchanges information between all CPUs and yields a pair of fresh nodes ($m_l, n_r$) that may depends on one or more CPUs, to the representative CPU (Algorithm 6). All CPUs then share the pair of fresh nodes by OblivMCast from those representative CPUs, and each CPU computes the updated parent node of the updated pair directly by the public parameter pp$_{Acc}$. With the updated parent node, the procedure is able to continue with the next node in $\pi_i$ iteratively. The procedure is finished when the root node of $\pi_i$ is updated.

Some additional notations used in Acc.OUpdate is listed in Table 2.
Algorithm 5: Acc.OUpdate

Input : $i, \text{loc}, b, \pi$
Output: $w$
Data: $\text{pp}_{\text{Acc}, \text{mem}}$
1 Parse $\pi = (\text{root}, (n_l, n_r)_0, \ldots, (n_l, n_r)_{\text{MemAccDepth} - 1})$;
2 Let the leaf node $\pi[\text{MemAccDepth} - 1][\text{loc}[\text{MemAccDepth} - 1]] \leftarrow b$;
3 for $(\text{MemAccDepth} > z \geq 0)$ do
4   key$_i$ $\leftarrow$ loc$_{z-1}$;
5   (rep, key$_i$, aggdata) $\leftarrow$ Run OblivAgg with input $(i, \text{key}_i, (\text{loc}[z], \pi[z][0], \pi[z][1]))$ and aggregation function Agg;
6   (flag, n$_l$, n$_r$) $\leftarrow$ Run OblivMCast with input $(\text{key}_i, \text{aggdata})$;
7   $\pi[z-1][\text{loc}[z-1]]$ $\leftarrow$ Acc.Combine($\text{pp}_{\text{Acc}, \text{mem}}, n_l, n_r, \text{loc}_{z-1}$);
8 return root;

Algorithm 6: Agg

Input : datatemp$_1$, datatemp$_2$
Output: aggdata
1 if datatemp$_1$ has the form $(\text{Done}, n_l, n_r)$ then
2   // If any data has already done, return it.
3   return datatemp$_1$;
4 if datatemp$_2$ has the form $(\text{Done}, n_l, n_r)$ then
5   return datatemp$_2$;
6 if datatemp$_1$ = datatemp$_2$ has the form $(\text{loc}[z], n_l, n_r)$ then
7   // If both data is identical, keep any one.
8   return datatemp$_1$;
9 if datatemp$_1$ has the form $(\text{loc}[z]_1, n_l, n_r)$ and datatemp$_2$ has the form $(\text{loc}[z]_2, n_l, n_r)$ then
10  // If two data differs, merge by their freshness and mark as done.
11     if $(\text{loc}[z]_1 > \text{loc}[z]_2)$ then
12       Swap $(\text{loc}[z]_1, n_l, n_r)$, $(\text{loc}[z]_2, n_l, n_r)$;
13     return $(\text{Done}, n_l, n_r)$;
We can use $F_{\text{Update}}$ (Algorithm 5).

As a warm-up, we construct $C_i$ implicitly by $O_{\text{Update}}$.

These stages are controlled by the simple counter $d$ where $F$ always reads at even rounds and writes at odd rounds, and thus $\Pi_{\text{check}}$ has a straightforward construction: repeatedly invokes (i) step function $F$ one reading round, (ii) step function $F$ one writing round, (iii) step function $F_{\text{Update}}$ a fixed number $D_{\text{Acc}}$ of rounds. Specifically,

$$
\Pi_{\text{check}} = \left( (\text{mem}^0, \{s^0_k, a^0_{k-\lambda}, a^0_{\lambda-1} \}_{k=1}^m), F_{\text{check}} \right),
$$

where $F_{\text{check}}$ is defined in Algorithm 7, $s^0$ and $a^0$ are defined by augmenting the corresponding $s$ and $a$ from $\Pi$. We can use $F_{\text{check}} = \text{AccCompile}(F, \text{Acc.OUpdate}\{pp_{\text{Acc,mem}}\})$ to specify the compilation.

$F_{\text{check}}$ has three major stages, which is READ, WRITE, and OUpdate.

- In a READ state, it has no memory input and just invokes $F$, which issues a READ command.
- In a WRITE state, the previous state must be READ. Therefore, $F_{\text{check}}$ verifies the value read from memory and invokes $F$, which issues a WRITE command.
- In OUpdate states, $F_{\text{check}}$ first verifies the proof $\pi_{\text{in}}$ against old accumulator digest. Then, it initializes $F_{\text{Update}}$ with the correct proof $\pi_{\text{in}}$ and runs $F_{\text{Update}}$ stepwise to obtain the new accumulator digest.

These stages are controlled by the simple counter $d_{\text{Acc}}$ and the fixed running time $D_{\text{Acc}}$, which is defined implicitly by OUpdate.

### 7.5 Warm-up: Construction for CiO-PRAM$^-$

As a warm-up, we construct CiO in the memoryless PRAM (PRAM$^-$) model. Recall in Section A.1.3 that the PRAM$^-$ model is similar to the PRAM model except that it has no external memory, but oblivious communication between pairs of CPUs is allowed. Formally, the class of distributed computation for PRAM$^-$, denoted by $\mathcal{P}_{\text{PRAM}}^-$, is defined as follows:

**Definition 7.5 (PRAM$^-$ Computation Class).** $\mathcal{P}_{\text{PRAM}}^-$ is a class of distributed computation for PRAM$^-$ with $m$ agents without external memory where

---

**Table 2: Additional notations for the OUpdate protocol.** We omit subscription $i$ and use loc, $b$ and $\pi$ in OUpdate (Algorithm 5).

<table>
<thead>
<tr>
<th>Notations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$z$</td>
<td>The depth of node to be update in $\pi$</td>
</tr>
<tr>
<td>$\text{loc}_x$</td>
<td>The $x$ bit prefix of loc</td>
</tr>
<tr>
<td>$\text{loc}[x]$</td>
<td>The $x$-th bit of loc such that $\text{loc}[-1] := \epsilon$</td>
</tr>
<tr>
<td>$\text{loc}[x] = 0$ (for $x = 1$)</td>
<td>Implies that the left (right) node should be updated</td>
</tr>
<tr>
<td>$\pi[x]$</td>
<td>The pair of nodes $(n_l, n_r)_x$ at depth $x$ such that $\pi[-1] := \text{root}$</td>
</tr>
<tr>
<td>$\pi[x][0]$ ($\pi[x][1]$)</td>
<td>The left node $n_l$ (right node $n_r$) in the pair $(n_l, n_r)_x$ such that $\pi[-1][\epsilon] := \text{root}$</td>
</tr>
<tr>
<td>flag = Done</td>
<td>Implies that both node $(n_l, n_r)$ is fresh in aggdata</td>
</tr>
</tbody>
</table>

---
Algorithm 7: $F_{\text{check}}$

Input: $id, \overline{st}^{in}, \overline{\alpha}^{in} = (\overline{t}^{in}, \overline{com}^{in}, \overline{\pi}^{in})$

Data: $D_{\overline{Acc}}$

1. Parse $\overline{st}^{in}$ as $((\overline{st}^{in}_{II}, \overline{st}^{in}_{\overline{Acc}}), d_{\overline{Acc}}, b, w, \text{loc})$;
2. if ($d_{\overline{Acc}} = \text{Read}$ or $d_{\overline{Acc}} = \text{Write}$) then
   3. ($\overline{st}^{out}_{\overline{Acc}}, \overline{com}^{out}$) ← $\langle \bot, \bot \rangle$;
   4. if $d_{\overline{Acc}} = \text{Read}$ then
      5. Compute $\overline{st}^{out}_{II} = ((\overline{st}^{out}_{II}, \overline{st}^{out}_{\overline{Acc}}), \text{Write}, b^{out}, w, \text{loc}^{out}));$
      6. If $\overline{st}^{out}_{II} = \text{Reject}$, then output $\text{Reject}$;
      7. Set $\overline{st}^{out} = ((\overline{st}^{out}_{II}, \overline{st}^{out}_{\overline{Acc}}), \text{Write}, b^{out}, w, \text{loc}^{out}));$
     else
        8. if $d_{\overline{Acc}} = \text{Write}$ then
           9. If $\overline{Acc}.\text{VerifyRead}(pp_{\overline{Acc}, \text{mem}}, w, (\text{loc}, b^{in}), \pi^{in}) = 0$ output $\text{Reject}$;
          10. Compute $\overline{st}^{out}_{II} = ((\overline{st}^{out}_{II}, \overline{st}^{out}_{\overline{Acc}}), \text{Write}, b^{out}, w, \text{loc}^{out}));$
          11. If $\overline{st}^{out}_{II} = \text{Reject}$, then output $\text{Reject}$;
          12. Set $\overline{st}^{out} = ((\overline{st}^{out}_{II}, \overline{st}^{out}_{\overline{Acc}}), \text{Write}, b^{out}, w, \text{loc}^{out}));$
     else
        13. ($\overline{st}^{out}_{\overline{Acc}}, \overline{com}^{out}$) ← $F_{\text{OUpdate}}(id, \overline{st}^{in}_{\overline{Acc}}, \overline{com}^{in});$
           // Execute $F_{\text{OUpdate}}$ iteratively
        14. $d_{\overline{Acc}} ← d_{\overline{Acc}} + 1$;
        15. if $d_{\overline{Acc}} = D_{\overline{Acc}}$ then
           16. Parse $\overline{st}^{out}_{\overline{Acc}}$ to obtain new accumulator digest $w^{out}$;
           17. $d_{\overline{Acc}} ← \text{Read}$;
        else
           18. Let $w^{out} = w$;
        19. Set $\overline{st}^{out} ← ((\overline{st}^{in}_{II}, \overline{st}^{out}_{\overline{Acc}}), d_{\overline{Acc}}, \bot, w^{out}, \bot)$;
        20. Set $\overline{\alpha}^{out} ← (\overline{com}^{out}, (\bot, \bot))$;
    return $\overline{st}^{out}, \overline{\alpha}^{out}$;
- the terminating time \( t^* \) is bounded by \( 2^\lambda \),
- the communication between agents are restricted in the sense that in each round \( t \), each agent \( k \) is only allowed to receive a single message \( c^t_k \) from agent \( \text{src}(t,k) \) where \( \text{src} \) is a public function, and the agent \( k \) is allowed to at most send one message to other agent,
- for all \( k \in [m] \), the state size \( |st_k| \) is bounded by \( \text{poly} \log(\lambda) \),
- for all \( k \in [m] \), the access commands are restricted to \( a^t_{k-\text{tr}} := \bot \) and \( a^t_{k-\text{m}} := \bot \),
- for all \( k \in [m] \), the initial communication messages are restricted to \( c^0_k := \bot \).

### Table 3: Additional notations for \( CiO \) in PRAM\(^{-} \) model

<table>
<thead>
<tr>
<th>Notations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>( m )</td>
<td>The total number of CPUs in a PRAM program</td>
</tr>
<tr>
<td>node</td>
<td>A node contains ((t, \text{index}, w_{\text{st}}, w_{\text{com}}, v, \sigma))</td>
</tr>
<tr>
<td>src((\cdot, \cdot))</td>
<td>A function decides an oblivious communication (e.g., at time ( t ), ( id_{\text{cpu}}(b) ) sends to ( id_{\text{cpu}}(a) ), then ( \text{src}(t, id_{\text{cpu}}(a)) \rightarrow id_{\text{cpu}}(b) ))</td>
</tr>
<tr>
<td>max-cpu((\cdot))</td>
<td>A mapping function, defined on ( \text{index} ), outputs a leaf node: If ( \text{index} ) is a leaf, ( \text{max-cpu}(\text{index}) = \text{index} ). If not, outputs the maximum leaf index from ( \text{index} )'s descendants.</td>
</tr>
<tr>
<td>min-cpu((\cdot))</td>
<td>A mapping function, defined on ( \text{index} ), outputs a leaf node: If ( \text{index} ) is a leaf, ( \text{min-cpu}(\text{index}) = \text{index} ). If not, outputs the minimum leaf index from ( \text{index} )'s descendants:</td>
</tr>
<tr>
<td>( C_{i,j} )</td>
<td>A set of indices of internal nodes defined by an index ( j ) for ( t = i ). (For all ( \text{index} \in C_{i,j}, \text{index} &lt; j ) and ( \text{index} )'s parent ( \notin C_{i,j} ))</td>
</tr>
<tr>
<td>( M_{i,j} )</td>
<td>A set of hardwired output messages corresponding to indices of ( C_{i,j} )</td>
</tr>
</tbody>
</table>

We now describe our scheme \( CiO = CiO.\{\text{Obf}, \text{Eval}\} \) in the PRAM\(^{-} \) model. For readability, we first introduce additional notations in Table 3. Our construction of \( CiO \) for PRAM\(^{-} \) follows the structure of the construction of \( CiO \) for RAM, except for the following differences. First, since there is no memory access in the PRAM\(^{-} \) model, no accumulator is needed for storing the memory content. However, we do need two new accumulators to store the states and messages, as we wish to compress \( m \) states and messages into their corresponding digests respectively. In order to compute these digests, the next step function \( \tilde{F} \) of the obfuscated program is split into the branch stage and the combine stage. The branch stage is essentially the first half of \( \tilde{F} \) in the construction of \( CiO \) for RAM, where the function verifies its inputs and performs the actual computation. The steps for computing the digests are deferred to the combine stage, where the \( m \) CPUs collaboratively updates the digests for their states and messages.

The compilation procedure \( CiO.\text{Obf} \) can transform a given computation system \( \Pi \) in the memoryless PRAM model, i.e., \( \Pi \in \mathcal{P}_{\text{PRAM}^{-}} \), into an obfuscated computation system \( \Pi\). Here

\[
\Pi = (\{st^0_k\}_{k=1}^m, F)
\]

\[
\Pi = ((\text{mem}^0, \{st^0_k\}_{k=1}^m), \tilde{F})
\]

We note that in \( \Pi \in \mathcal{P}_{\text{PRAM}^{-}} \), the variables \( \text{mem}, a_{k-\text{tr}}, a_{k-\text{m}} \) are not defined.

**Compilation procedure** \( \Pi \leftarrow CiO.\text{Obf}(1^\lambda, \Pi) \): The compilation procedure \( \text{Obf}() \) consists of several steps.
Step 1: Generating parameters. A set of parameters will be generated:

\[ K_A \leftarrow \text{PRF.Setup}(1^k), \]
\[ (pp_{\text{Acc},st}, \hat{w}_{\text{st},0}, \hat{store}_{\text{st},0}) \leftarrow \text{Acc.Setup}(m), \]
\[ (pp_{\text{Acc,com}}, \hat{w}_{\text{com},0}, \hat{store}_{\text{com},0}) \leftarrow \text{Acc.Setup}(m), \]
\[ (pp_{\text{itr}}, v^0) \leftarrow \text{Tltr.Setup}(T). \]

Step 2: Generating stateful algorithms \( \hat{F} \). Based on the parameters \( T, pp_{\text{Acc},st}, pp_{\text{Acc,com}}, pp_{\text{itr}}, K_A \) generated above, as well as program \( F \), we define the program \( \hat{F} \) in Algorithm 8. Here \( \hat{F} \) executes internal programs \( F_{\text{branch}} \) (Algorithm 9), which in turn executes \( F \), or \( F_{\text{combine}} \) (Algorithm 10) depending on its input. Similar to the program \( \hat{F} \) (Algorithm 1) in the construction of CiO for RAM, \( F_{\text{branch}} \) first verifies its input, perform the actual computation of \( F \), and authenticates its output. The communication commands of \( F \) is interpreted as access commands in the obfuscated program, and will be accumulated to the corresponding memory accumulator. The difference is that here updating the accumulator is deferred to the combine stage of \( \hat{F} \) defined in \( F_{\text{combine}} \), and the obfuscated CPU state \( \hat{st} \) is never signed or verified by signature.

\( m \) copies of \( F_{\text{combine}} \) will be executed multiple rounds so as to combine the \( m \) newly accumulated value into a common digest. At the first iteration of \( F_{\text{combine}} \), each pair of neighboring CPUs form a group to combine their accumulated access commands into a common value in the parent node. Then, each pair of neighboring groups will form a larger group to combine their values into a common parent node. This process will continue until a common root node is reached, so that the program \( \hat{F} \) will resume to the branch stage.

The compilation procedure then computes an obfuscation of the program \( \hat{F} \). That is, \( F \leftarrow \text{iO.Gen}(\hat{F}) \).

Algorithm 8: \( \hat{F} \)

```plaintext
// for simplicity, we drop the subscripts from \( \tilde{a}_{\text{in}}^{\text{cpu}}, \tilde{a}_{\text{out}}^{\text{cpu}} \) and use \( \tilde{a}_{\text{in}} \) and \( \tilde{a}_{\out} \) respectively

\[ \text{Input : } \tilde{st}_{\text{in}} = (\text{st}_{\text{in}}, \text{id}_{\text{cpu}}, \text{root}_{\text{node}}), \tilde{a}_{\text{in}} \]

1 if \( \text{st}_{\text{in}} = (\text{halt}, \cdot) \) then
2 \hspace{1em} Output Reject;
3 else if \( \text{root}_{\text{node}} \neq \bot \) then
4 \hspace{1em} Compute \( (\tilde{a}_{\text{out}}, \tilde{a}_{\text{out}}) = F_{\text{branch}}(\tilde{st}_{\text{in}}, \tilde{a}_{\text{in}}); \)
5 else
6 \hspace{1em} Compute \( (\tilde{a}_{\text{out}}, \tilde{a}_{\text{out}}) = F_{\text{combine}}(\tilde{st}_{\text{in}}, \tilde{a}_{\text{in}}); \)
7 Output \( (\tilde{a}_{\text{out}}, \tilde{a}_{\text{out}}); \)
```

Step 3: Generating the initial configuration \( (\tilde{\text{mem}}^0, \{\tilde{\text{st}}^0_k\}_{k=1}^m) \). Recall that \( c_0^0 = \bot \). Based on given \( \text{st}^0_1, \ldots, \text{st}^0_m \), the compilation procedure computes the initial configuration for the complied computation system as follows.

- For each \( j \in \{1, \ldots, m\} \), it computes iteratively:

\[ \pi_j \leftarrow \text{Acc.PrepWrite}(pp_{\text{Acc},st}, \text{store}_{\text{st},j-1}, j - 1) \]
\[ \hat{w}_{\text{st},j} \leftarrow \text{Acc.Update}(pp_{\text{Acc},st}, \hat{w}_{\text{st},j-1}, j - 1, \text{st}^0_j, \pi_j) \]
\[ \hat{\text{store}}_{\text{st},j} \leftarrow \text{Acc.WriteStore}(pp_{\text{Acc},st}, \hat{\text{store}}_{\text{st},j-1}, j - 1, \text{st}^0_j) \]

Set \( \text{w}^0_{\text{st}} := \hat{w}_{\text{st},m} \), and \( \text{store}^0_{\text{st}} := \hat{\text{store}}_{\text{st},m} \).
Finally the compilation procedure returns the value $\texttt{II}$ and carries out the result at the halting time $t^*$.

**Final step.** Finally the compilation procedure returns the value $\texttt{II} = (\tilde{\texttt{mem}}^0, \{\tilde{\texttt{st}}^0_j\}_{k=1}^m, \tilde{\texttt{F}})$ as output.

**Evaluation algorithm** $\text{conf} := \text{Eval}(\texttt{II})$: Upon receiving an obfuscated system $\texttt{II}$, the evaluator runs Algorithm 11 and carries out the result

$$(\tilde{\texttt{mem}}^*, \{\tilde{\texttt{st}}^*_{k}, \tilde{\texttt{a}}^*_{M-k}\}_{k=1}^m)$$

at the halting time $t^*$.

- For each $1 \leq k \leq m$, parse:

$$\tilde{\texttt{st}}^*_{k} = (\texttt{st}^*_{k}, k, \cdot)$$

$$\tilde{\texttt{a}}^*_{M-k} = (\texttt{com}^*_{k})$$

- Return $\text{conf} = \{\texttt{st}^*_{k}, \texttt{com}^*_{k}\}_{k=1}^m$.
Algorithm 10: $F_{\text{combine}}$

// for simplicity, we drop the subscripts from $\tilde{a}_{\text{idegu}}$ and $\tilde{a}_{\text{idegu}}^\dagger$, and use $\tilde{a}^{\text{in}}$ and $\tilde{a}^{\text{out}}$ respectively

Input: $\tilde{st}^{\text{in}} = (st^{\text{in}}, id_{\text{cpu}}, \bot), \tilde{a}^{\text{in}} = (\text{node}_1, \text{node}_2)$

Data: $T, \text{pp}_{\text{Acc, st}}, \text{pp}_{\text{Acc, com}}, \text{pp}_{\text{It}}, K_A$

1. Parse node as $(t_\zeta, \text{index}_\zeta, w_{\text{st, }\zeta}, w_{\text{com, }\zeta}, v_\zeta, \sigma_\zeta)$ for $\zeta = 1, 2$;
2. If $t_1 \neq t_2$, output $\\text{Reject}$. Else, let $t = t_1$;
3. If $t < 1$, output $\\text{Reject}$;
4. If $\text{index}_1$ and $\text{index}_2$ are not siblings, output $\text{Reject}$;
5. Set $\text{parent}_\text{index}$ as the parent of $\text{index}_1$ and $\text{index}_2$;
6. for $\zeta = 1, 2$ do
   7. Let $r_{A, \zeta} = \text{PRF}(K_A, (t_\zeta, \text{index}_\zeta))$;
   8. Compute $(sk_{A, \zeta}, v_{A, \zeta}, v_{A, \text{req, }\zeta}) = \text{Spl.Setup}(1^\lambda; r_{A, \zeta})$;
   9. Let $m_\zeta = (t_\zeta, \text{index}_\zeta, w_{\text{st, }\zeta}, w_{\text{com, }\zeta}, v_\zeta)$;
   10. If Spl.Verify($v_{A, \zeta}, m_\zeta, \sigma_\zeta) = 0$ output $\text{Reject}$;
7. Compute $w_{\text{st}}' = \text{Acc.Combine}($pp$_{\text{Acc, st}}, w_{\text{st, }1, 2}, \text{parent}_\text{index})$;
8. Compute $w_{\text{com}}' = \text{Acc.Combine}($pp$_{\text{Acc, com}}, w_{\text{com, }1, 2}, \text{parent}_\text{index})$;
9. Compute $v' = \text{It.r.iterate2to1}($pp$_{\text{It}}, (v_1, v_2), (t, \text{parent}_\text{index}, w_{\text{st, }1, 2}, w_{\text{com, }1, 2})$);
10. Let $r_A' = \text{PRF}(K_A, (t, \text{parent}_\text{index}))$;
11. Compute $(sk_A', v_{A}', v_{A, \text{req}}) = \text{Spl.Setup}(1^\lambda; r_A')$;
12. Let $m' = (t, \text{parent}_\text{index}, w_{\text{st}}, w_{\text{com}}, v')$;
13. Compute $\sigma' = \text{Spl.Sign}(sk_A', m')$;
14. Let parent_node = $(t, \text{parent}_\text{index}, w_{\text{st}}, w_{\text{com}}, v', \sigma')$;
15. if $\text{parent}_\text{index} = \epsilon$ then
   16. Output st$^{\text{out}}$ = $(st^{\text{in}}, id_{\text{cpu}}, \text{parent}_\text{node}), \tilde{a}^{\text{out}} = \bot$;
   17. else
   18. Output st$^{\text{out}}$ = $(st^{\text{in}}, id_{\text{cpu}}, \bot), \tilde{a}^{\text{out}} = \text{parent}_\text{node}$;
Algorithm 11: Eval: Evaluator of $\Pi$

Input: $\Pi = ((\text{mem}^0, \{s_k^t\}_{k=1}^m), F)$

1. Let $z_{\text{max}} \leftarrow \lceil \log(m) \rceil$ be the length of $m$ in binary;

2. for $1 \leq t \leq T$ do

3. Parse $\text{mem}^{t-1} = (\text{store}_{\text{st}}^{t-1}, \text{store}_{\text{com}}^{t-1})$;

4. for $1 \leq k \leq m$ do

5. Compute $(\cdot, \pi_{\text{st}, k}) \leftarrow \text{PrepRead}(pp_{\text{Acc}, \text{st}}, \text{store}_{\text{st}}^{t-1}, k)$;

6. Compute $(\text{com}_{k}^{t-1}, \pi_{\text{com}, k}) \leftarrow \text{PrepRead}(pp_{\text{Acc}, \text{com}}, \text{store}_{\text{com}}^{t-1}, \text{src}(t-1, k))$;

7. Let $\tilde{a}_{k}^\text{in} \leftarrow (\text{com}_{k}^{t-1}, \pi_{\text{st}, k}, \pi_{\text{com}, k})$;

8. Evaluate $(\text{st}_{k}^{t, z_{\text{max}}}, \tilde{a}_{k}^\text{in}) \leftarrow \tilde{F}(\text{st}_{k}^{t-1}, \tilde{a}_{k}^\text{in})$; \hfill // Evaluate $F_{\text{branch}}$

9. Parse $\tilde{a}_{k}^\text{out} = (\cdot, \text{st}_{k}^{t, z_{\text{max}}}, \text{com}_{k}^{t}, \cdot, \cdot)$;

10. Let $\text{store}_{\text{st}}^{t}[k] \leftarrow \text{st}_{k}^{t, z_{\text{max}}}$, which stores $\text{st}_{k}^{t, z_{\text{max}}}$ in the $k$-th cell in $\text{store}_{\text{st}}^{t}$;

11. Let $\text{store}_{\text{com}}^{t}[k] \leftarrow \text{com}_{k}^{t}$, which stores $\text{com}_{k}^{t}$ in the $k$-th cell in $\text{store}_{\text{com}}^{t}$;

12. Let node$_{k}^{t} \leftarrow \tilde{a}_{k}^\text{out}$;

13. if all $\text{st}_{k}^{t, z_{\text{max}}}$ is halt state then

14. Let $\text{mem}^{t} \leftarrow (\text{store}_{\text{st}}^{t}, \text{store}_{\text{com}}^{t})$;

15. For $1 \leq k \leq m$, let $\tilde{a}_{k}^{t} \leftarrow \text{st}_{k}^{t, z_{\text{max}}}$;

16. For $1 \leq k \leq m$, let $\tilde{a}_{k}^{t-1} \leftarrow \text{com}_{k}^{t}$;

17. return $(\text{mem}^{t}, \{\text{st}_{k}^{t}, \tilde{a}_{k}^{t}\}_{k=1}^{m})$;

18. foreach $z$ from $z_{\text{max}} - 1$ to 0 do

19. For each $k \in [m]$, represent $k - 1$ in a binary string $s(k - 1)$ of length $z_{\text{max}}$ and let $k_{z}$ denotes the prefix $z$ bits of $s(k - 1)$;

20. Let $k_{z}||b$ denotes the binary string that $k_{z}$ concatenates bit $b$;

21. for $1 \leq k \leq m$ do

22. Let $\tilde{a}_{k}^\text{in} \leftarrow (\text{node}_{k_{z}||0}, \text{node}_{k_{z}||1})$;

23. Evaluate $(\text{st}_{k_{z}}^{t, z_{\text{max}}}, \tilde{a}_{k_{z}}^\text{in}) \leftarrow \tilde{F}(\text{st}_{k_{z}}^{t, z_{\text{max}}}, \tilde{a}_{k_{z}}^\text{in})$; \hfill // Evaluate $F_{\text{combine}}$

24. Let node$_{k_{z}}^{t} \leftarrow \tilde{a}_{k_{z}}^\text{out}$;

25. Let $\tilde{\text{mem}}^{t} \leftarrow (\text{store}_{\text{st}}^{t}, \text{store}_{\text{com}}^{t})$; \hfill // Input to the next iteration

26. Let $\text{st}_{k}^{t} \leftarrow \tilde{\text{st}}_{k}^{t}$:
**Efficiency.** Let $m$ be the number of CPUs, $|F|$ be the description size of program $F$, $n/m$ be the size of each initial states $s_{t_0}^k$ for $k \in [m]$, computation system $\Pi$ proceeds with time bound $T$. We first note the circuit size of $\tilde{F}$ is $|F| + O(\log m)$, where $\log m$ is the amount of hardwired information in some hybrid programs that required in security proof. Please refer to Section B.3.2 for details. Assuming of Definition 7.7 is defined as follows:

- Compilation time is $O(\text{poly}(|F|) + n)$.
- Compilation size is $O(\text{poly}(|F|) + n)$.
- Parallel evaluation time is $O(T \cdot \text{poly}(|F|))$.
- Evaluation space is $O(m)$, where $m$ term is to keep CPU states of $F$ while branch and combine.

**Theorem 7.6.** Assuming $\iO$ is a secure indistinguishability obfuscator, PRF is a selectively secure puncturable PRF, $\tilde{T}l$tr is a secure topological iterator, $\text{Acc}$ is a secure accumulator, $\text{Spl}$ is a secure splittable signature scheme. Then $\text{CiO}$ is a secure computation-trace indistinguishability obfuscation with respect to $\mathcal{P}_{\text{PRAM}^-}$.

Proof can be found in Section B.3.

### 7.6 CiO for PRAM

Finally, we construct $\text{CiO}$ in the (standard) PRAM (PRAM) model. Recall in Section A.1.2 that, informally, a PRAM consists of $m$ CPUs running simultaneously with random access to a shared memory, but without communication with each others. Formally, the class of distributed computation for PRAM, denoted by $\mathcal{P}_{\text{PRAM}}$, is defined as follows:

**Definition 7.7 (PRAM Computation Class).** $\mathcal{P}_{\text{PRAM}}$ is a class of distributed computation systems for PRAM with $m$ agents (a.k.a. CPU) $1, \ldots, m$ and a shared memory $\mathcal{M}$ where

- the terminating time $t^*$ is bounded by $2^\lambda$,
- the communication between agents are not allowed, i.e., $e_{j \leftarrow k}^t := \bot$ for all $t \in [t^*]$ and for all $j, k \in [m]$,
- the memory size $|\text{mem}|$ is bounded by poly($\lambda$),
- for all $k \in [m]$, the state size $|s_t^k|$ and the communication buffers size $|a_{t \leftarrow k}|$ and $|a_{t \leftarrow k}|$ are bounded by $\text{poly} \log (\lambda)$,
- for all $k \in [m]$, the initial access commands are restricted to $a_0^k \leftarrow \bot$ and $a_0^k \leftarrow \bot$,
- for all $k \in [m]$, the initial states are restricted to $s_{t_0}^k := \bot$.

Our construction of $\text{CiO}$ for PRAM is very similar to that of $\text{CiO}$ for PRAM$^-$ except that $F_{\text{branch}}$ now also takes as input a bit read from the memory with its proof, and outputs a bit to be written to some memory location. Thus, as for $\text{CiO}$ for RAM, the evaluator in addition maintain an accumulator for storing the actual memory content. Correspondingly, instead of executing $F$ directly, $F_{\text{branch}}$ executes another program called $F_{\text{check}}$ which encapsulates $F$ and the oblivious update mechanism described above.

We next describe in detail our scheme $\text{CiO} = \text{CiO}.\{\text{Obf, Eval}\}$ in the PRAM model. The compilation procedure $\text{CiO}.\text{Obf}$ can transform a given computation system $\Pi \in \mathcal{P}_{\text{PRAM}}$ into an obfuscated computation system $\bar{\Pi}$. Here

$$\Pi = (\text{mem}^0, F)$$

$$\bar{\Pi} = ((\text{mem}^0, s^0), F)$$

**Compilation procedure** $\bar{\Pi} \leftarrow \text{CiO}.\text{Obf}(1^\lambda, \Pi)$: We provide the details of the compilation procedure $\text{Obf}(\cdot)$ which consists of several steps as follows.
Step 1: Generating parameters. The compilation procedure computes the following parameters for the obfuscated computation system:

\[ K_A \leftarrow \text{PRF.} \text{Setup}(1^\lambda) \]

\[ (pp_{\text{Acc,mem}}, \hat{w}_{\text{mem},0}, \hat{store}_{\text{mem},0}) \leftarrow \text{Acc.} \text{Setup}(m) \]

\[ (pp_{\text{Acc,ST}}, \hat{w}_{\text{ST},0}, \hat{store}_{\text{ST},0}) \leftarrow \text{Acc.} \text{Setup}(m) \]

\[ (pp_{\text{Acc,COM}}, \hat{w}_{\text{COM},0}, \hat{store}_{\text{COM},0}) \leftarrow \text{Acc.} \text{Setup}(m) \]

\[ (pp_{\text{tr}}, \nu^0) \leftarrow \text{Ttlr.} \text{Setup}(T) \]

Step 2: Generating stateful algorithms \( \hat{F} \). Based on the parameters \( T, pp_{\text{Acc,mem}}, pp_{\text{Acc,ST}}, pp_{\text{Acc,COM}}, pp_{\text{tr}}, K_A \) generated above, as well as program \( F \), we define the program \( \hat{F} \) in Algorithm 12. \( \hat{F} \) executes internal programs \( F_{\text{branch}} \) (Algorithm 13) or \( F_{\text{combine}} \) (Algorithm 14) depending on its input. Now \( F_{\text{branch}} \) in turn executes \( F_{\text{check}} \) defined in Algorithm 7, where \( F_{\text{check}} = \text{Acc.} \text{Compile}(F, \text{Acc.} \text{OU} \text{pdate}(pp_{\text{Acc,mem}})) \).

The compilation procedure then computes an obfuscation of the program \( \hat{F} \). That is, \( \hat{F} \leftarrow iO. \text{Gen}(\hat{F}) \).

Algorithm 12: \( \hat{F} \), which is identical to its PRAM\(^{-} \) counterpart (Algorithm 8).

// for simplicity, we drop the subscripts from \( \hat{a}_{\text{id_cpu}} \) and \( \hat{a}_{\text{id_cpu}} \), and use \( \hat{a} \) in and \( \hat{a} \) out respectively

\begin{verbatim}
Input : \( \hat{s}^\text{in} = (st^\text{in}, id_{\text{CPU}}, \text{root_node}) \), \( \hat{a}^\text{in} \\
1 if \( \hat{s}^\text{in} = (halt,.) \) then \\
2 Output Reject; \\
3 else if \( \text{root_node} \neq \perp \) then \\
4 Compute \( \hat{s}^\text{out} = F_{\text{branch}}(\hat{s}^\text{in}, \hat{a}^\text{in}) \); \\
5 else \\
6 Compute \( \hat{s}^\text{out} = F_{\text{combine}}(\hat{s}^\text{in}, \hat{a}^\text{in}) \);
7 Output \( \hat{s}^\text{out} \);
\end{verbatim}

Step 3: Generating the initial configuration \( (\hat{\text{mem}}^0, \hat{s}^0) \). Recall that initial memory accesses are empty:

\[ \hat{a}_{k \leftarrow \text{mem}}^0 = \perp, \hat{a}_{k \leftarrow \text{cpu}}^0 = \perp \]. Based on \( \hat{\text{mem}}^0 \) and \( \hat{s}^0_k = \perp \) for all \( k \in [m] \), the compilation procedure computes the initial configuration for the compiled computation system as follows.

- For each \( j \in \{1, \ldots, |\text{mem}|\} \), it computes iteratively:

\[ \hat{store}_{\text{mem},j} \leftarrow \text{Acc.} \text{WriteStore}(pp_{\text{Acc,mem}}, \hat{store}_{\text{mem},j-1}, j, \hat{\text{mem}}^0[j]) \]

\[ \pi_j \leftarrow \text{Acc.} \text{PrepWrite}(pp_{\text{Acc,mem}}, \hat{store}_{\text{mem},j-1}, j) \]

\[ \hat{w}_j \leftarrow \text{Acc.} \text{Update}(pp_{\text{Acc,mem}}, \hat{w}_{j-1}, j, x_j, \pi_j) \]

Set \( \hat{w}^0_{\text{mem}} := \hat{w}|_{\text{mem}}^0 \), and \( \hat{store}^0_{\text{mem}} := \hat{store}|_{\text{mem}}^0 \).
- Set \( \hat{w}^0_{\text{ST}} := \perp \) and \( \hat{store}^0_{\text{ST}} := \hat{store}_{\text{ST},0} \), where \( \hat{store}_{\text{ST},0} \) is initialized with value \( \perp \) as the initial state in all \( m \) cells.
- Set \( \hat{w}^0_{\text{COM}} := \perp \) and \( \hat{store}^0_{\text{COM}} := \hat{store}_{\text{COM},0} \), where \( \hat{store}_{\text{COM},0} \) is initialized with value \( \perp \) as no communication in all \( m \) cells.
Finally, the compilation procedure returns the value $\tilde{\Pi}$ and use $\tilde{a}$ and $\tilde{a}$ respectively.

**Algorithm 13**: $F_{\text{branch}}$

// for simplicity, we drop the subscripts from $\tilde{\Pi}$, and $\tilde{a}$, and use $\tilde{a}$ and $\tilde{a}$ respectively

**Input**: $\tilde{\Pi}$ = ($\tilde{a}$, $\tilde{a}$, root_node), $\tilde{a}$ = ($\tilde{a}$, $\tilde{a}$, $\tilde{a}$, $\tilde{a}$, $\tilde{a}$, $\tilde{a}$, $\tilde{a}$, $\tilde{a}$), $\tilde{a}$ = ($\tilde{a}$, $\tilde{a}$, $\tilde{a}$, $\tilde{a}$, $\tilde{a}$, $\tilde{a}$, $\tilde{a}$, $\tilde{a}$)

**Data**: $\Pi$, $\Pi$, $\Pi$, $\Pi$, $\Pi$, $\Pi$, $\Pi$, $\Pi$, $\Pi$, $\Pi$, $\Pi$, $\Pi$, $\Pi$, $\Pi$

1. Parse root_node as (t, root_index, w, w, v, v, v)
2. Let $r_A$ = PRF($K_A$, (t, root_index))
3. Compute $(sk_A, vk_A, vk_A)$ = $\text{Spl.Setup}(1^\lambda, r_A)$
4. Let $b = (t, root_index, w, w, v, v, v)$
5. If $\text{Spl.Verify}(vk_A, b)$ = 0 output Reject;
6. If $\text{Acc.VerifyRead}(ppp, w, w, (id_c, loc), (v, v, v)) = 0$ output Reject;
7. Compute $v = \text{itr. Iterate}(ppp, t, id_c, w, w, v, v, v, v, v, v, v)$
8. If $st = \text{Reject}$ then
   9. Output Reject;
   10. else
   11.   Let $r_A'$ = PRF($K_A$, (t, root_index))
   12.   Compute $(sk_A', vk_A', vk_A', re)$ = $\text{Spl.Setup}(1^\lambda, r_A')$
   13.   Let $m = (t, root_index, w, w, v, v, v)$ and $m = \text{Spl.Sign}(sk_A, m)$
   15.   Output $\tilde{a}$ = ($\tilde{a}$, $\tilde{a}$, $\tilde{a}$, $\tilde{a}$, $\tilde{a}$, $\tilde{a}$, $\tilde{a}$, $\tilde{a}$, $\tilde{a}$, $\tilde{a}$, $\tilde{a}$, $\tilde{a}$, $\tilde{a}$, $\tilde{a}$, $\tilde{a}$, $\tilde{a}$, $\tilde{a}$, $\tilde{a}$)

- Set $root_node^0 = (t, root_index, w, w, v, v, v)$ where $t = 0$, root_index is $\epsilon$; and $w, v, v, v$ are computed above; and $v$ is computed as follows:

$$r_A = PRF(K_A, 0)$$

$$\text{Prf}(sk_A, vk_A) = \text{Spl.Setup}(1^\lambda, r_A)$$

- $\sigma = \text{Spl.Sign}(sk_A, (0, root_index, w, w, v))$

- $st = ((st, st), d, b, w, v) = ((\bot, \bot), \text{READ}, \bot, \bot, \bot)$ where $w$ is computed above.

- $buff[1] = \ldots = buff[m] = (\bot, \bot)$

- Now we can define the initial configuration as

$$\tilde{\Pi} = (\tilde{a}, \tilde{a}, \tilde{a}, \tilde{a}, \tilde{a}, \tilde{a}, \tilde{a}, \tilde{a}, \tilde{a})$$

**Final step.** Finally, the compilation procedure returns the value $\tilde{\Pi} = (\tilde{a}, \tilde{a}, \tilde{a})$ as output.

**Evaluation algorithm** conf := Eval($\tilde{\Pi}$): Upon receiving an obfuscated system $\tilde{\Pi}$, the evaluator parses $\tilde{\Pi} = (\tilde{a}, \tilde{a})$, where $\tilde{a} = (root_node, root_node, v, v, v)$. It sets $\tilde{a}_k = (root_node, k, root_node, v, v, v)$ for $k = 1$ to $m$. It then runs Algorithm 11 and carries out the result

$$(\tilde{a}, \tilde{a}, \tilde{a})_{k=1}^m$$

at the halting time $t^*$. 

48
Algorithm 14: $F_{\text{combine}}$, which is identical to its PRAM counterpart (Algorithm 10).

// for simplicity, we drop the subscripts from $\tilde{a}_{\text{in}}$ and $\tilde{a}_{\text{out}}$ and use $\tilde{a}_{\text{in}}$ and $\tilde{a}_{\text{out}}$ respectively

Input: $\tilde{\text{st}}_{\text{in}} = (\text{st}_{\text{in}}, \text{id}_{\text{cpu}}, \bot), \tilde{\text{a}}_{\text{in}} = (\text{node}_1, \text{node}_2)$

Data: $\text{pp}_{\text{Acc, st}}, \text{pp}_{\text{Acc, com}}, \text{pp}_{\text{itr}}, K_A$

1. Parse node$_\zeta$ as $(t_\zeta, \text{index}_\zeta, w_{\text{st},\zeta}, w_{\text{com},\zeta}, v_\zeta, \sigma_\zeta)$ for $\zeta = 1, 2$;
2. If $t_1 \neq t_2$, output Reject. Else, let $t = t_1$;
3. If $t < 1$, output Reject;
4. If index$_1$ and index$_2$ are not siblings, output Reject;
5. Set parent$_\text{index}$ as the parent of index$_1$ and index$_2$;
6. for $\zeta = 1, 2$ do
   7. Let $r_{A,\zeta} = \text{PRF}(K_A, (t_\zeta, \text{index}_\zeta));$
   8. Compute $(\text{sk}_{A,\zeta}, \text{vk}_{A,\zeta}, \text{vk}_{A,\text{rej},\zeta}) = \text{Spl.Setup}(1^\lambda; r_{A,\zeta});$
   9. Let $m_\zeta = (t_\zeta, \text{index}_\zeta, w_{\text{st},\zeta}, w_{\text{com},\zeta}, v_\zeta);$
   10. If Spl.Verify$(\text{vk}_{A,\zeta}, m_\zeta, \sigma_\zeta) = 0$ output Reject;
7. Compute $w'_{\text{st}} = \text{Acc.Combine}(\text{pp}_{\text{Acc, st}}, w_{\text{st},1}, w_{\text{st},2}, \text{parent}_\text{index});$
8. Compute $w'_{\text{com}} = \text{Acc.Combine}(\text{pp}_{\text{Acc, com}}, w_{\text{com},1}, w_{\text{com},2}, \text{parent}_\text{index});$
9. Compute $v' = \text{itr.iterate2to1}(\text{pp}_{\text{itr}}, (v_1, v_2), (t, \text{parent}_\text{index}, w_{\text{st},1}, w_{\text{com},1}, w_{\text{st},2}, w_{\text{com},2}));$
10. Let $r'_A = \text{PRF}(K_A, (t, \text{parent}_\text{index}));$
11. Compute $(\text{sk}'_A, \text{vk}'_A, \text{vk}'_{A,\text{rej}}) = \text{Spl.Setup}(1^\lambda; r'_A);$
12. Let $m' = (t, \text{parent}_\text{index}, w'_{\text{st}}, w'_{\text{com}}, v');$
13. Compute $\sigma' = \text{Spl.Sign}(\text{sk}'_A, m');$
14. Let parent$_\text{node} = (t, \text{parent}_\text{index}, w'_{\text{st}}, w'_{\text{com}}, v', \sigma');$
15. if parent$_\text{index} = \epsilon$ then
   16. Output $\tilde{\text{st}}_{\text{out}} = (\text{st}_{\text{in}}, \text{id}_{\text{cpu}}, \text{parent}_\text{node}), \tilde{\text{a}}_{\text{out}} = \bot;$
   17. else
   18. Output $\tilde{\text{st}}_{\text{out}} = (\text{st}_{\text{in}}, \text{id}_{\text{cpu}}, \bot), \tilde{\text{a}}_{\text{out}} = \text{parent}_\text{node};$
For $1 \leq k \leq m$, parse:

\[
\text{mem}^{t^*} = (\text{store}^{t^*}_{\text{mem}}, \text{store}^{t^*}_{\text{st}}, \text{store}^{t^*}_{\text{com}}, \text{buff}^{t^*})
\]

\[
\text{st}_k = (\text{st}^{t^*}_k, k, \cdot)
\]

\[
\text{a}^{t^*}_{\text{H} \leftarrow k} = (\text{node}^{t^*}_k, \text{loc}^{t^*}_k, b_k^{t^*})
\]

For $1 \leq k \leq m$, let

\[
a^{t^*}_{\text{H} \leftarrow k} = (\text{loc}^{t^*}_k, b_k^{t^*})
\]

\[
a^{t^*}_{k \leftarrow \text{H}} = \bot.
\]

Let \(\text{mem}^{t^*} = \text{store}^{t^*}_{\text{mem}}\).

Return \(\text{conf} = (\{\text{st}^{t^*}_k, a^{t^*}_{\text{H} \leftarrow k}, a^{t^*}_{k \leftarrow \text{H})}_{k=1}^m, \text{mem}^{t^*})\).

**Efficiency.** Let \(m\) be the number of CPUs, \(|F|\) be the description size of program \(F\), \(n\) be the description size of initial memory \(\text{mem}^0\), computation system \(\Pi\) proceeds with time and space bound \(T\) and \(S\). We first note the circuit size of \(\tilde{F}\) is \(|F| + O(\log m)|\), where \(\log m\) is the amount of hardwired information required in security proof (similar to Section B.3.2). Assume that \(iO\) is a circuit obfuscator with circuit size \(|iO(C)| \leq poly|C|\) for given circuit \(C\). Our CiO for PRAM has following complexity:

- Compilation time is \(\tilde{O}(\text{poly}(|F|) + n)\).
- Compilation size is \(\tilde{O}(\text{poly}(|F|) + n)\).
- Parallel evaluation time is \(\tilde{O}(T \cdot \text{poly}(|F|))\).
- Evaluation space is \(\tilde{O}(m + S)\), where \(m\) term is to keep CPU states of \(F\) while branch and combine, and \(S\) term is needed by \(F\) intrinsically.

**Theorem 7.8.** Assuming \(iO\) is a secure indistinguishability obfuscator, PRF is a selectively secure puncturable PRF, TItr is a secure topological iterator, Acc is a secure positional accumulator, Spl is a secure splittable signature scheme. Then CiO is a secure computation-trace indistinguishability obfuscation with respect to \(P_{\text{PRAM}}\).

The proof sketch can be found in Section B.4.

## 8 Constructing \(\mathcal{RE}\) in the RAM Model (\(\mathcal{RE}\)-RAM)

In this section, we showcase the power of our fully succinct CiO for RAM, and we construct the first fully succinct randomized encoding in the RAM model. Recall in Section A.2 that, a randomized encoding of a computation instance \((P, x)\) requires to hide everything except its output \(y = P(x)\) and runtime \(t^*\). This requires to hide both the content and the access pattern of the computation. At a high level, our construction is a fairly natural one: we use public-key encryptions to hide the content (including the input) and oblivious RAM to hide the access pattern, and then use CiO to obfuscate the compiled computation instance. Namely, our \(\mathcal{RE}\) encoding algorithm outputs \(\Pi = \text{CiO}(\Pi_{\text{hide}})\), where \(\Pi_{\text{hide}}\) is a computation instance defined by \(P_{\text{hide}}\) and \(x_{\text{hide}}\). \(P_{\text{hide}}\) is a \(PK\mathcal{E}\) and ORAM compiled version of \(P\), and \(x_{\text{hide}}\) is an encrypted version of \(x\). Namely, \(P_{\text{hide}}\) outputs encrypted CPU states and memory contents at each time step, and uses ORAM to compile its memory access (with randomness supplied by PRF for succinctness).

Intuitively, if \(PK\mathcal{E}\) and ORAM are secure, then the computation should be hidden. However, note that, the decryption keys need to be hardwired in \(P_{\text{hide}}\) to evaluate \(P(x)\). As CiO does not hide anything explicitly, it is not clear whether we can use the security of \(PK\mathcal{E}\) and ORAM at all. In particular, it is unlikely that we can use the security of ORAM, since it only hides the access pattern when the CPU state and memory contents are hidden from the adversary. Indeed, hiding the access pattern is the major technical challenge to prove the security of our \(\mathcal{RE}\) construction. Next we provide an overview of our main ideas.
Algorithm 15: Eval: Evaluator of $\tilde{\Pi}$

Input: $\tilde{\Pi} = (\overline{\text{mem}}^t, \{\overline{\text{st}}_{st,k}\}_{k=1}^m, \overline{F})$

1. Let $z_{\text{max}} \leftarrow \lceil \log(m) \rceil$ be the length of $m$ in binary;

2. for $1 \leq t \leq T$ do

   3. Parse $\overline{\text{mem}}^{t-1} = (\overline{\text{store}}_{\text{mem}}^{t-1}, \overline{\text{store}}_{\text{st}}^{t-1}, \overline{\text{store}}_{\text{com}}^{t-1}, \overline{\text{buff}}^{t-1})$

      for $1 \leq k \leq m$ do

         5. Compute $(\cdot, \pi_{\text{st},k}^{t-1}) \leftarrow \text{PrepRead}(\overline{\text{pp}}_{\text{Acc},\text{st}}, \overline{\text{store}}_{\text{st}}^{t-1}, k)$

         6. Compute $(\overline{\text{com}}_{k}^{t-1}, \pi_{\text{com},k}^{t-1}) \leftarrow \text{PrepRead}(\overline{\text{pp}}_{\text{Acc},\text{com}}, \overline{\text{store}}_{\text{com}}^{t-1}, \text{src}(t-1, k))$

         7. Parse $\overline{\text{buff}}^{t-1}[k] = (b_{k}^{\text{in}}, \pi_{\text{mem},k}^{\text{in}})$

         8. Let $\overline{\pi}_{k}^{\text{in}} \leftarrow (t_{k}^{\text{in}}, \overline{\text{com}}_{k}^{t-1}, \pi_{\text{mem},k}^{\text{in}}, \pi_{\text{st},k}^{t-1}, \pi_{\text{com},k}^{t-1})$

         9. Evaluate $(\overline{\text{st}}_{k}^{t,z_{\text{max}}}, \overline{\pi}_{k}^{t-1}) \leftarrow \overline{F}(\overline{\text{st}}_{k}^{t-1}, \overline{\pi}_{k}^{t-1})$;  // Evaluate $F_{\text{branch}}$

   10. Parse $\overline{\pi}_{k}^{t-1} = (\cdot, \overline{\text{st}}_{k}^{t,z_{\text{max}}}, \overline{\text{com}}_{k}^{t-1}, \cdot)$

   11. Let $\overline{\text{store}}_{\text{st}}^{t}[k] \leftarrow \overline{\text{st}}_{k}^{t,z_{\text{max}}}$, which stores $\overline{\text{st}}_{k}^{t,z_{\text{max}}}$ in the $k$-th cell in $\overline{\text{store}}_{\text{st}}^{t}$

   12. Let $\overline{\text{store}}_{\text{com}}^{t}[k] \leftarrow \overline{\text{com}}_{k}^{t-1}$, which stores $\overline{\text{com}}_{k}^{t-1}$ in the $k$-th cell in $\overline{\text{store}}_{\text{com}}^{t}$

if $\overline{\text{loc}}_{k}^{t} = \bot$ for $1 \leq k \leq m$ then

   15. Let $\overline{\text{store}}_{\text{mem}}^{t-1}$

   16. For $1 \leq k \leq m$, let $\overline{\text{buff}}^{t}[k] = (\bot, \bot)$

else

   for $1 \leq k \leq m$ do

      19. Compute $\overline{\text{buff}}^{t}[k] = (b_{k}^{\text{in}}, \pi_{\text{mem},k}^{\text{in}}) \leftarrow \text{PrepRead}(\overline{\text{pp}}_{\text{Acc},\text{mem}}, \overline{\text{store}}_{\text{mem}}^{t-1}, \overline{\text{loc}}_{k}^{t})$

      20. Let $\overline{\text{store}}_{\text{mem}}^{t} \leftarrow \overline{\text{store}}_{\text{mem}}^{t-1}$

      21. For $1 \leq k \leq m$, compute $\overline{\text{store}}_{\text{st}}^{t,k} \leftarrow \text{WriteStore}(\overline{\text{pp}}_{\text{Acc},\text{st}}, \overline{\text{store}}_{\text{st}}^{t-1,k}, (\overline{\text{loc}}_{k}^{t}, b_{k}^{t})$)

      22. Let $\overline{\text{store}}_{\text{com}}^{t} \leftarrow \overline{\text{store}}_{\text{com}}^{t-1}$

if all $\overline{\text{st}}_{k}^{t,z_{\text{max}}}$ is halt state then

   24. Let $\overline{\text{mem}}^{t} \leftarrow (\overline{\text{store}}_{\text{mem}}^{t}, \overline{\text{store}}_{\text{st}}^{t}, \overline{\text{store}}_{\text{com}}^{t}, \overline{\text{buff}}^{t})$

   25. For $1 \leq k \leq m$, let $\overline{\text{st}}_{k}^{t} \leftarrow \overline{\text{st}}_{k}^{t,z_{\text{max}}}$

   26. For $1 \leq k \leq m$, let $\overline{\pi}_{k,z_{\text{max}}} \leftarrow (\overline{\text{node}}_{k}^{t}, \overline{\text{loc}}_{k}^{t}, b_{k}^{t})$

   27. return $(\overline{\text{mem}}^{t}, \{\overline{\text{st}}_{k}^{t}, \overline{\pi}_{k,z_{\text{max}}}\}_{k=1}^{m})$

for each $z$ from $z_{\text{max}} - 1$ to 0 do

   For each $k \in [m]$, represent $k-1$ in a binary string $s(k-1)$ of length $z_{\text{max}}$ and let $k_{z}$ denotes the prefix $z$ bits of $s(k-1)$

   Let $k_{z} \| b$ denotes the binary string that $k_{z}$ concatenates bit $b$

   for $1 \leq k \leq m$ do

      32. Let $\overline{\pi}_{k}^{t} \leftarrow (\overline{\text{node}}_{k_{z} \| 0}, \overline{\text{node}}_{k_{z} \| 1})$

      33. Evaluate $(\overline{\text{st}}_{k}^{t,z_{z_{\text{max}}}+1}, \pi_{k}^{t}) \leftarrow \overline{F}(\overline{\text{st}}_{k}^{t,z_{z_{\text{max}}}+1}, \overline{\pi}_{k}^{t-1})$;  // Evaluate $F_{\text{combine}}$

      34. Let $\overline{\text{node}}_{k_{z} \| 0} \leftarrow \overline{\pi}_{k}^{t}$

   35. Let $\overline{\text{mem}}^{t} \leftarrow (\overline{\text{store}}_{\text{mem}}^{t}, \overline{\text{store}}_{\text{st}}^{t}, \overline{\text{store}}_{\text{com}}^{t}, \overline{\text{buff}}^{t})$;  // Input to the next iteration

   36. Let $\overline{\text{st}}_{k}^{t} \leftarrow \overline{\text{st}}_{k}^{t,0}$
Basic version: \( \mathcal{RE} \) for oblivious RAM computation To demonstrate the ideas in our full-fledged construction, we start with the simpler case of \( \mathcal{RE} \) for oblivious RAM computation where the given RAM computation instance \( \Pi \) defined by \((P, x)\) has oblivious access pattern. Namely, we assume that there is a public access function \( \text{ap}(t) \) that predicts the memory access at each time step \( t \), which is given to the simulator. Thus, we only need to hide the content of CPU state and memory in each step of the computation, but do not need to use oblivious RAM to hide the access pattern.

For this simpler case, we can directly use techniques developed by [KLW15] to hide the content using public-key encryptions. In fact, the construction of machine-hiding encoding for oblivious only need to hide the content of CPU state and memory in each step of the computation, but do not need to use instance \( \Pi \) for oblivious RAM (\( \text{ORAM} \)). We also initiate the \( \text{ORAM} \) for circuits. Our \( \text{CiO} \)-based construction presented below can be viewed as a modularization and simplification of their construction through our \( \text{CiO} \) notion.

Recall that our construction is of the form \( \mathcal{RE}.\text{Encode}(P, x) = \text{CiO}(\Pi_{\text{hide}}) \), where \( \Pi_{\text{hide}} \) is defined by \( P_{\text{hide}} \) and \( x_{\text{hide}} \). Here, we only use \( \mathcal{PKE} \) to compile \( P \), and denote the compiled program as \( P_{\mathcal{PKE}} \) instead of \( P_{\text{hide}} \). We also denote encrypted input by \( x_{\mathcal{PKE}} \) instead of \( x_{\text{hide}} \). At a high level, \( P_{\mathcal{PKE}} \) emulates \( P \) step by step, but instead of outputting the CPU state and memory content in the clear, \( P_{\mathcal{PKE}} \) outputs an encrypted version of them. \( P_{\mathcal{PKE}} \) also expects encrypted CPU states and memory contents as input, and emulate \( P \) on the decryption of the input. A key idea here (following [KLW15]) is to encrypt each message (either a CPU state of a memory cell) using different keys, and generate these keys (as well as encryption randomness) using puncturable PRF (PPRF), which allows us to use a standard puncturing argument (extended to work with \( \text{CiO} \)) to move to a hybrid where semantic security holds for a particular message so that we can “erase” the message.

In the detailed proof, we prove the security by a sequence of hybrids that “erase” the computation backward in time, which leads to a simulated encoding \( \text{CiO}(\Pi_{\text{Sim}}) \) where all ciphertexts generated by \( P_{\text{Sim}} \) as well as in \( x_{\text{Sim}} \) are replaced by encryption of a special dummy symbol. More precisely, \( P_{\text{Sim}} \) simulates the access pattern using the public access function \( \text{ap} \) at each time step \( t < t^* \), simply ignores the input and outputs encryptions of dummy (for both CPU state and memory content), and output \( y \) at time step \( t = t^* \).

Full solution: \( \mathcal{RE} \) for general RAM computation We now turn to our full solution, and deal with the main challenge of hiding access pattern. As mentioned, our approach is a natural one, where we use oblivious RAM (ORAM) compiler to hide the access pattern. Recall that an ORAM compiler compiles a RAM program by replacing each memory access by a randomized procedure \( \text{OACCESS} \) that implements to memory access in a way that hides the access pattern. Given a computation instance \( \Pi \) defined by \((P, x)\), we first compile \( P \) using an ORAM compiler with randomness supplied by puncturable PRF. Let \( \mathcal{F}_{\text{ORAM}} \) denote the compiled program. We also initiate the ORAM memory by inserting the input \( x \). Let \( x_{\text{ORAM}} \) denote the resulting memory. We then compile \((P_{\text{ORAM}}, x_{\text{ORAM}})\) using \( \mathcal{PKE} \) in the same way as in the basic version above. Namely, we use PPRF to generate multiple keys, and use each key to encryption a single message, including the input \( x_{\text{ORAM}} \). Denote the resulting instance by \((P_{\text{hide}}, x_{\text{hide}})\). Our randomized encoding of computation instance \((P, x)\) is now \( \Pi = \text{CiO}(\Pi_{\text{hide}}) \), where \( \Pi_{\text{hide}} \) is defined by \( P_{\text{hide}} \) and \( x_{\text{hide}} \).

Note that ORAM security only holds when the adversary does not learn any content of the computation. Given the fact that \( \text{CiO} \) does not hide anything explicitly, it is unlikely that we can use the security of ORAM in a black-box way. In a previous seminal work [CHJV15], Canetti et al. provide a novel solution to this problem, and prove the security via a sequence of hybrids that “erase” the computation forward in time. Unfortunately, their solution incurs dependency on the space complexity of the RAM program, and thus is not fully succinct.

To solve this problem, we rely on the specific ORAM construction of [CP13] (referred to as CP ORAM hereafter), and develop a puncturing technique to reason about the simulation. As in our basic version, we prove the security by a sequence of hybrids that “erase” the computation backward in time. At a very high level, to move from the \( i \)-th hybrid to the \((i - 1)\)-th hybrid, i.e., erase the computation at \( i \)-th time step, we “puncture” ORAM at time step \( i \) (i.e., the \( i \)-th memory access), which enables us to replace the access pattern by a simulated one at this time step. We can then move to the \((i - 1)\)-th hybrid by replacing the access pattern,
erasing the content and computation, and undoing the “puncturing.”

Puncturing the ORAM access pattern cleanly could be very subtle. Note that the access pattern at time step $i$ is generated at the latest time step $i'$ that access the same memory location as time step $i$; this last access time $i'$ can be much smaller than $i$, so the puncturing may cause global changes in the computation. Thus, moving to the punctured hybrid, i.e., the $(i - 1)$-th hybrid in the previous paragraph, requires a sequence of sub-hybrids that modifies the computation step by step. We therefore further introduce an auxiliary “partially puncturing” to achieve this goal. This completes the overview of our main ideas. In the detailed proof in Section B.5, we will elaborate the above ideas.

**Section Outline.** The remaining of this section will be organized as follows. We will first list all required building blocks in Section 8.1 and then review the CP ORAM in Section 8.2. Next we provide the RE construction details in Section 8.3, and finally, we prove the security in Section B.5.

### 8.1 Building Blocks

In our RE construction in Section 8.3, we will use several building blocks:

- Public-key encryption scheme $\mathcal{PKE} = \mathcal{PKE}.\{\text{Gen}, \text{Encrypt}, \text{Decrypt}\}$ with IND-CPA security. Here we use $\ell_1 = \ell_1(\lambda)$ bits of randomness in $\mathcal{PKE}.\text{Gen}$, and $\ell_2 = \ell_2(\lambda)$ bits of randomness in $\mathcal{PKE}.\text{Encrypt}$ respectively; we let $\ell_{\text{rnd}} = \ell_1 + \ell_2$, and assume the ciphertext length in $\mathcal{PKE}.\text{Encrypt}$ is $\ell_3$.
- Puncturable PRF scheme $\mathcal{PPRF} = \mathcal{PPRF}.\{\text{Setup}, \text{Puncture}, \text{Eval}\}$ with key space $\mathcal{K}$, punctured key space $\mathcal{K}_{\text{punct}}$, domain $[T] \cup ([T] \times [\log n])$, and range $\{0, 1\}^{\ell_{\text{rnd}}}$.
- Computation-trace indistinguishability obfuscation scheme in the RAM model, $\text{CiO} = \text{CiO}.\{\text{Obf}, \text{Eval}\}$.
- The oblivious RAM compiler by Chung and Pass [CP13].

The computation-trace indistinguishability obfuscation for RAM has been introduced and constructed in Sections 5.1 and 6.2. In the next subsection, we review the oblivious RAM compilation technique in [CP13].

We also use several primitives in vector form (Section 8.3), and they are defined here for completeness. Bold face symbols, such as $\text{pk}$, $\text{sk}$, $\text{r}$, and $\text{dummy}$, denote vectors, and a vector $v$ concatenated with index $i$ in square brackets $v[i]$ denotes the $i$th element in $v$. The public key encryption scheme is generalized to vector form as follows:

- $\mathcal{PKE}.\text{Gen}(1^\lambda; \text{r})$: The key generating algorithm takes as input the security parameter $\lambda$ and a vector of randomness $\text{r}$. It outputs vector of pairs of public and secret keys $(\text{pk}, \text{sk})$, where $(\text{pk}[i], \text{sk}[i]) = \mathcal{PKE}.\text{Gen}(1^\lambda, \text{r}[i])$ for each $i$.
- $\mathcal{PKE}.\text{Encrypt}(\text{pk}, \text{m}; \text{r})$: The encrypting algorithm takes as input a vector of public keys $\text{pk}$, a vector of messages $\text{m}$, and a vector of randomness $\text{r}$. It outputs a vector of ciphertext $\text{c}$, where $\text{c}[i] = \mathcal{PKE}.\text{Encrypt}(\text{pk}[i], \text{m}[i], \text{r}[i])$ for each $i$.
- $\mathcal{PKE}.\text{Decrypt}(\text{sk}, \text{c})$: The decrypting algorithm takes as input a vector of secret keys $\text{sk}$ and a vector of ciphertext $\text{c}$. It outputs a vector of messages $\text{m}$, where $\text{m}[i] = \mathcal{PKE}.\text{Decrypt}(\text{sk}[i], \text{c}[i])$ for each $i$.

The puncturable PRF scheme is generalized to vector form as follows, and we did not extend the puncturing procedure Puncture.

- $\text{PRF}(K, \text{x})$: The pseudorandom function takes as input the key $K$ and a vector $\text{x}$. It outputs vector of pseudorandom numbers $\text{r}$, where $\text{r}[i] = \text{PRF}(K, \text{x}[i])$ for each $i$.
- $\text{PPRF}.\text{Eval}(K\{x\}', \text{x})$: The pseudorandom function takes as input the punctured key $K\{x\}'$ and a vector $\text{x}$. It outputs vector of pseudorandom numbers $\text{r}$, where $\text{r}[i] = \text{PPRF}.\text{Eval}(K\{x\}', \text{x}[i])$ for each $i$.
8.2 Recap: The CP-ORAM

As mentioned in the section summary above, we use ORAM techniques to hide the access pattern. Our construction is essentially based on the ORAM compilation technique by Chung and Pass [CP13]; for short, we call it CP-ORAM. We believe that our construction can also be based on all existing tree-based ORAM compilation techniques [SCSL11]. Below, we give an overview of CP-ORAM; please refer to [CP13] for more details. For better presentation, we use both function program and next-step program to describe the programs that used in our construction.

In CP ORAM (as well as all tree-based ORAM), the memory is stored in a complete binary tree (called ORAM tree), where each node of the tree is associated with a bucket that can store a few memory blocks. A position map $\text{Pos}$ is used to record where each memory block is stored in the tree, where a block $b$ is stored in a node somewhere along a path from the root to the leaf indexed by $\text{Pos}[b]$. Each memory block $b$ in the ORAM tree also stores its index $b$ and position map value $\text{Pos}[b]$ as meta data. Each memory access (say, to block $b$) is performed by $\text{OACCESS}$, which (i) reads the position map value $\text{pos} = \text{Pos}[b]$ and refresh $\text{Pos}[b]$ to a random value, (ii) fetches and remove the block $b$ from the path, (iii) updates the block content and puts it back to the root, and (iv) performs a flush operation along another random path $\text{pos}'$ to move the blocks down along $\text{pos}'$ (subject to the condition that each block is stored in the path specified by their position map value). At a high level, the security follows by the fact that the position map values are uniform and hidden from the adversary, and thus the access pattern of each $\text{OACCESS}$ is simply two uniformly random paths, which is trivial to simulate. This completes the basic version of CP ORAM. The details can be found in Section 8.2.1. The position map is large in the above basic version and is recursively outsourced to lower level ORAM structures to reduce its size. See Section 8.2.2 for more details.

8.2.1 Basic version: ORAM with $\Theta(n)$ registers

We here present the basic version of CP-ORAM. Consider memory be an array with $n$ cells. The CP compiler can transform a given program $P$ into a new program $P_o$, which replaces the memory access instructions by the oblivious memory access algorithm $\text{OACCESS}$. More concretely, each memory access command $\text{READ}(\text{loc})$ and $\text{WRITE}(\text{loc}, \text{val})$ is replaced by corresponding commands $\text{OACCESS}(\text{loc}, \perp)$ and $\text{OACCESS}(\text{loc}, \text{val})$ respectively which will be specified shortly. The new program $P_o$ has the same registers as $P$ and additionally has $n/\alpha$ registers for storing a position map $\text{Pos}$, plus a polylogarithmic number of additional work registers used by $\text{OACCESS}$, where $\alpha \geq 2$ is a constant to ensure that the position map is smaller than the memory size. In its external memory, $P_o$ will maintain a complete binary tree $\Gamma$ of depth $\log(n/\alpha)$; we index nodes in the tree by a binary string of length at most tree depth $\log(n/\alpha)$, where the root is indexed by the empty string $\epsilon$, and each node indexed by $\gamma$ has left and right children indexed $\gamma0$ and $\gamma1$, respectively. Each memory cell at location $\text{loc}$ will be associated with a random leaf $\text{pos}$ in the tree, specified by the position map $\text{Pos}$; as we shall see shortly, the memory cell $\text{loc}$ will be stored at one of the nodes on the path from the root $\epsilon$ to the leaf $\text{pos}$. We assign a block of $\alpha$ consecutive memory cells to the same leaf; thus any memory cell $\text{loc}$ corresponding to block $b = \lfloor \text{loc}/\alpha \rfloor$ will be associated with leaf $\text{pos} = \text{Pos}(b)$.

Each node in the tree is associated with a bucket which stores (at most) $K$ tuples $(b, \text{pos}, v)$, where $v$ is the content of block $b$ and $\text{pos}$ is the leaf associated with the block $b$, and $K \in \omega(\log n) \cap \text{polylog}(n)$ is a parameter that will determine the security of the ORAM (thus each bucket stores $K(\alpha + 2)$ words). A bucket may store 0 to $K$ valid tuples, and each empty slot in the bucket is denoted as $\text{Empty} = (\perp, \perp, \perp)$. We assume that all registers and memory cells are initialized with a special symbol $\perp$, and all buckets are initialized with $\text{Empty}$. The following is a specification of the $\text{OACCESS}(\text{loc}, \text{val})$ procedure:

\textbf{Update Position Map:} Pick a uniformly random leaf $\text{pos}' \leftarrow [n/\alpha]$

\textbf{Fetch:} Let $b = \lfloor \text{loc}/\alpha \rfloor$ be the block containing memory cell $\text{loc}$ (in the original database), and let $i = \text{loc} \mod \alpha$ be $\text{loc}$’s component within the block $b$. We first look up the position of the block $b$ using the
position map: \( \text{pos} = \text{Pos}(b) \) and let \( \text{Pos}(b) = \text{pos}' \); if \( \text{pos} = \perp \), then choose a uniformly random leaf \( \text{pos} \leftarrow \lfloor n/\alpha \rfloor \).

Next, traverse the data tree from the root to the leaf \( \text{pos} \), making exactly one \text{READ} and one \text{WRITE} operation for the memory bucket associated with each of the nodes along the path. More precisely, we read the content once, and then we either write it back (unchanged), or we simply “erase it” (writing \( \perp \)) so as to implement the following task: search for a tuple of the form \((b, \text{pos}, v)\) for the desired \(b, \text{pos}\) in any of the nodes during the traversal; if such a tuple is found, remove it from its place in the tree and set \(v\) to the found value, and otherwise set \(v = \perp\). Finally, return the \(i\)th component of \(v\) as the output of the \text{OACCESS}(\text{loc}, \text{val})\) operation.

### Put Back:
If \(\text{val}\) is not \(\perp\) (which means this is a \text{WRITE}), let \(v'\) be the string \(v\) but the \(i\)th component is set to \(\perp\). Otherwise, let \(v' = v\). Add the tuple \((b, \text{pos}', v')\) to the root \(\epsilon\) of the tree. If there is not enough space left in the root bucket, abort and output \text{overflow}.

### Flush:
Pick a uniformly random leaf \(\text{pos}'' \leftarrow \lfloor n/\alpha \rfloor\) and traverse the tree from the root to the leaf \(\text{pos}''\), making exactly one \text{READ} and one \text{WRITE} operation for every memory cell associated with the nodes along the path so as to implement the following task: “push down” each tuple \((b, \text{pos}, v)\) that reads in the nodes traversed so far as possible along the path to \(\text{pos}''\) while ensuring that the tuple is still on the path to its associated leaf \(\text{pos}\) (that is, the tuple ends up in the node \(\gamma = \text{longest common prefix of pos and pos}''\)). Note that this operation can be performed trivially as long as the CPU has sufficiently many work registers to load two whole buckets into memory; since the bucket size is polylogarithmic, this is possible. If at any point some bucket is about to overflow, abort and output \text{overflow}.

We overloaded the second parameter of \text{OACCESS} to replace both \text{READ} and \text{WRITE} with the special symbol \(\perp\) in the “Put Back” steps. Note that with all input including \(\text{val} = \perp\), \text{OACCESS} always outputs the original memory content of the memory cell \(\text{loc}\); this feature will be useful in the “full-fledged” construction.

#### 8.2.2 The full-fledged construction: ORAM with polylog registers

The full-fledged construction of the CP ORAM proceeds as above, except that instead of storing the position map in registers in the CPU, we now recursively store them in another ORAM (which only needs to operate on \(n/\alpha\) memory cells, but still using buckets that store \(K\) tuples). Recall that each invocation of \text{OACCESS} requires reading one position in the position map and updating its value to a random leaf; that is, we need to perform a single recursive \text{OACCESS} call (recall that \text{OACCESS} updates the value in a memory cell, and returns the old value) to emulate the position map.

At the base of the recursion, when the position map is of constant size, we use the trivial ORAM construction which simply stores the position map in the CPU registers.

#### 8.2.3 Notations for CP ORAM compilation

We use CP-\text{ORAM.}\{\text{Compile, Eval}\} to denote the CP ORAM scheme described above, where \text{Compile} and \text{Eval} denote the compilation and evaluation algorithms respectively. As mentioned before, the CP ORAM can compile a given RAM program \(P\) into a new RAM program \(P_o\) by replacing the memory access instructions with the oblivious memory access algorithm \text{OACCESS}; we now write

\[
P_o = \text{CP-ORAM.Compile}(P, \text{OACCESS})
\]

We next represent the oblivious access pattern algorithm in [CP13], \text{OACCESS}\{\text{K}_N\} in Algorithm 16. The involved randomness is produced by invoking \text{PRF} with a key \(\text{K}_N\) and the time parameter \(t\). If not specified, we use \text{OACCESS} instead of \text{OACCESS}\{\text{K}_N\} for simplicity. Other detailed routines are abstracted as follows:

55
PATH($d, pos$) outputs the path $I$ from root $\epsilon$ to leaf $pos$ in the $d$th ORAM tree $\Gamma_d$, where $d$ is the recursion level of OACCESS.

FETCHANDUPDATE($B_{\text{fetch}}$, $\text{loc, val, } \alpha, pos, newpos$) performs the “Fetch” and “Put Back” steps.

FLUSH($B_{\text{flush}}$, pos$''$) performs “Flush” steps from tree root to leaf pos$''$. We remark that there is a negligible probability (w.r.t. bucket size $K$) that overflow occurs at this step. For simplicity, we just assume that OACCESS is supplied with a “good” randomness

32

We remark that OACCESS initializes the memory during the compilation, and the compiled program is still a RAM program. Therefore the evaluation algorithm Eval is a standard evaluation algorithm for RAM programs. In addition, we could be able to construct a simulation algorithm SIMOACCESS to generate statistically indistinguishable memory access pattern, and define a simulated RAM program $P_{o,\text{sim}}$ based on SIMOACCESS, and we write

$$P_{o,\text{sim}} = \text{CP-ORAM.\text{Compile(SIMOACCESS)}}$$

We note that the simulated access pattern is independent of the original program $P$.

Algorithm 16: OACCESS{$K_N$}; the recursive ORAM accessing function

<table>
<thead>
<tr>
<th>Input</th>
<th>t, d, loc, val</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output</td>
<td>oldval</td>
</tr>
<tr>
<td>Data</td>
<td>$K_N, \alpha, \text{MaxDepth}$ (Memory size $S = \alpha^{\text{MaxDepth}}$)</td>
</tr>
</tbody>
</table>

1. if $d \geq \text{MaxDepth}$ then
2. return 0
3. Pick leaf newpos at recursion level $d$ based on PRF($K_N, (t, d, \text{FetchR})$);
4. $I_{\text{fetch}} \leftarrow \text{PATH}(d, \text{pos})$;
5. $B_{\text{fetch}} \leftarrow \text{READ}(I_{\text{fetch}})$;
6. ($B_{\text{out}}^{\text{fetch}}, \text{oldval}$) $\leftarrow$ FETCHANDUPDATE($B_{\text{fetch}}, \text{loc, val, } \alpha, pos, newpos$);
7. WRITE($I_{\text{fetch}}, B_{\text{out}}^{\text{fetch}}$);
8. Pick leaf pos$''$ at recursion level $d$ based on PRF($K_N, (t, d, \text{FlushR})$);
9. $I_{\text{flush}} \leftarrow \text{PATH}(d, pos'')$;
10. $B_{\text{flush}} \leftarrow \text{READ}(I_{\text{flush}})$;
11. $B_{\text{out}}^{\text{flush}} \leftarrow \text{FLUSH}(B_{\text{flush}}, pos'')$;
12. WRITE($I_{\text{flush}}, B_{\text{out}}^{\text{flush}}$);
13. return oldval;

8.2.4 ORAM compilation of a computation system

Next, we describe how to use CP-ORAM to compile a computation system. We overload the notations above and for a given next-step program, we also write

$$F_o = \text{CP-ORAM.\text{Compile}}(F, \text{OACCESS})$$

Given a RAM computation system $\Pi = ((\text{mem}^0, \text{st}^0), F)$, we compile it into $\Pi_o$ as follows. First, the compilation runs OACCESS to initialize mem$^0_o$ for each non-empty memory cell in mem$^0$, and sets st$^0_o = \text{Init}$. 

32 If the honest encoding overflowed, then an adversary could distinguish that from a simulated one. However, the overall probability to distinguish the honest is still negligible because the probability to overflow is negligible.

56
Then the compilation transforms next-step program $F$ into a new next-step program $F_o$. Finally it outputs $\Pi_o := ((\text{mem}_0^0, \text{st}_0^0), F_o)$. We abuse the notation again, and write

$$\Pi_o = \text{CP-ORAM}.\text{Compile}(\Pi, \text{OACCESS})$$

Similarly, based on SIMOACCESS, we can define $F_{o, sim}$ and write

$$F_{o, sim} = \text{CP-ORAM}.\text{Compile}($$

Complied next-step program $F_o$. For readability, we present $F_o$ as a stateful, next-step program that reads or writes a complete ORAM tree path (rather than one memory cell) in each round, while the locations of memory cells on this path are denoted with a vector $I$, as follows:

$$(\text{st}^{\text{out}}, \text{I}^{\text{out}}, B^{\text{out}}) \leftarrow F_o(t, \text{st}^{\text{in}}, I^{\text{in}}, B^{\text{in}})$$

Here $F_o$ takes as input, round counter $t$ of the given program $F$, state $\text{st}^{\text{in}}$, a vector of input locations $I^{\text{in}}$, a vector of input values $B^{\text{in}}$, and outputs state $\text{st}^{\text{out}}$, a vector of output locations $I^{\text{out}}$, a vector of output values $B^{\text{out}}$. We note that the efficiency does not suffer too much in this vectorized notation because any path in the ORAM tree has length $\log(n)$, and it is straightforward to transform it to a cell-wise function. ORAM compiled program has a multiplicative overhead $q_o$ in computation time. We denote the time counter of program $F$ as $t$ and denote the time counter of $F_o$ as $t$, where $t = \lceil t/q_o \rceil$. In the remaining of this section (Section 8), Both time metrics are used when simulating access patterns.

We further abuse the notation of the READ and WRITE operations in OACCESS such that they now work on vector of locations $I$ and values $B$. In particular, $F_o$ has the following output cases:

1. A round with no READ nor WRITE memory command outputs both $I$ and $B$ as an empty set.
2. A round with READ memory command outputs $I$ as a vector of locations to read and $B$ as an empty set.
3. A round with WRITE memory command outputs $I$ as a vector of locations to write and $B$ as a vector of values to write.

8.3 Construction for $\mathcal{RE}$-RAM

A randomized encoding of a computation instance $(P, x)$ hides everything about the computation instance except its output $y = P(x)$ and runtime $t^*$. This requires hiding both the content and the access pattern of the computation. We follow a natural construction idea: we use public-key encryptions to hide the content (including the input) and oblivious RAM to hide the access pattern, and then use $\text{CiO}$ to obfuscate the compiled computation instance. Namely, our $\mathcal{RE}$ encoding algorithm outputs $\text{CiO}(\Pi_{\text{hide}})$ as the encoding, where $\Pi_{\text{hide}}$ is defined by $P_{\text{hide}}$ and $x_{\text{hide}}$. $P_{\text{hide}}$ is a $\mathcal{PKE}$ and ORAM compiled version of $P$, and $x_{\text{hide}}$ is an encrypted version of $x$. Namely, $P_{\text{hide}}$ outputs encrypted CPU states and memory contents at each time step, and uses ORAM to compile its memory access.

More concretely, our construction of $\mathcal{RE}$ in the RAM model is split into four major steps: (i) given a RAM program $P$ and its input $x$, we interpret it as a RAM computation $\Pi$; (ii) we compile $\Pi$ into $\Pi_o$ using CP ORAM compiler to hide the access pattern; (iii) we transform $\Pi_o$ into $\Pi_e$, which further hides the content in the computation system; and (iv) we obfuscate $\Pi_e$ into $\text{ENC}$ using $\text{CiO}$ for RAM. Formally, we construct our $\mathcal{RE} = \mathcal{RE}.\{\text{Encode}, \text{Decode}\}$ for the RAM program $P$ and input $x$ as follows:
The encoding algorithm takes the following steps to generate the encoding $\text{ENC}$.

- Upon receiving the description of RAM program $P$ and an input value $x$, first, the encoding algorithm transforms them into a computation system. It represents $P$ into a next-step program $F$, and stores $x$ into the memory, i.e., sets $\text{mem}^0 := x$. Then it sets $\text{st}^0 := \text{Init}$, and defines the following computation system in the RAM model:

$$\Pi = ((\text{mem}^0, \text{st}^0), F)$$

- Second, the encoding algorithm hides the access pattern in the computation system. It randomly chooses puncturable PRF key $K_N \leftarrow \text{PPRF}\text{-Setup}(1^\lambda)$. Then it runs the CP-ORAM compilation described in Section 8.2, i.e., $\Pi_o = \text{CP}\text{-ORAM}\text{.Compile} (\Pi, \text{OACCESS}\{K_N\})$ and obtains $\Pi_o = ((\text{mem}^0, \text{st}^0)_o, F_o)$

- Third, the encoding algorithm further hides the content in the memory and in the CPU state. That is, it transforms $\Pi_o$ into $\Pi_e = ((\text{mem}^0, \text{st}^0)_e, F_e)$

Here the encoding algorithm randomly chooses puncturable PRF key $K_E \leftarrow \text{PPRF}\text{-Setup}(1^\lambda)$, and generates an initial configuration of the encrypted version of memory and CPU state as follows:

To initialize memory $\text{mem}^0$, the encoding algorithm parses $\text{mem}^0$ as ORAM trees $\{\Gamma\}$, and for each $\Gamma$ it further parses all paths $I$ from root to leaf. For each path $(I, B)$ with its index $I$ and buckets $B$, the encoding algorithm computes

$$(r_1^0, r_2^0) = \text{PRF}(K_E, (Iw^0, h(I))) \text{ where } Iw^0 = 0,$$

$$(pk^0, sk^0) = \mathcal{PK}\text{\text{-Gen}}(1^\lambda; r_0^0),$$

$$\begin{cases} \mathcal{PK}\text{\text{-Encrypt}}(pk^0[i], B[i]), & \text{if } B[i] \text{ stores any valid block} \\ B[i], & \text{otherwise,} \end{cases}$$

where $h$ is a function to compute the “height” of elements in vector $I$. That is, for any vector $I$ of length $|I|$, define $h(I) = (1, 2, \ldots, |I|)$. For each non-empty encrypted bucket $B[i]$, store $(B[i], 0)$ to its corresponding location $I[i]$ in $\text{mem}^0$, which are the encrypted ORAM trees. Because many buckets are empty and never touched while OACCESS initializes $\text{mem}^0$, we represent $\text{mem}^0$ and $\text{mem}^0$ in sparse arrays for efficiency, where only those non-empty buckets are stored and processed with encryption. Therefore, the encoding time and space of $\text{mem}^0$ are both efficient.

In addition, the encoding algorithm computes $(r_3^0, r_4^0) = \text{PRF}(K_E, 0), (pk_{st}, sk_{st}) = \mathcal{PK}\text{\text{-Gen}}(1^\lambda; r_3^0)$, and $\text{st}^0 \leftarrow \mathcal{PK}\text{\text{-Encrypt}}(pk_{st}, \text{st}_0^0)$. Then it sets $\text{st}_e^0 = (\text{st}_0^0, 0)$.

The encoding algorithm then upgrades $F_o$ into a more sophisticated next-step program $F_e$ which decrypts its inputs, performs the computation of $\Pi_o$, and encrypts its outputs. Please refer to Algorithm 17 for more details of $F_e$. Because there are non-encrypted empty buckets in $\text{mem}^0$, the procedure $\mathcal{PK}\text{\text{-Encrypt}}$ to decrypt $B^\text{in}$ in $F_e$ is augmented to ignore any empty bucket in $\text{mem}^0$, that is for each $i$

$$B^\text{in}[i] = \begin{cases} \mathcal{PK}\text{\text{-Encrypt}}(sk[i], B^\text{in}[i]), & \text{if } B^\text{in}[i] \neq \text{empty bucket} \\ B^\text{in}[i], & \text{otherwise.} \end{cases}$$

This technique is applied to eliminate the dependency of memory size $S$ from the complexity of encoding size and time, and we summarize it in Table 4.

Note that $F_e$ (Algorithm 17) abuses the notation of PRF, $\mathcal{PK}\text{\text{-Gen}}$, $\mathcal{PK}\text{\text{-Encrypt}}$, $\mathcal{PK}\text{\text{-Decrypt}}$, which computes on a vector of inputs and returns a vector of outputs. Please refer to Section 8.1 for formal description.

- Finally, the encoding algorithm computes $\text{ENC} \leftarrow \mathcal{CiO}\text{\text{-Obf}}(1^\lambda, \Pi_e)$ and outputs $\text{ENC}$.  

58
Table 4: Techniques to improve encoding efficiency.

<table>
<thead>
<tr>
<th>Observation</th>
<th>Technique to encode input efficiently</th>
<th>Corresponding shorthand in program $F_e$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input data in ORAM tree structure is sparse</td>
<td>Encrypt only those buckets have data</td>
<td>For each encrypted bucket $B_i$, decrypt ciphertext except empty bucket</td>
</tr>
</tbody>
</table>

**Decoding algorithm** $y \leftarrow \mathcal{RE}.\text{Decode}(\text{ENC}, 1^\lambda, T, S)$: Upon receiving the encoding $\text{ENC}$, the decoding algorithm executes $\text{CiO.Eval(ENC)}$. If the decoding algorithm does not terminate in $T$ steps, then it outputs $y := \bot$. Otherwise, if it terminates at step $t^*$, and obtains $(\widetilde{\text{mem}}_{t^*}, \widetilde{\text{st}}_{t^*})$ where $\widetilde{\text{st}}_{t^*} = (\text{halt}, y)$ then it outputs $y$.

It is straightforward to verify the correctness of the above construction. Next, we describe the efficiency and then present a theorem for its security.

**Efficiency.** Let $|F|$ be the description size of program $F$, $n$ be the size of input $x$, $F$ computes on $x$ with time and space bound $T$ and $S$. Assuming $\text{CiO}$ has compilation time $O(\text{poly}(|F|) + n \log S)$, ciphertext size $O(\text{poly}(|F|) + n)$, evaluation time $O(\log S)$ multiplicative, and evaluation space proportional to $S$. Observing only constant amount of information is hardwired throughout our security proof (Section B.5), our $\mathcal{RE}$ has following complexity:
- Encoding time is $\tilde{O}(\text{poly}|F| + n)$.
- Encoding size is $\tilde{O}(\text{poly}|F| + n)$.
- Decoding time is $\tilde{O}(T \cdot \text{poly}(|F|))$.
- Decoding space is $\tilde{O}(S)$.

**Security.** We now prove the following theorem that the randomized encoding scheme $\mathcal{RE}$ described above is secure. Please refer to Section A.2 for the security definition of randomized encoding scheme.

**Theorem 8.1.** Let $\mathcal{PKE}$ be an IND-CPA secure public key encryption scheme, $\text{CiO}$ be a computation-trace indistinguishability obfuscation scheme in RAM model, PRF be a secure puncturable PRF scheme. Then $\mathcal{RE}$ is a secure randomized encoding scheme.

The security proof can be found in Section B.5.

9 Constructing $\mathcal{RE}$ in the PRAM Model ($\mathcal{RE}$-PRAM)

In this section, we describe our construction of randomized encoding for PRAM ($\mathcal{RE}$-PRAM). As $\mathcal{RE}$-RAM, the main goal of $\mathcal{RE}$-PRAM is to hide states and memory access pattern. Recall the construction of $\mathcal{RE}$-RAM in Section 8 based on $\text{CiO}$ for RAM, tree-based ORAM, and $\mathcal{PKE}$. Naturally, we use $\text{CiO}$ for PRAM, tree-based oblivious PRAM (OPRAM) and $\mathcal{PKE}$ as building blocks to achieve $\mathcal{RE}$ simulation security.

Our $\mathcal{RE}$-PRAM construction works as follows.
- We first use OPRAM compiler to hide the access pattern. Given a computation instance $\Pi$ defined by $(P, x)$, we compile $P$ using an OPRAM compiler with randomness supplied by a puncturable PRF. Let $P_{\text{OPRAM}}$ denote the compiled program. We also initiate the OPRAM memory by inserting the input $x$. Let $x_{\text{OPRAM}}$ denote the resulting memory.
Algorithm 17: \( F_e \)

\( \text{Input}: \tilde{\text{st}}^\text{in} = (\text{st}^\text{in}, t), \tilde{\text{a}}_{\text{st-M}}^\text{in} = (\text{I}^\text{in}, (\text{B}^\text{in}, \text{lw}^\text{in})) \)

\( \text{Data}: T, K_E, K_N \)

1. Compute \( t = \lceil t/q_0 \rceil \); // \( q_0 \) is the ORAM compilation overhead
2. Compute \( (r_1^\text{in}, r_2^\text{in}) = \text{PRF}(K_E, (\text{lw}^\text{in}, h(\text{I}^\text{in}))) \); // For any vector \( \text{I} \) of length \( |\text{I}| \), define \( h(\text{I}) = (1, 2, \ldots, |\text{I}|) \)
3. Compute \( (\text{pk}^\text{in}, \text{sk}^\text{in}) = \mathcal{PKE}.\text{Gen}(1^\lambda; r_1^\text{in}) \);
4. Compute \( \text{B}^\text{in} = \mathcal{PKE}.\text{Decrypt}(\text{sk}^\text{in}, \text{B}^\text{in}) \);
5. Compute \( (r_3^{t-1}, r_4^{t-1}) = \text{PRF}(K_E, t - 1) \);
6. Compute \( (\text{pk}'_{\text{st}}, \text{sk}'_{\text{st}}) = \mathcal{PKE}.\text{Gen}(1^\lambda; r_3^{t-1}) \);
7. Compute \( \text{st}^\text{in} = \mathcal{PKE}.\text{Decrypt}(\text{sk}'_{\text{st}}, \text{st}^\text{in}) \);
8. Compute \( (\text{st}^\text{out}, \text{I}^\text{out}, \text{B}^\text{out}) = F_0(t, \text{st}^\text{in}, \text{I}^\text{in}, \text{B}^\text{in}) \);

9. Set \( \text{lw}^\text{out} = (t, \ldots, t) \);
10. Compute \( (r_1^\text{out}, r_2^\text{out}) = \text{PRF}(K_E, (\text{lw}^\text{out}, h(\text{I}^\text{out}))) \);
11. Compute \( (\text{pk}'_{\text{out}}, \text{sk}'_{\text{out}}) = \mathcal{PKE}.\text{Gen}(1^\lambda; r_1^\text{out}) \);
12. Compute \( \text{B}^\text{out} = \mathcal{PKE}.\text{Encrypt}(\text{pk}'_{\text{out}}, \text{B}^\text{out}, r_2^\text{out}) \);
13. if \( \text{st}^\text{out} \neq (\text{halt}, \cdot) \) then
   14. \( \text{Compute } (r_3', r_4') = \text{PRF}(K_E, t) \);
   15. \( \text{Compute } (\text{pk}', \text{sk}') = \mathcal{PKE}.\text{Gen}(1^\lambda; r_3') \);
   16. \( \text{Compute } \text{st}'_{\text{out}} = \mathcal{PKE}.\text{Encrypt}(\text{pk}', \text{st}^\text{out}; r_4') \);
17. else
   18. \( \text{Output } \tilde{\text{st}}^\text{out} = \text{st}^\text{out} \)
19. \( \text{Output } \tilde{\text{st}}^\text{out} = (\text{st}^\text{out}, t + 1), \tilde{\text{a}}_{\text{st-M}}^\text{out} = (\text{I}^\text{out}, (\text{B}^\text{out}, \text{lw}^\text{out})) \);
We then compile \((P_{OPRAM}, x_{OPRAM})\) using \(PKE\) in the same way as in the RAM version above. Namely, we use PPRF to generate multiple keys, and use each key to encryption a single message, including the input \(x_{OPRAM}\). Denote the resulting instance by \((P_{hide}, x_{hide})\).

The randomized encoding of computation instance \(\Pi\) is \(\tilde{\Pi} = CiO(\Pi_{hide})\), where \(CiO(\Pi_{hide})\) is defined by \((P_{hide}, x_{hide})\).

To build \(RE\)-PRAM, we use the oblivious PRAM compiler by Boyle, Chung, and Pass \([BCP14b]\) (BCP-OPRAM) and the other building blocks which are identical to Section 8.1. The security proof of the \(RE\)-PRAM construction also follows identical steps, where we prove the security by a sequence of hybrids that erases the computation backward in time, and argue simulation of access patterns by generalizing the puncturing ORAM argument to puncturing BCP-OPRAM. However, there are two natural issues in the arguments of generalization. (i) As the OPAccess algorithm of BCP-OPRAM is more complicated, we need to be slightly careful in defining the simulated encoding \(CiO(P_{Sim}, x_{Sim})\). (ii) To avoid dependency on the number \(m\) of CPUs, we need to gradually handle a single CPU at a time in the hybrids to puncture ORAM.

**Section Outline.** We will review BCP-OPRAM compilation technique in the next subsection. Then, the construction of \(RE\) for PRAM and its proof sketch will be shown in Section 9.2 and Section B.6.

### 9.1 Recap: The BCP-OPRAM

For hiding access pattern, the security of our \(RE\) for PRAM must rely heavily on oblivious PRAM (OPRAM) as a building block. We first briefly review BCP’s OPAccess \([BCP14b]\), and then show its puncturability property similar to that of OACCESS where the randomness is generated from a PPRF.

**The BCP OPRAM Construction.** The OPRAM compiler, on input \(m, n \in \mathbb{N}\) and an \(m\)-processor PRAM program \(P\) with memory size \(n\), outputs a program \(P'\) that is identical to \(P\), except that each access \((r, v)\) operation is replaced by a sequence of operations defined by subroutine OPAccess\((r, v)\), which is described as follows.

The OPAccess procedure begins with \(m\) CPUs, each requesting data cell \(r\) (within some block \(b\)) and some action to be taken (either \(\perp\) to denote read, or \(v\) to denote rewriting cell \(r\) with value \(v\)). The primary challenges in implementing oblivious parallel data accesses within the tree-based ORAM structure of \([SCSL11, CP13]\) are in handling collisions between processor accesses, and in reinserting data to the ORAM (and flushing data down the tree) in parallel. OPAccess addresses these challenges by the following sequence of tasks:

1. **Conflict Resolution:**
   - Choose one representative CPU per requested data block \(b\) (in the real database). This representative will perform the real data fetch and computation on \(b\) in later steps, while the other CPUs will simply make “dummy” accesses into the ORAM structure.
   - Aggregate all CPU instructions to take place on each requested block \(b\).

2. **Read/Write Position Map:**
   - Each representative CPU: Sample a fresh random leaf id \(\ell'\). Perform a (recursive) Read/Write access command on the position map database \(\ell \leftarrow \text{OPAccess}(b_i, \ell')\) to fetch the current position map value \(\ell\) and rewrite it with the newly sampled value \(\ell'\).
   - Each dummy CPU: Perform a dummy access to an arbitrary cell in the position map database, say the first. (Recall that the position map database is itself protected by a layer of ORAM). That is, execute \(\ell \leftarrow \text{OPAccess}(1, \emptyset)\), and ignore the read value \(\ell\).
3. **Look Up Current Memory Values**: Each representative CPU fetches memory from ORAM database nodes corresponding to accessing his desired data block \( b \) (i.e., the collection of buckets down the relevant path in the ORAM tree) and copies the values into local memory. Non-chosen CPUs choose a random path \( \ell \) (independent of the position map above) and make analogous dummy data fetches along the path to \( \ell \), ignoring all read values. Recall that simultaneous data reads do not yield conflicts.

4. **Remove Old Data**: Consider the paths down the ORAM tree accessed in the previous step.
   - Aggregate instructions across CPUs accessing the same “buckets” of memory on the server side. Each representative CPU \( \text{rep}(b) \) begins with the instruction of “remove block \( b \) if it occurs” and dummy CPUs hold the empty instruction. (Aggregation is as before, but at bucket level instead of the block level).
   - For each bucket to be modified, the CPU with the *smallest* id from those who wish to modify it executes the aggregated block-removal instructions for the bucket.

5. **Insert Updated Data into Database in Parallel**: All CPUs execute a parallel insertion procedure into the ORAM database at the appropriate level (corresponding to the number of active CPUs) in order to insert the updated data tuples \((b, \ell', v')\) with new leaf node \( \ell' \) as sampled in Step 1 and new value \( v' \) into the bucket along the path to \( \ell' \).

6. **Flush the ORAM Database**: In parallel, each CPU initiates an independent flush of the ORAM tree. (Recall that this corresponds to selecting a random path down the tree, and pushing all data blocks in this path as far as they will go). To implement the simultaneous flush commands, as before, commands are aggregated across CPUs for each bucket to be modified, and the CPU with the smallest id performs the corresponding aggregated set of commands. (For example, all CPUs will wish to access the root node in their flush; the aggregation of all corresponding commands to the root node data will be executed by the lowest-numbered CPU who wishes to access this bucket, in this case CPU 1).

7. **Return Output**: Each representative CPU \( \text{rep}(b) \) communicates the *original* value of the data block \( b \) to the subset of CPUs that originally requested it.

As a result, the BCP-OPRAM compiler enjoys the same advantages with CP-ORAM by finishing the above tasks. Intuitively, CP-ORAM and BCP-OPRAM must have the same property, puncturability.

**Puncturability of BCP-OPRAM.** In the above OPAccess, observe that the location to be looked up (in step 3) only depends on the previous fresh random sample \( \ell' \) (in step 2). Therefore, if previous random sample \( \ell' \) is information-theoretically hidden, the look up step can be simulated. Specifically, the punctured OPRAM program erases that block \( \text{blk}^* \) containing \( \ell' \) at that time step \( \ell' \) such that \( \ell' \) is generated by PPRF and does not recursively write \( \ell' \) to the position map. With this punctured OPRAM (and PPRF key punctured at the corresponding point of \( \ell' \)), the step looking for \( \text{blk}^* \) can be simulated indistinguishably with a uniformly random ORAM tree path. Hence, BCP-OPRAM achieves puncturability similar to that of ORAM described in Section B.5.4.

9.2 **Construction for \( \mathcal{RE} \)-PRAM**

A randomized encoding of a computation instance \((P, x)\) hides both the content and the access pattern of the computation except for its output \( y = P(x) \) and runtime \( t^* \). Conceptually, we follow the same natural idea to use public-key encryption to hide the content (including the input) and oblivious PRAM to hide the access pattern, and then use CiO for PRAM to obfuscate the compiled computation instance. Namely, our \( \mathcal{RE} \) encoding algorithm outputs CiO\((\Pi_{\text{hide}})\) as the encoding, where \( \Pi_{\text{hide}} \) is defined by \((P_{\text{hide}}, x_{\text{hide}})\), \( P_{\text{hide}} \) is
a \mathcal{PKE} and OPRAM compiled version of \( P \), and \( x_{\text{hide}} \) is an encrypted version of \( x \). \( P_{\text{hide}} \) outputs encrypted CPU states and memory contents at each time step, and uses OPRAM to compile its memory access.

Our construction of \( \mathcal{RE} \) in the PRAM model is split into four major steps: (i) given a PRAM program \( P \) and its input \( x \), we interpret it as a PRAM computation \( \Pi \); (ii) we compile \( \Pi \) into \( \Pi_o \) using BCP OPRAM compiler to hide the access pattern; (iii) we transform \( \Pi_o \) into \( \Pi_c \), which further hides the content in the computation system; and (iv) we finally obfuscate \( \Pi_c \) into \( \mathcal{ENC} \) using CiO-OPRAM. Formally, we construct our \( \mathcal{RE} = \mathcal{RE}.\{\text{Encode, Decode}\} \) for the RAM program \( P \) and input \( x \) as follows:

**Encoding algorithm** \( \text{ENC} \leftarrow \mathcal{RE}.\text{Encode}(P, x, 1^\lambda) \): The encoding algorithm takes the following steps to generate the encoding \( \text{ENC} \).

- **Upon receiving the description of PRAM program \( P \) and an input value \( x \), first, the encoding algorithm transforms them into a computation system \( \Pi \). It represents \( P \) into a next-step program \( F \), and stores \( x \) into the memory, i.e., sets \( \text{mem}^0 := x \). Then it sets \( \text{st}^0_k := \perp \) for all \( k, 1 \leq k \leq m \), and then defines the following computation system in the PRAM model
  \[
  \Pi = ((\text{mem}^0, \{\text{st}^0_{k,1}\}_{k=1}^m), F)
  \]

- Second, the encoding algorithm hides the access pattern in the computation system. It chooses puncturable PRF key \( K_N \leftarrow \text{PPRF.Setup}(1^\lambda) \). Then it runs the BCP-OPRAM compilation described in Section 9.1, i.e., \( \Pi_o = \text{BCP-OPRAM.Compile}(\Pi, \text{OPAccess}(K_N)) \) and obtains
  \[
  \Pi_o = ((\text{mem}^0, \{\text{st}^0_{o,k}\}_{k=1}^m), F_o)
  \]
  where \( \text{st}^0_{o,k} = \text{st}^0_k \) such that all CPUs have the same OPRAM state.

- Third, the encoding algorithm further hides the content in the memory and in the CPU state. That is, it transforms \( \Pi_o \) into
  \[
  \Pi_c = ((\text{mem}^0, \{\text{st}^0_{c,k}\}_{k=1}^m), F_c)
  \]

Here the encoding algorithm chooses puncturable PRF key \( K_E \leftarrow \text{PPRF.Setup}(1^\lambda) \), and generates an initial configuration of the encrypted version of memory and CPU state as follows:

To initialize memory \( \text{mem}^0_c \), the encoding algorithm parses \( \text{mem}^0_o \) as trees \( \Gamma \), and then for each \( \Gamma \) it further parses all paths \( \Gamma \) from root to leaf. For each vector \( \Gamma \), the encoding algorithm computes

\[
\begin{align*}
(r^0_1, r^0_2) &= \text{PRF}(K_E, (\text{l}w^0, h(\Gamma))) \text{ where } \text{l}w^0 = \mathbf{0}, \\
(p^0_k, s^0_k) &= \mathcal{PKE}.\text{Gen}(1^\lambda; r^0_k), \quad \text{if } \mathbf{B}[i] \text{ stores any valid block} \\
\mathbf{B}[i] &= \begin{cases} \mathcal{PKE}.\text{Encrypt}(p^0_k[i], \mathbf{B}[i]), & \text{if } \mathbf{B}[i] \text{ stores any valid block} \\
\mathbf{B}[i], & \text{otherwise}
\end{cases}
\end{align*}
\]

where \( \mathbf{B}[i] \) denotes the \( i \)-th element (which is also a bucket here) in vector \( \mathbf{B} \), and \( h \) is a function to compute the “height” of elements in vector \( \Gamma \). That is, for any vector \( \Gamma \) of length \( |\Gamma| \), define \( h(\Gamma) = (1, 2, \ldots, |\Gamma|) \). For each non-empty \( \mathbf{B} \), store \((\mathbf{B}, \text{l}w^0)\) to its corresponding path \( \Gamma \) in \( \text{mem}^0_c \).

In addition, the encoding algorithm sets \( \text{st}^0_{o,k} = \text{st}^0_{c,k} \) for all \( k \in [m] \). Note that each CPU holds the same non-encrypted \( \text{st}^0_{c,k} \) because \( \text{st}^0_k \) is only \( \perp \) for all \( k \). To work with such initialization, the procedure \( \mathcal{PKE}.\text{Decrypt}(\text{sk}_c, \cdot) \) to decrypt states (in \( F_c \)) is augmented to ignore non-encrypted special value \( \perp \) as follows:

\[
\text{st}^{\text{in}}_A = \begin{cases} 
\mathcal{PKE}.\text{Decrypt}(\text{sk}_c, \text{st}^{\text{in}}_A), & \text{if } \text{st}^{\text{in}}_A \neq \perp \\
\perp, & \text{otherwise}
\end{cases}
\]
These techniques are applied to eliminate the dependency of memory size $S$ and number of CPUs $m$ from the complexity of encoding size and time, and we summarize them in Table 5.

The encoding algorithm then upgrades $F_o$, into a more sophisticated next-step program $F_e$ which decrypts its inputs, performs the computation of $\Pi_o$, and decrypts its outputs. Please refer to Algorithm 18 for more details of $F_e$.

- Finally, the encoding algorithm computes $\text{ENC} \leftarrow \text{CiO.Obf}(1^\lambda, \Pi_e)$ and outputs $\text{ENC}$.

### Table 5: Techniques to improve encoding efficiency.

<table>
<thead>
<tr>
<th>Observation</th>
<th>Technique to encode input efficiently</th>
<th>Corresponding shorthand in program $F_e$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input data in ORAM tree structure is sparse</td>
<td>Encrypt only those buckets have data</td>
<td>For each encrypted bucket $B_{1,2}^{\text{in}}$, decrypt ciphertext except empty bucket</td>
</tr>
<tr>
<td>All $m$ initial CPU states are the same empty value</td>
<td>Leave the state in plaintext</td>
<td>Decrypt ciphertext $\text{st}_{1,2}^{\text{in}}$ except empty state</td>
</tr>
</tbody>
</table>

**Decoding algorithm** $y \leftarrow \mathcal{RE}.\text{Decode(ENC, 1^\lambda, T, S)}$: Upon receiving the encoding $\text{ENC}$, the decoding algorithm executes $\text{CiO.Eval(ENC)}$. If the decoding algorithm does not terminate in $T$ steps, then it outputs $y := \bot$. Otherwise, if it terminates at step $t^*$, and obtains $(\text{mem}^{t^*}, \text{st}_{1}^{t^*})$ where $\text{st}_{1}^{t^*} = (\text{halt}, y)$ then it outputs $y$ by cpu 1.

**Efficiency.** Let $|F|$ be the description size of program $F$, $n$ be the description size of initial memory $\text{mem}^0$, $m$ be the total number of CPUs, $T$ and $S$ be time and space bound. According to $\text{CiO}$ for PRAM, assume that $\text{CiO}$ has encoding time $O(\text{poly}(|F| + \log m) + n \log S)$ and ciphertext size $O(\text{poly}(|F| + \log m) + n)$, and parallel decoding time $O(T \cdot \text{poly}(|F| + \log m) \log S)$ and space $O(m + S)$. However, there remains OPRAM computation overhead $\text{poly} \log m \text{poly} \log S$ and space overhead $\omega(\log S)$. Finally, our $\mathcal{RE}$ has following complexity:

- Encoding time is $\tilde{O}(\text{poly}(|F| + n))$.
- Encoding size is $\tilde{O}(\text{poly}(|F| + n))$.
- Parallel decoding time is $\tilde{O}(T \cdot \text{poly}(|F|))$.
- Decoding space is $\tilde{O}(m + S)$.

**Security.** We prove the following theorem that the randomized encoding scheme $\mathcal{RE}$ described above is secure. Please refer to Section A.2 for the security definition of randomized encoding scheme.

**Theorem 9.1.** Let $\mathcal{PKE}$ be a semantically-secure public key encryption scheme, $\text{CiO}$ be a computation-trace indistinguishability obfuscation scheme in PRAM model, PRF be a secure puncturable PRF scheme. Then $\mathcal{RE}$ is a secure randomized encoding scheme in the PRAM model.

The proof sketch can be found in Section B.6.
Algorithm 18: \( F_e \) in \( \mathcal{RE} \)-PRAM

\[
\text{Input} : \overline{\text{st}}_{\text{in}} = (\text{A}, \text{st}_{\text{in}}^\text{A}, t), \overline{\text{st}}_{\text{in}} = (\text{I}_A^\text{in}, (B_A^\text{in}, \text{lw}_A^\text{in}))
\]

\[
\text{Data} : T, K_E, K_N
\]

1. Compute \( t = \lceil t/\alpha \rceil \);
2. Compute \( (r_1^\text{in}, r_2^\text{in}) = \text{PRF}(K_E, (\text{lw}_A^\text{in}, h(I_A^\text{in}))) \);
3. Compute \( (pk^\text{in}, sk^\text{in}) = \mathcal{PE}.\text{Setup}(1^\lambda; r_1^\text{in}) \);
4. Compute \( B_A^* = \mathcal{PE}.\text{Decrypt}(sk^\text{in}; B_A^\text{in}) \);
5. Compute \( (r_3^t, r_4^t) = \text{PRF}(K_E, t - 1) \);
6. Compute \( (pk_{\text{st}}, sk_{\text{st}}) = \mathcal{PE}.\text{Setup}(1^\lambda; r_3^t) \);
7. Parse \( \text{st}_{\text{in}}^\text{A} \) as \( (\text{st}_{\text{in}}^\text{A||st}_{\text{in}}^\text{A}) \);
8. Compute \( \text{st}_{\text{in}}^\text{A} = \mathcal{PE}.\text{Decrypt}(sk_{\text{st}}, \text{st}_{\text{in}}^\text{A}) \);
9. Set \( \text{st}_{\text{in}}^\text{A} = (\text{st}_{\text{in}}^\text{in||st}_{\text{in}}^\text{A}) \);
10. Compute \( r_N = \text{PRF}(K_N, t) \);
11. Compute \( (\text{st}_{\text{out}}^\text{A}, \text{I}_A^\text{out}, B_A^\text{out}) = F_0(t, \text{A}, \text{st}_{\text{in}}^\text{A}, \text{I}_A^\text{in}, B_A^\text{in}, r_N) \);
12. Parse \( \text{st}_{\text{out}}^\text{A} \) as \( (\text{st}_{\text{out}}^\text{A||st}_{\text{out}}^\text{A}) \);
13. Set \( \text{lw}_A^\text{out} = (t, \ldots, t) \);
14. Compute \( (r_1^\text{out}, r_2^\text{out}) = \text{PRF}(K_E, (\text{lw}_A^\text{out}, h(I_A^\text{out}))) \);
15. Compute \( (pk', sk') = \mathcal{PE}.\text{Setup}(1^\lambda; r_1^\text{out}) \);
16. Compute \( B_A^\text{out} = \mathcal{PE}.\text{Encrypt}(pk', B_A^\text{in}; r_2^\text{out}) \);
17. if \( \text{st}_{\text{out}}^\text{A} \neq (\text{halt,}.) \) then
18. \quad Compute \( (r_3^t, r_4^t) = \text{PRF}(K_E, t) \);
19. \quad Compute \( (pk', sk') = \mathcal{PE}.\text{Setup}(1^\lambda; r_3^t) \);
20. \quad Compute \( \text{st}_{\text{out}}^\text{A} = \mathcal{PE}.\text{Encrypt}(pk', \text{st}_{\text{out}}^\text{A}; r_4^t) \);
21. \quad Set \( \text{st}_{\text{in}}^\text{A} = (\text{st}_{\text{out}}^\text{A||st}_{\text{in}}^\text{A}) \);
22. else
23. \quad If all agents output \( \text{st}_{\text{out}}^\text{A} = (\text{halt,} Þ) \), then a special CPU agent returns the output \( y \);
24. \quad Else, \( A \) returns \( \text{st}_{\text{out}}^\text{A} \) as \( (\text{halt,}.) \);
25. Output \( \text{st}_{\text{out}}^\text{A} = (\text{A}, \text{st}_{\text{out}}^\text{A}, t + 1), \text{I}_A^\text{out} = (\text{I}_A^\text{out}, D_A^\text{out}) \), where \( D_A^\text{out} = (B_A^\text{out}, \text{lw}_A^\text{out}) \).
10 Extensions

In this section, we extend our results in previous sections to suit for several important scenarios of delegation of computations. One of our major extensions is to let \( \mathcal{RE} \) support persistent database (PDB). This can be achieved by first defining and constructing the corresponding variants of CiO with PDB. Next, recall that ordinary \( \mathcal{RE} \) only provides input and program privacy, and produces a short output in the clear. For practical scenarios of delegation of computation, other properties such as long output, output hiding and output verifiability may be desirable. Thus, we will demonstrate how we can obtain these extensions by possibly using other primitives such as encryption and signatures.

10.1 CiO with Persistent Database

In the persistent database setting, we consider an initial memory and a sequence of programs which work on the memory content processed and left over by the previous program. Recall that CiO in some sense forces the evaluator to evaluate an obfuscated program as intended to produce the intended computation trace. In the persistent database setting, we further require that the sequence of programs is executed in the intended order.

10.1.1 Definition

Let a computation system \( \Pi \in \mathcal{P} \) be composed of an initial database and many programs written as \( \Pi = (\text{mem}^{0,0}, \{F_{\text{sid}}\}_{l=1}^l) \) where \( \text{sid} \) denotes the session identity and \( l \) denotes the total number of programs. Each stateful function \( F_{\text{sid}} \) has its program and state hardwired. For simplicity, we adopt a convention that the label of the database and the state are set to 1) \((\text{sid} - 1, 0)\) at the beginning of session \( \text{sid} \), 2) \((\text{sid} - 1, i)\) where \( i \neq 0 \) in the duration of session \( \text{sid} \), and finally 3) \((\text{sid}, 0)\) in the termination stage.

**Definition 10.1** (CiO with Persistent Database). A computation-trace indistinguishability obfuscation scheme with persistent database w.r.t. \( \mathcal{P} \), denoted as CiO = CiO, \{DBCompile, Obf, Eval\}, is defined as follows:

**Database compilation algorithm** \( (\widetilde{\text{mem}}^{0,0}, \widetilde{\text{st}}^{0,0}) := \text{DBCompile}(1^\lambda, \text{mem}^{0,0}, \rho) \): DBCompile() is a probabilistic algorithm which takes as input the security parameter \( \lambda \), the database \text{mem}^{0,0} and some randomness \( \rho \), and returns the compiled database and state \((\widetilde{\text{mem}}^{0,0}, \widetilde{\text{st}}^{0,0})\) as output.

**Program compilation algorithm** \( \widetilde{F}_{\text{sid}} := \text{Obf}(1^\lambda, F_{\text{sid}}; \rho') \): Obf() is a probabilistic algorithm which takes as input the security parameter \( \lambda \), the stateful function \( F_{\text{sid}} \) and some randomness \( \rho' \), and returns a compiled / obfuscated function \( \widetilde{F}_{\text{sid}} \) as output.

**Evaluation algorithm** \( \text{conf} := \text{Eval}(\widetilde{\text{mem}}^{\text{sid} - 1,0}, \widetilde{\text{st}}^{\text{sid} - 1,0}, \widetilde{F}_{\text{sid}}) \): Eval() is a deterministic algorithm which takes as input \((\widetilde{\text{mem}}^{\text{sid} - 1,0}, \widetilde{\text{st}}^{\text{sid} - 1,0}, \widetilde{F}_{\text{sid}})\), and returns a configuration \( \text{conf} = (\text{mem}^{\text{sid} - 1,0}, \text{st}^{\text{sid} - 1,0}) \) as output.

**Correctness.** For all \( F_{\text{sid}} \) with termination time \( t'_{\text{sid}} \) and all randomness \( \rho' \), let \( \widetilde{F}_{\text{sid}} := \text{Obf}(1^\lambda, F_{\text{sid}}; \rho') \). It holds that \( \text{Eval}(\widetilde{\text{mem}}^{\text{sid} - 1,0}, \widetilde{\text{st}}^{\text{sid} - 1,0}, \widetilde{F}_{\text{sid}}) = \text{Conf}(\text{mem}^{\text{sid} - 1,0}, \text{st}^{\text{sid} - 1,0}, F_{\text{sid}}, t'_{\text{sid}}) \).

**Security.** For any (not necessarily uniform) PPT distinguisher \( D \), there exists a negligible function \( \text{negl}(\cdot) \) such that, for all security parameters \( \lambda \in \mathbb{N}, \Pi^0, \Pi^1 \in \mathcal{P} \) where \( \Pi^b = (\text{mem}^{0,0}, F_1^b, ..., F_l^b) \) for \( b \in \{0, 1\} \) and \( \text{Trace}(\Pi^0) = \text{Trace}(\Pi^1) \), it holds that

\[
| \Pr[D(\text{Obf}(1^\lambda, \Pi^0)) = 1] - \Pr[D(\text{Obf}(1^\lambda, \Pi^1)) = 1] | \leq \text{negl}(\lambda).
\]

66
Efficiency. We require DBCompile and Obf runs in time $\tilde{O}(\lvert \text{mem}^{0,0} \rvert)$ and $\tilde{O}(\text{poly}(\lvert F_{\text{sid}} \rvert))$, and efficient Eval runs in time $\tilde{O}(t_{\text{sid}}^*)$.

10.1.2 Constructing CiO for RAM with persistent database

Construction. We construct CiO for RAM with persistent database from the ordinary CiO for RAM (without persistent database). In general, we still follow the original setting of CiO for RAM, but use $(\text{sid}, t)$ as timestamp instead. Moreover, a new key $K_T$ (so-called termination key) is involved in the obfuscated state function and only used at the beginning and end of a program. These three algorithms work as follows.

- Database compilation algorithm DBCompile is identical to Steps 1 and 3 of CiO for RAM (without persistent database). It generates the initial configuration $(\text{mem}^{-0,0}, \text{st}^{-0,0})$ except that $\sigma^{0,0}$ is generated from the (pseudo-)randomness $r_0 \leftarrow \text{PRF}(K_T, 0)$.
- Program compilation algorithm Obf is similar to Step 2 of CiO for RAM except that adding authentications under $K_T$ for each sid, $1 \leq \text{sid} \leq l$. It generates the obfuscated stateful function (See Algorithm 19). Note that the authentications under $K_T$ are only performed in the beginning and end of a program. This algorithm outputs $\tilde{F}_{\text{sid}} \leftarrow i_{\text{O, Gen}}(\tilde{F}_{\text{sid}}')$.
- Evaluation algorithm Eval$(\text{mem}^{-\text{sid}-1,0}, \text{st}^{-\text{sid}-1,0}, \tilde{F}_{\text{sid}})$ is identical to Evaluation algorithm of CiO for RAM. It outputs $(\text{mem}^{-\text{sid},0}, \text{st}^{-\text{sid},0})$ for the next session.

Algorithm 19: $\tilde{F}_{\text{sid}}'$ in CiO for RAM with persistent database

\begin{algorithm}
\begin{algorithmic}
\STATE \textbf{Input} : $\text{st}^{\text{in}} = ((\text{sid}, t), \text{st}^{\text{in}}, t^{\text{in}}, w^{\text{in}}, \sigma^{\text{in}}), \ldots$
\STATE \textbf{Data}: $\ldots, K_T$
\STATE \textbf{if} \text{sid} is correct and (\text{sid}, t) is the beginning of the \text{sid} session \textbf{then}
\STATE \hspace{1em} Compute $r_{\text{sid}-1} = \text{PRF}(K_T, \text{sid} - 1)$ and $(\text{sk}_{\text{sid}-1}, \text{vk}_{\text{sid}-1}, \text{vk}_{\text{sid}-1, \text{rej}}) = \text{Spl.Setup}(1^\lambda; r_{\text{sid}-1})$;
\STATE \hspace{1em} If $\text{Spl.Verify}(\text{vk}_{\text{sid}-1}, (\text{sid} - 1, \text{st}^{\text{in}}, t^{\text{in}}, w^{\text{in}}, \sigma^{\text{in}})) = 0$, output $\text{Reject}$;
\STATE \hspace{1em} Set $\text{st}^{\text{in}} = \text{Init}$;
\STATE \hspace{1em} \ldots // Lines 1 to 16, Algorithm 1
\STATE \textbf{if} $\text{st}^{\text{out}}$ returns halt for termination \textbf{then}
\STATE \hspace{1em} Compute $r_{\text{sid}} = \text{PRF}(K_T, \text{sid})$ and $(\text{sk}_{\text{sid}}, \text{vk}_{\text{sid}}, \text{vk}_{\text{sid}, \text{rej}}) = \text{Spl.Setup}(1^\lambda; r_{\text{sid}})$;
\STATE \hspace{1em} Compute $\sigma^{\text{out}} = \text{Spl.Sign}(\text{sk}_{\text{sid}}, (\text{sid}, \text{st}^{\text{out}}, t^{\text{out}}, w^{\text{out}}));$
\STATE \hspace{1em} Output $\text{st}^{\text{out}} = ((\text{sid}, 0), \text{st}^{\text{out}}, t^{\text{out}}, w^{\text{out}}, \sigma^{\text{out}}) // \text{no database access}$
\end{algorithmic}
\end{algorithm}

Security Sketch. Recall that the computation system II consists of an initial memory and a sequence of programs. Although we cannot directly use the security of CiO for RAM, using the pebble game analogy, we can go through the hybrid argument that is quite similar to CiO for RAM without persistent database. Conceptually, we can view the computation paths of the sequence of programs as a single large computation path. The proof strategy is modified as follows: Recall that in the security proof of CiO for RAM without persistent database, we move the check point from $t = 1$ to $t = t^*$ through hybrid argument. In the persistent database setting, the technique of moving from the timestamp $(\text{sid}, t)$ to $(\text{sid}, t + 1)$ is identical to that in the setting without PDB. The only difference here is that we need to move from the termination time $(\text{sid}, t_{\text{sid}}^*)$ of session $\text{sid}$ to the beginning $(\text{sid} + 1, 0)$ of the next session. For this, we can use the same technique as
before to switch between the type A and B termination key $K_T$. We note that the purpose of $K_T$ is to introduce keys which are independent to the termination time of the programs. It is otherwise conceptually the same as the type A key $K_A$ used to sign the internal states. A special conceptual point to note is that, in some intermediate hybrids, the enforcement of the accumulator or iterator is required to enforce the whole history from the initiation to the current timestamp.

10.1.3 Constructing CiO for PRAM with persistent database

Construction. Following the same technique and conventions above, we construct CiO for PRAM with persistent database from full-fledged CiO for PRAM. In our construction of CiO for PRAM with persistent database, database compilation $\text{DBCompile}$, program compilation $\text{Obf}$, and evaluation algorithm $\text{Eval}$ works as those in CiO for RAM with persistent database respectively, except for the obfuscated stateful function (See Algorithm 20). Note that once all CPUs terminate in session $\text{sid}$, the stateful function $\hat{F}_{\text{sid}}'$ only takes the CPU1’s state to generate the signature for connecting the next session.

Algorithm 20: $\hat{F}_{\text{sid}}'$ in CiO for PRAM with persistent database

```
Input : $\text{st}^{\text{in}} = (\text{sid, st}^{\text{in}}, \text{id}_{\text{cpu}}, \text{root_node}), ...$
Data : $..., K_T$

1 Parse root_node as before // extract $t$ from root_node
2 if $\text{sid}$ is correct and ($\text{sid, t}$) is the beginning of the $\text{sid}$ session then
3     Compute $r_{\text{sid} - 1} = \text{PRF}(K_T, \text{sid})$ and $(\text{sk}_{\text{sid} - 1}, \text{vk}_{\text{sid} - 1}, \text{vk}_{\text{sid} - 1, \text{rej}}) = \text{Spl.Setup}(1^\lambda; r_{\text{sid} - 1});$
4     If Spl.Verify($\text{vk}_{\text{sid} - 1}, (\text{sid} - 1, \text{st}^{\text{in}}, v^{\text{in}}, w^{\text{in}}_{\text{st}}, w^{\text{in}}_{\text{com}}, \sigma^{\text{in}}) = 0$, output Reject;
5     Set $\text{st}^{\text{in}} = \text{Init};$
6 ... // Branch and Combine of CiO for PRAM
7 if all CPUs enter halt for termination then
8     Set $\text{st}^{\text{out}}$ as CPU1’s state;
9     // Let CPU1’s final state be the initial state of the next session
10    Computes $r_{\text{sid}} = \text{PRF}(K_T, \text{sid})$ and $(\text{sk}_{\text{sid}}, \text{vk}_{\text{sid}}, \text{vk}_{\text{sid}, \text{rej}}) = \text{Spl.Setup}(1^\lambda; r_{\text{sid}});$
11    Compute $\sigma^{\text{out}} = \text{Spl.Sign}(\text{sk}_{\text{sid}}, (\text{sid, st}^{\text{out}}, v^{\text{out}}, w^{\text{out}}_{\text{st}}, w^{\text{out}}_{\text{com}}));$
12    Generate root_node = ($t$, Root, $w^{\text{out}}_{\text{st}}, w^{\text{out}}_{\text{com}}, v^{\text{out}}, \sigma^{\text{out}});$
13    Output $\text{st}^{\text{out}} = (\text{sid, st}^{\text{out}}, \text{root_node});$
```

Security Sketch. As for CiO for RAM with persistent database, the enforcement of the accumulator or iterator is required to enforce the whole history from the initiation to the current timestamp. We can use the same proof technique illustrated by the pebble game to go through the hybrid argument.

10.2 RE with Persistent Database

As in the ordinary setting without persistent database, after obtaining CiO which forces the obfuscated program to be executed as intended, we can extend it to RE so as to provide input and program privacy. In the persistent database setting, we wish to protect the privacy of the entire sequence of inputs and programs, while allowing the output of each program in the sequence to be learnt by the decoder in the clear.
10.2.1 Definition

**Definition 10.2 (RE with Persistent Database).** A randomized encoding scheme \( \mathcal{RE} \) with persistent database consists of algorithms \( \mathcal{RE} = \{ \text{RE}, \{ \text{DBInit, Encode, Decode} \} \) described below:

- \( \mathcal{RE} \).DBEncode\{mem\( ^{0,0}, 1^\lambda \) \( \rightarrow \) mem\( ^{0,0} \): The database compilation algorithm DBEncode is a randomized algorithm which takes as input the security parameter \( 1^\lambda \) and a database mem\( ^{0,0} \). It outputs a compiled database mem\( ^{0,0} \).
- \( \mathcal{RE} \).Encode\{P\( _{\text{sid}} \), x\( _{\text{sid}} \), 1^\lambda \) \( \rightarrow \) ENC\( _{\text{sid}} \): The encoding algorithm Encode is a randomized algorithm which takes as input the security parameter \( 1^\lambda \), the description of a RAM program \( P\_\text{sid} \) with time bound \( T \) and space bound \( S \), and an input \( x\_\text{sid} \). It outputs an encoding ENC\( _{\text{sid}} \).
- \( \mathcal{RE} \).Decode\{ENC\( _{\text{sid}}, \text{mem}\_\text{sid}^{\text{sid}−1,0}, 1^\lambda, T, S \) \( \rightarrow \) (y\( _{\text{sid}}, \text{mem}\_\text{sid}^{\text{sid},0} \): The decoding algorithm Decode is a deterministic algorithm which takes as input the security parameter \( 1^\lambda \), time bound \( T \) and space bound \( S \), an encoding ENC\( _{\text{sid}} \), and a compiled database mem\( _{\text{sid}}^{\text{sid}−1,0} \). It outputs \( y\_\text{sid} = P\_\text{sid} (x\_\text{sid}) \) or \( \perp \), and a compiled database mem\( _{\text{sid}}^{\text{sid},0} \).

**Correctness.** A randomized encoding scheme \( \mathcal{RE} \) is said to be correct if

\[
\Pr[\text{mem}^{0,0} \leftarrow \mathcal{RE}.\text{DBEncode}(\text{mem}^{0,0}, 1^\lambda); \text{ENC}\_\text{sid} \leftarrow \mathcal{RE}.\text{Encode}(P\_\text{sid}, x\_\text{sid}, 1^\lambda); (y\_\text{sid}, \text{mem}\_\text{sid}^{\text{sid},0}) \leftarrow \mathcal{RE}.\text{Decode}(\text{ENC}\_\text{sid}, \text{mem}\_\text{sid}^{\text{sid}−1,0}, 1^\lambda, T, S) : y\_\text{sid} = P\_\text{sid} (x\_\text{sid}) \text{ \forall \text{sid}, 1 \leq \text{sid} \leq l}] = 1.
\]

**Security.** A randomized encoding scheme \( \mathcal{RE} \) with persistent database is said to be hiding if for all PPT adversary \( A \), time \( l \), database \( \text{mem}^{0,0} \), program \( P\_\text{sid} \) with time bound \( T \) and space bound \( S \), input value \( x\_\text{sid} \), and output value \( y\_\text{sid} = P\_\text{sid} (x\_\text{sid}) \) for \( \text{sid} \geq 0 \) that generated at termination time \( t\_\text{sid}^* \) there exists a PPT simulator \( S \) such that

\[
| \Pr[\text{mem}^{0,0} \leftarrow S(1|\text{mem}^{0,0}, 1^\lambda); \text{ENC}\_\text{sid} \leftarrow S(1|P\_\text{sid}, 1|x\_\text{sid}, t\_\text{sid}^*, y\_\text{sid}, 1^\lambda, T, S) : A(1^\lambda, \text{mem}^{0,0}, \{\text{ENC}\_\text{sid}\}_{\text{sid}=1}^{\text{sid}=1}) = 1] - \Pr[\text{mem}^{0,0} \leftarrow \mathcal{RE}.\text{DBEncode}(\text{mem}^{0,0}, 1^\lambda); \text{ENC}\_\text{sid} \leftarrow \mathcal{RE}.\text{Encode}(P\_\text{sid}, x\_\text{sid}, 1^\lambda); A(1^\lambda, \text{mem}^{0,0}, \{\text{ENC}\_\text{sid}\}_{\text{sid}=1}^{\text{sid}=1}) = 1]| \leq \text{negl}(\lambda).
\]

**Efficiency.** We require DBEncode and Encode runs in time \( \tilde{O}(|\text{mem}^{0,0}|) \) and \( \tilde{O}(\text{poly}(|P\_\text{sid}|) + |x\_\text{sid}|) \), and efficient Decode runs in time \( \tilde{O}(t\_\text{sid}^*) \).

10.2.2 Constructing \( \mathcal{RE} \) with Persistent Database

**Construction.** The construction of \( \mathcal{RE} \) with PDB relies on the same technique to build \( \mathcal{RE} \) from CiO without PDB. As in Section 8, we use public-key encryption to hide the content including the database and state, use oblivious RAM or PRAM to hide the access pattern, and finally use CiO for RAM or PRAM with PDB to obfuscate the compiled programs. The \( \mathcal{RE} \) with PDB construction works as follows.

- \( \mathcal{RE} \).DBEncode: It first compiles database \( \text{mem}^{0,0} \) to \( \overline{\text{mem}^{0,0}} \) by ORAM or OPRAM compiler, then generates encryption of \( \overline{\text{mem}^{0,0}} \) by \( \mathcal{PK} \_\text{CiO} \). Finally, it outputs \( \overline{\text{mem}^{0,0}} \) by DBCompile of \( \text{CiO} \) with PDB.

- \( \mathcal{RE} \).Encode: Unlike in ordinary \( \mathcal{RE} \) where the input is written to the memory, we embed both the program \( P\_\text{sid} \) and the input \( x\_\text{sid} \) into a stateful function \( F\_\text{sid} \). It compiles the stateful function \( F\_\text{sid} \) to \( F\_\text{sid,e} \) by ORAM or OPRAM compiler, and then generates \( F\_\text{sid,e} \) which includes decryption and encryption, except that at \( t = 0 \) \( F\_\text{sid,e} \) accepts the plaintext output generated by the previous program without performing decryption.
Security Sketch. As in the security proof of 
that the later does not learn anything from about the input, the program, nor the output. Observe that this
in some applications, a client might want to delegate a computation to a server while at the same time ensuring
intermediate outputs are given to the simulator.

state, which is simply the plaintext output of the previous program, is hardwired. This is possible since all

Hiding. A scheme \( \mathcal{RE} \) with output hiding \( \mathcal{RE}_{\text{ohiding}} \), is defined as follows.

\( \mathcal{RE}_{\text{ohiding}}.\text{Encode}(P, x, 1^\lambda) \rightarrow (\text{ENC}, \text{sk}): \) The encoding algorithm \( \text{Encode} \) is a randomized algorithm which takes as input the security parameter \( 1^\lambda \), the description of a RAM or PRAM program \( P \) with time bound \( T \) and space bound \( S \), and an input \( x \). It outputs an encoding \( \text{ENC} \) and a private key \( \text{sk} \).

\( \mathcal{RE}_{\text{ohiding}}.\text{Decode}(\text{ENC}, 1^\lambda, T, S) \rightarrow c: \) The decoding algorithm \( \text{Decode} \) is a deterministic algorithm which takes as input the security parameter \( 1^\lambda \), time bound \( T \), space bound \( S \), and an encoding \( \text{ENC} \). It outputs ciphertext \( c \), or \( \perp \).

\( \mathcal{RE}_{\text{ohiding}}.\text{Decrypt}(\text{sk}, c) \rightarrow y: \) The output decrypting algorithm \( \text{Decrypt} \) is a deterministic algorithm which takes as input the private key \( \text{sk} \) and the ciphertext \( c \). It outputs the plain text \( y \).

For efficiency, we require that \( \text{Encode} \) runs in time \( \tilde{O}(\text{poly}(|P| + |x|)) \) and \( \text{Decrypt} \) runs in time \( \tilde{O}(1) \), and efficient \( \text{Decrypt} \) runs in time \( \tilde{O}(T) \). That is, a client can efficiently \( \text{Encode} \) a computation and \( \text{Decrypt} \) the ciphertext \( c \) of output, and a server carries out \( \text{Decrypt} \) in time comparable to the insecure computation.

Correctness. A scheme \( \mathcal{RE}_{\text{ohiding}} \) is said to be correct if

\[
\Pr[\text{(ENC, sk)} \leftarrow \mathcal{RE}_{\text{ohiding}}.\text{Encode}(P, x, 1^\lambda); c \leftarrow \mathcal{RE}_{\text{ohiding}}.\text{Decode}(\text{ENC}, 1^\lambda, T, S); \]
\[
y \leftarrow \mathcal{RE}_{\text{ohiding}}.\text{Decrypt}(\text{sk}, c) : y = P(x)] = 1.
\]

Hiding. A scheme \( \mathcal{RE}_{\text{ohiding}} \) is said to have output hiding if for all PPT adversary \( \mathcal{A} \), program \( P \) with time bound \( T \) and space bound \( S \), input value \( x \), and output value \( y = P(x) \) that generated at termination time \( t^* \), there exists a PPT simulator \( \mathcal{S} \) such that

\[
|\Pr[\text{ENC} \leftarrow \mathcal{S}(1^{|P|}, 1^{|x|}, 1^{|y|}, t^*, 1^\lambda, T, S) : \mathcal{A}(1^\lambda, \text{ENC}) = 1]| \leq \text{negl}(\lambda).
\]

\[
- \Pr[\text{(ENC, sk)} \leftarrow \mathcal{RE}_{\text{ohiding}}.\text{Encode}(P, x, 1^\lambda) : \mathcal{A}(1^\lambda, \text{ENC}) = 1]| \leq \text{negl}(\lambda).
\]

70
Construction. Let \( \mathcal{RE} = \mathcal{RE}.\{\text{Encode, Decode}\} \) be a randomized encoding scheme. Let \( \mathcal{SKE} = \mathcal{SKE}.\{\text{Gen, Encrypt, Decrypt}\} \) be a symmetric key encryption scheme. The randomized encoding scheme with output hiding, \( \mathcal{RE}_{\text{ohiding}} = \mathcal{RE}_{\text{ohiding}}.\{\text{Encode, Decode, Decrypt}\} \), is constructed as follows:

1. Let \( \mathcal{RE} \) be a randomized encryption scheme. Let \( \mathcal{SKE} \) be a symmetric key encryption scheme. The randomized encoding scheme with output hiding, \( \mathcal{RE}_{\text{ohiding}} = \mathcal{RE}_{\text{ohiding}}.\{\text{Encode, Decode, Decrypt}\} \), is constructed as follows:

2. **ENC** \( \leftarrow \mathcal{RE}_{\text{ohiding}}.\text{Encode}(P, x, 1^\lambda) \):
   - Compute \( sk \leftarrow \mathcal{SKE}.\text{Gen}(1^\lambda) \).
   - Sample \( \rho \leftarrow \{0, 1\}^\lambda \).
   - Compute \( ENC \leftarrow \mathcal{RE}_{\text{ohiding}}.\text{Encode}(P', (x, \rho), 1^\lambda) \), where \( P' \) is defined in Algorithm 21.
   - Return \( (ENC, sk) \).

3. Let \( c \leftarrow \mathcal{RE}_{\text{ohiding}}.\text{Decode}(ENC, 1^\lambda, T, S) \):
   - Compute \( c \leftarrow \mathcal{RE}_{\text{ohiding}}.\text{Decode}(ENC, 1^\lambda, T, S) \).

4. Let \( c \leftarrow \mathcal{RE}_{\text{ohiding}}.\text{Decrypt}(sk, c) \):
   - Return \( y \leftarrow \mathcal{SKE}.\text{Decrypt}(sk, c) \).

Algorithm 21: \( P' \)

| **Input** | \((x, \rho)\) |
| **Data** | \(P, sk\) |
| 1 | Compute \( y \leftarrow P(x) \); |
| 2 | Compute \( c \leftarrow \mathcal{SKE}.\text{Encrypt}(sk, y; \rho) \); |
| 3 | Output \( c \); |

Security. The security follows directly from the security of \( \mathcal{RE} \) and \( \mathcal{SKE} \).

10.4 \( \mathcal{RE} \) with Verifiability (Or Verifiable Encoding (\( \mathcal{VE} \)))

In this extension, we consider adding verifiability to \( \mathcal{RE} \) which we call a verifiable randomized encoding (\( \mathcal{VRE} \)). Intuitively, verifiability can be achieved by generating a signing key and verification key during the encoding process, which uses \( CIO \) to obfuscate a program which signs the output of the program being encoded using the signing key.

Observe that although such a construction is non-black-box, it is mostly orthogonal to the construction of \( \mathcal{RE} \). On the other hand, an encoding with verifiability but without privacy, which we call a verifiable encoding (\( \mathcal{VE} \)), is already useful in some delegation scenarios. Thus, it makes sense to consider \( \mathcal{VE} \) as a stand-alone extension from \( CIO \).

More explicitly, we consider a verifiable encoding \( \mathcal{VE} \) which encodes a program \( P \) and an input \( x \) into an encoding \( ENC \), which can be decoded by the decoder to produce the computation result \( y = P(x) \) and a proof \( \pi \) which proves the correctness of the computation. The encoding algorithm also outputs a public verification key \( vk \), with which any public verifier can check the correctness of \( y \) by verifying the proof \( \pi \). This directly implies a two-message publicly-verifiable delegation scheme in the respective model.

10.4.1 Verifiable Encoding (\( \mathcal{VE} \))

Formally, a verifiable encoding scheme \( \mathcal{VE} \) consists of algorithms \( \mathcal{VE} = \mathcal{VE}.\{\text{Encode, Decode, Verify}\} \) described below.

- \( \mathcal{VE}.\text{Encode}(P, x, 1^\lambda) \to (ENC, vk) \):
  - The encoding algorithm \( \text{Encode} \) is a randomized algorithm which takes as input the security parameter \( 1^\lambda \), the description of a RAM / PRAM program \( P \) with time bound \( T \) and space bound \( S \), and an input \( x \). It outputs an encoding \( ENC \) and a verification key \( vk \).

- \( \mathcal{VE}.\text{Decode}(ENC, 1^\lambda, T, S) \to (y, \pi) \):
  - The decoding algorithm \( \text{Decode} \) is a deterministic algorithm which takes as input the security parameter \( 1^\lambda \), time bound \( T \), space bound \( S \), and an encoding \( ENC \). It outputs \( y = P(x) \) or \( \bot \), and a proof \( \pi \).
Our construction uses several building blocks listed as follows:

10.4.2 Building Blocks

- **Verifiability.** A verifiable randomized encoding scheme \( VE \) is said to be verifiable if

\[
\Pr[(\text{ENC}, vk) \leftarrow VE.\text{Encode}(P, x, 1^\lambda); (y, \pi) \leftarrow VE.\text{Decode}(\text{ENC}, 1^\lambda, T, S); \\
b \leftarrow VE.\text{Verify}(vk, \pi, y) : y = P(x) \land b = 1] \leq \text{negl}(\lambda)
\]

10.4.3 The Construction

We define our \( VE = VE.\{\text{Encode}, \text{Decode}, \text{Verify}\} \) for the program \( P \) and input \( x \) as follows:

- **Encoding algorithm** \( (\text{ENC}, vk) \leftarrow VE.\text{Encode}(P, x, 1^\lambda) \): The encoding algorithm represents \( (P, x) \) into \( \Pi = ((\text{mem}^0, \text{st}^0), F) \) for RAM program \( P \) or \( \Pi = (\text{mem}^0, F) \) for PRAM program \( P \) with \( x \) written to \( \text{mem}^0 \) sequentially. The encoding algorithm randomly choose \( r_1, r_2, r_3 \), and computes \( (\text{sk}, vk) = \text{SIG}.\text{Gen}(1^\lambda; r_1) \). It then further compiles \( F \) into a program \( F' \) defined in Algorithm 22. Let \( \tilde{\Pi} = ((\text{mem}^0, \text{st}^0_1, \ldots, \text{st}^0_m), F') \), it computes \( \text{ENC} \leftarrow \text{CiO}.\text{Obf}(1^\lambda, \tilde{\Pi}) \). Finally, it outputs \( (\text{ENC}, vk) \).

- **Decoding algorithm** \( (y, \pi) \leftarrow VE.\text{Decode}(\text{ENC}, 1^\lambda, T, S) \): The decoding algorithm executes \( \text{CiO}.\text{Eval}(\text{ENC}) \) to obtain the configuration \( (\text{st}^t_1 = (\text{halt}, y), \sigma), \text{st}^t_2, \ldots, \text{st}^t_m, \text{mem}^t) \) upon termination, and outputs \( (y, \pi) = (y, \sigma) \).

- **Verification algorithm** \( b \leftarrow VE.\text{Verify}(vk, y, \sigma) \): The verification algorithm outputs \( b = \text{SIG}.\text{Verify}(vk, y, \sigma) \).

**Theorem 10.4.** Let \( \text{CiO} \) be an indistinguishability obfuscation for computation in RAM / PRAM model, \( \text{SIG} \) be a secure signature scheme. Then \( VE \) is a secure verifiable encoding scheme.

The proof can be found in Section B.7.
Algorithm 22: $\tilde{F}$ // this program is used in $\forall E$

\begin{algorithm}
\begin{algorithmic}[1]
\Statex \textbf{Input} : $\text{st}^{\text{in}} = (\text{st}^{\text{in}}, t), a^{\text{in}}$
\Statex \textbf{Data} : $T, r_1, r_2, sk$
\LineComment{Compute $(\text{st}^{\text{out}}, a^{\text{out}}) = F(\text{st}^{\text{in}}, a^{\text{in}})$;}
\LineComment{if $\text{st}^{\text{out}} \neq (\text{halt}, \cdot)$ then}
\LineComment{Set $\hat{\text{st}}^{\text{out}} = (\text{st}^{\text{out}}, t + 1)$;}
\LineComment{else}
\LineComment{Parse $\text{st}^{\text{out}} = (\text{halt}, y)$;}
\LineComment{if $y = \bot$ then}
\LineComment{Set $\hat{\text{st}}^{\text{out}} = \text{st}^{\text{out}}$;}
\LineComment{else}
\LineComment{Compute $(sk, vk) = \text{SIG.Gen}(1^\lambda; r_1)$;}
\LineComment{Compute $\sigma = \text{SIG.Sign}(sk, y; r_2)$;}
\LineComment{Set $\hat{\text{st}}^{\text{out}} = (\text{st}^{\text{out}}, \sigma)$;}
\LineComment{Set $a^{\text{out}} = \bot$;}
\LineComment{Output $\hat{\text{st}}^{\text{out}}, a^{\text{out}}$;}
\end{algorithmic}
\end{algorithm}

10.5 $\mathcal{RE}$ and $\forall E$ with Long Output

Recall that in the definitions of $\mathcal{RE}$ and its extensions (including $\forall E$), we always consider a program $P$ and input $x$ such that $y = P(x)$ is of a fixed short length. However, in practical applications, the program might produce an output of long, and possibly variable, length. Our main strategy is to let the main program write its output onto a specified area of the memory. In the following, we first consider the simpler case of $\mathcal{RE}$ with output hiding. In this case, the decoder simply returns the ciphertexts stored in the specified area. Next, for the more complicated case $\mathcal{RE}$ without output hiding, $\mathcal{RE}$ with long output can be constructed using $\mathcal{RE}$ with persistent database. The idea is to encode a sequence of short programs which reads, decrypts and outputs a short portion of the specified area. Finally, for $\forall E$ which only provides verifiability but without any privacy, our strategy is very similar to that of $\mathcal{RE}$ with output hiding. Concretely, the main program writes its output, which is in plaintext, along with a signature onto a specified area of the memory. Note that in $\forall E$ the content of the memory is not encrypted. Thus, the decoder simply returns the plaintexts stored in the specified area.

$\mathcal{RE}$ with Long Output with Output Hiding. In this setting, instead of the output $y$, a position-length pair is put in the termination state. The decoder then simply return the specified portion of the memory to the encoder. In the case where verifiability (of the ciphertexts) is required, the main program signs the long sequence of ciphertexts using the hash-then-sign paradigm, so that a single short signature can be appended at the end of the sequence. Concretely, the main program maintains a hash tree which compresses the long sequence of output ciphertexts into a short digest stored in the root of the tree. The root is then signed to authenticate the entire tree. Notice that in this setting the size of the encoding is independent to the size of the output. This corresponds to the fact that the simulator can simply simulate the encrypted output sequence by a sequence of random values, so that no hardwiring of the long output is needed.

$\mathcal{RE}$ with Long Output without Output Hiding. In the following, we let $l$ be an upper bound of the output length of the program $P$ with input $x$. $\mathcal{RE}$ with long output without output hiding can be achieved by first writing the sequence of ciphertext onto the memory as specified above, then encoding a sequence of $l$ short programs which reads, decrypts and outputs a short portion of the specified area. In the case where verifiability
We note the number of encodings \( l \) depends on the output length of the program. This is due to the fact that the entire sequence of outputs must be hardwired to the simulated encoding in the security proof. Thus, \( \mathcal{RE} \) with output hiding not only provides output privacy, but also produces shorter encodings.

To see why the dependency on \( l \) is necessary, we consider a program which functions as a pseudo random generator (PRG) which has short input and long output. Suppose that there exists secure \( \mathcal{RE} \) with long output without output hiding which produces encoding of \( (P, x) \) with length independent to the length of \( y = P(x) \). By the security of \( \mathcal{RE} \), there exists a simulator for \( \mathcal{RE} \) which produces upon input \( y \) a simulated encoding with length independent to the length of \( y \). We wish to construct a distinguisher which distinguishes PRG from a random function. Suppose in the security game of PRG the challenger returns upon a query \( x \) an output \( y \). We then pass \( y \) to the simulator of \( \mathcal{RE} \). If the chosen function is a PRG, then the simulated encoding has length independent to \( y \). Other, if the chosen function is a random function, then either the simulated encoding has length depending on \( y \), or the decoding of the simulated encoding produces result different from \( y \) with non-negligible probability. In either case, we can distinguish the PRG from the random function.

\( \mathcal{VE} \) with Long Output. Similar to \( \mathcal{RE} \) with output hiding, the main program signs the long sequence of outputs using the hash-then-sign paradigm, so that a single short signature can be appended at the end of the sequence. Then, instead of the output \( y \), a position-length pair is put in the termination state. Finally, the decoder returns the specified portion of the memory to the encoder.

### 10.6 Application: Searchable Symmetric Encryption (SSE)

In the previous sections, we show how \( \mathcal{RE} \) for RAM and PRAM can be extended to support a wide range of properties, including persistent database (Section 10.2), output hiding (Section 10.3), long output (Section 10.5) and verifiability. Different combinations of these properties are useful for different scenarios of outsourced computation. In particular, we consider a very powerful searchable symmetric encryption scheme (SSE) with almost all desirable properties as a direct application of \( \mathcal{RE} \) with all the above extensions.

Roughly, SSE allows a client to outsource the storage of his encrypted data to a semi-honest (possibly malicious) server, while retaining the server’s ability to query over the encrypted data without learning the plaintext data. The query can be as general as data modification, (conjunctive / fuzzy) keyword search or essentially any function over the plaintext data. To query over the encrypted data, the client uses its private key to transform its query into a trapdoor, which is sent to the server. With the help of the trapdoor, the server updates the encrypted database and returns the encrypted query results to the client.

Ideally, an SSE scheme is considered security if the encrypted data and queries do not reveal any information about the plaintext data and query results respectively. It is commonly believed that such security requirements can be achieved using ORAM. In reality, typical SSE schemes which do not rely on ORAM leak some information such as the search and access patterns as a trade-off for efficiency.

Using \( \mathcal{RE} \) with persistent database, we can naturally encode our plaintext data which will then be stored in a cloud server. Then, with the support of long output and output hiding, an encoded query can be processed by the server to return a long sequence of ciphertext, which can be decrypted to obtain the results of the query. Moreover, by the succinctness of our \( \mathcal{RE} \) construction, the query complexity is preserved up to a logarithmic factor.

In terms of security, note that by the security of \( \mathcal{RE} \), the server only learns the sizes of the database and the query results. The security of this SSE scheme is thus not only much stronger than most of the existing schemes [KPR12, KP13, SPS14] which leak search and access patterns, but also achieves two very desirable property named forward privacy and backward privacy. Forward privacy means that a previously issued trapdoor for a query is not useful for querying newly added data. Similarly, backward privacy means that a trapdoor is not useful for querying deleted data. In addition, with the verifiability extension, the correctness of the query
results can be verified. It is also worth mentioning that while most \$SSE\$ schemes are proven secure in the random oracle model, our construction is secure in the standard model. The only drawback of our construction is that we cannot prove its adaptive security, which is in general an open problem for many obfuscation / garbling / randomized encoding related primitives.
A Preliminaries

Notations. Let λ be the security parameter. Let poly be any polynomial. Let negl be any negligible function.

A.1 Models of Computation

A.1.1 Random-Access Machines (RAM)

A random-access machine (RAM) consists of a CPU with a local register st of size $\log n$ and an external memory mem $\in \{0, 1\}^n$, where $n = \text{poly}(\lambda)$. A RAM program $P$ with random-access to mem takes as input $x \in \{0, 1\}^{\ell_{\text{input}}}$, where $\ell_{\text{input}} \leq n$, and outputs $y = P(x)$ as the result of the computation. During the computation, the CPU may access the memory multiple times using READ or WRITE operations:

- READ(loc): upon receiving a memory address loc, return the value $\text{mem}[\text{loc}]$.
- WRITE(loc, val): upon receiving a memory address loc and a value val, set $\text{mem}[\text{loc}] := \text{val}$.

In this work, we use both functional program and next-step program to present the RAM program, and we prepresent the above functional program $P$ as a series of executions of a small next-step program $F$ which executes a single CPU step:

$$(\text{st}^{\text{out}}, \text{loc}^{\text{out}}, \text{val}^{\text{out}}) = F(\text{st}^{\text{in}}, \text{loc}^{\text{in}}, \text{val}^{\text{in}}).$$

At each time step $t$, the CPU-step circuit takes as input an input state $\text{st}^{\text{in}}$, a location $\text{loc}^{\text{in}}$, and value $\text{val}^{\text{in}} = \text{mem}[\text{loc}^{\text{in}}]$ read from the memory, and outputs an output state $\text{st}^{\text{out}}$, a location $\text{loc}^{\text{out}}$ to be accessed, and value $\text{val}^{\text{out}}$.

By convention, at the first step (i.e. step 0), the next-step program is executed with $\text{loc}^{\text{in}} = \perp$ and $\text{val}^{\text{in}} = \perp$. At each step, a copy of the next-step program is executed. If $F$ issues a WRITE memory operation with $\text{loc}^{\text{out}}$ and $\text{val}^{\text{out}}$ specified, then the value $\text{val}^{\text{out}}$ will be written to $\text{mem}[\text{loc}^{\text{out}}]$, and the evaluator sets $\text{loc}^{\text{in}} = \perp$ and $\text{val}^{\text{in}} = \perp$ for the next step. Else if $F$ issues a READ memory operation with $\text{loc}^{\text{in}}$ specified and $\text{val}^{\text{out}} = \perp$, then the evaluator sets $\text{loc}^{\text{in}} = \text{loc}^{\text{out}}$, and the location $\text{loc}^{\text{in}}$ is read by setting $\text{val}^{\text{in}} = \text{mem}[\text{loc}^{\text{in}}]$ for the next step.

There are two ways to define the output of the computation. The first approach is to interpret the output state of the last CPU-step circuit as the output of the computation, which limits the size of the output to $\log n$. The second approach is to interpret a pre-defined region of the external memory mem as the output of the computation. For simplicity, we adopt in this work the first definition, but note that the second definition can also be adopted.

A.1.2 Parallel RAM (PRAM)

A parallel random-access machine (PRAM) consists of $m$ CPUs, each with local memory register of size $\log n$, sharing an external memory mem $\in \{0, 1\}^n$, where $n = \text{poly}(\lambda)$. A RAM is simply a PRAM with $m = 1$. A PRAM program $P$ has random-access to mem, takes as input $x$ and outputs $y = P(x)$ as the result of the computation. In general, a PRAM program utilizes a dynamic number of CPUs in each time step. In a simpler variant, it is assumed that the program always uses all the $m$ CPUs.

Similar to a RAM program, a PRAM program can be represented by a series of executions of the next-step program $F$, but with the additional ability to execute $m$ copies in parallel at each time step. For each CPU $k \in [m]$, $F$ computes a time step with its $k$th copy of state and memory operation, and an additional argument $k$ denoting which CPU it is computing. That is, for each $k \in [m]$

$$(\text{st}^{\text{out}}_k, \text{loc}^{\text{out}}_k, \text{val}^{\text{out}}_k) = F(k, \text{st}^{\text{in}}_k, \text{loc}^{\text{in}}_k, \text{val}^{\text{in}}_k).$$

The conflicts in read and write locations are resolved according to either the exclusive read exclusive write (EREW), concurrent read exclusive write (CREW), or concurrent read concurrent write (CRCW) strategy. For
simpler analysis, we always assume that a PRAM program \( P \) follows the CREW rule, so that there must not be any conflicting writes. We further assume for simplicity (but equivalently) that all \( m \) CPUs read and write synchronously and alternatively, which yields a two-fold (parallel) time overhead because any CPU can at least issue a dummy access and defer the actual access to the next iteration.

Without loss of generality, the input \( x \) is stored in a pre-defined region of the external memory \( \text{mem} \), and all initial states are the same value \( \bot \) for all CPUs. The output of the computation is the output state of the last CPU-step circuit of a specific CPU, which is defined similarly as that for RAM programs. All CPUs halt at the same time with a state \( \text{st} = (\text{halt}, \cdot) \). There is a special CPU \( \text{cpu}_1 \) which always halts with result \( y \) by outputting \( \text{st} = (\text{halt}, y) \) while all other CPUs output \( \text{st} = (\text{halt}, \bot) \).

In some occasions, we will assume additionally (but equivalently) that the CPUs can communicate with each other directly. Roughly speaking, such communication can be simulated by accessing the shared memory. We will explain the details when needed in Sections 7 and 9.

A.1.3 Memoryless PRAM (PRAM−)

A simpler variant of PRAM is the memoryless PRAM (denoted as PRAM−), which consists of \( m \) CPUs, each with local memory register of size \( \log n \), but without external memory. However, there are synchronous communications transmitting constant size messages between CPUs. Their communication pattern is assumed to be oblivious and, at each time step, each CPU only receives one message from one CPU and send one message to one other CPU.

Similar to the standard PRAM program, a PRAM− program can be represented by a series of executions of the next-step circuit, but with the additional ability to execute multiple copies of the circuit at a time step, corresponding to the number of CPUs used in that time step. Unlike in PRAM, the input and output are both stored in the corresponding initial and final CPU states. We will explain the details when needed in Section 7.

Memoryless PRAM is strictly weaker than the standard PRAM, which can emulate PRAM− with memory size \( m < n \) and emulates each communication by writing and reading memory cells.

A.2 Randomized Encoding (R\( \mathcal{E} \))

Randomized encoding scheme \( \mathcal{R} \mathcal{E} \) was originally introduced by Ishai and Kushilevitz [IK00]. Recently, Bitansky et al and Canetti et al studied \( \mathcal{R} \mathcal{E} \) in the TM/RAM models [BGL+15, CHJV15]. Here we state the definition in the RAM model, as follows. We can similarly define \( \mathcal{R} \mathcal{E} \) in the PRAM model.

A randomized encoding scheme \( \mathcal{R} \mathcal{E} \) consists of algorithms \( \mathcal{R} \mathcal{E} = \{ \text{Encode, Decode} \} \) described below.

\( \mathcal{R} \mathcal{E}\).Encode\((P, x, 1^\lambda) \rightarrow \text{ENC} \): The encoding algorithm Encode is a randomized algorithm which takes as input the security parameter \( 1^\lambda \), the description of a RAM program \( P \) with time bound \( T \) and space bound \( S \), and an input \( x \). It outputs an encoding \( \text{ENC} \).

\( \mathcal{R} \mathcal{E}\).Decode\((\text{ENC}, 1^\lambda, T, S) \rightarrow y \): The decoding algorithm Decode is a deterministic algorithm which takes as input the security parameter \( 1^\lambda \), time bound \( T \) and space bound \( S \), and an encoding \( \text{ENC} \). It outputs \( y = P(x) \) or \( \bot \).

**Correctness.** A randomized encoding scheme \( \mathcal{R} \mathcal{E} \) is said to be **correct** if

\[
\Pr[\text{ENC} \leftarrow \mathcal{R} \mathcal{E}.\text{Encode}(P, x, 1^\lambda); y \leftarrow \mathcal{R} \mathcal{E}.\text{Decode}(\text{ENC}, 1^\lambda, T, S) : y = P(x)] = 1.
\]

**Hiding.** A randomized encoding scheme \( \mathcal{R} \mathcal{E} \) is said to be **hiding** if for all PPT adversary \( \mathcal{A} \), program \( P \) with time bound \( T \) and space bound \( S \), input value \( x \), and output value \( y = P(x) \) that generated at termination time
there exists a PPT simulator $S$ such that
\[
\left| \Pr[\text{ENC} \leftarrow S(1^{|P|}, 1^{|x|}, t^*, y, 1^\lambda, T, S) : A(1^\lambda, \text{ENC}) = 1] - \Pr[\text{ENC} \leftarrow \mathcal{R}.\text{Encode}(P, x, 1^\lambda) : A(1^\lambda, \text{ENC}) = 1]\right| \leq \text{negl}(\lambda).
\]

**Efficiency.** We require Encode runs in time $O(\text{poly}(|P| + |x|))$, and efficient Decode runs in time $O(t^*)$. That is, a client can efficiently encode $(P, x)$, and a server carries out evaluation in time comparable to the insecure computation.

### A.3 Building Blocks

#### A.3.1 Iterators

An iterator [KLW15] is a cryptographic data structure which maintains a small iterator state regardless of the number of messages iterated. Although it is impossible for a small iterator state to uniquely identify a sequence of iterated messages, a secure iterator guarantees that normally generated public-parameters are computationally indistinguishable from specially constructed “enforcing” parameters, which ensures a particular iterator state to be obtainable only by iterating a specific message to another specific iterator state. Such a localized property can be achieved information-theoretically by fixing the enforcement ahead of time.

**Syntax.** An iterator $\text{itr}$ with message space $\mathcal{M}_\lambda = \{0, 1\}^{\text{poly}(\lambda)}$ and state space $S_\lambda$ consists of three algorithms: \text{itr}.\{Setup, SetupEnforceIterator, Iterate\}, defined below.

- $\text{itr.\text{Setup}}(1^\lambda, T)$: The setup algorithm takes as input the security parameter $\lambda$ (in unary), and an integer bound $T$ (in binary) on the number of iterations. It outputs public parameters $\text{pp}_{\text{itr}}$ and an initial state $v^0 \in S_\lambda$.
- $\text{itr.\text{SetupEnforceIterator}}(1^\lambda, T, m)$: The enforced setup algorithm takes as input the security parameter $\lambda$ (in unary), an integer bound $T$ (in binary), and a vector of messages $m = (m^1, \ldots, m^k)$. It outputs public parameters $\text{pp}_{\text{itr}}$ and an initial state $v^0 \in S_\lambda$.
- $\text{itr.\text{Iterate}}(\text{pp}_{\text{itr}}, v^m, m)$: The iterate algorithm takes as input the public parameters $\text{pp}_{\text{itr}}$, a state $v^m$, and a message $m \in \mathcal{M}_\lambda$. It outputs a state $v^{\text{out}} \in S_\lambda$.

For presentation convenience, we use the notation $\text{itr.\text{Iterate}}^j(\text{pp}_{\text{itr}}, v^0, (m^1, \ldots, m^j))$ to denote $v^j$ where $v^j \leftarrow \text{itr.\text{Iterate}}(\text{pp}_{\text{itr}}, v^{j-1}, m^j)$ for all $j \in [k]$.

**Security.** Let $\text{itr} = \text{itr}.\{\text{Setup, SetupEnforceIterator, Iterate}\}$, be an iterator with message space $\mathcal{M}_\lambda$ and state space $S_\lambda$. We require the following notions of security.

**Definition A.1** (Indistinguishability of Setup). An iterator $\text{itr}$ is said to satisfy indistinguishability of Setup phase if any PPT adversary $A$’s advantage in the security game Exp-Setup-Itr$(1^\lambda, \text{itr}, A)$ is at most negligible in $\lambda$, where Exp-Setup-Itr is defined as follows.

- **Exp-Setup-Itr$(1^\lambda, \text{itr}, A)$**
  - The adversary $A$ chooses a bound $N \in \Theta(2^\lambda)$ and sends it to the challenger.
  - $A$ sends $m$ to the challenger, where $m = (m^1, \ldots, m^k) \in (\mathcal{M}_\lambda)^k$.
  - The challenger chooses a bit $b$. If $b = 0$, the challenger outputs $(\text{pp}_{\text{itr}}, v^0) \leftarrow \text{itr.\text{Setup}}(1^\lambda, T)$. Else, it outputs $(\text{pp}_{\text{itr}}, v^0) \leftarrow \text{itr.\text{SetupEnforceIterator}}(1^\lambda, T, m)$ where $m = (m^1, \ldots, m^k) \in (\mathcal{M}_\lambda)^k$.
  - $A$ sends a bit $b'$.
  - $A$ wins the security game if $b = b'$.
Definition A.2 (Enforcing). Consider any $\lambda \in \mathbb{N}, T \in \Theta(2^\lambda), \mathbf{m} = (m^1, \ldots, m^k) \in (\mathcal{M}_\lambda)^k$. Let $(\mathsf{pp}_{\text{ltr}}, v^0) \leftarrow \text{SetupEnforceIterate}(1^\lambda, T, \mathbf{m})$ and $v^j = \text{litr}.\text{iterate}^j(\mathsf{pp}_{\text{ltr}}, v^0, (m^1, \ldots, m^k))$ for all $j \in [k]$. Then, ltr = ltr.\{\text{Setup, SetupEnforceIterate, Iterate}\} is said to be enforcing if $v^k = \text{litr}.\text{iterate}(\mathsf{pp}_{\text{ltr}}, v', m') \Rightarrow (v', m') = (v^{k-1}, m^k)$.

Note that this is an information-theoretic property.

A.3.2 Positional Accumulators

A positional accumulator [KLW15] is a cryptographic data structure which maintains a relatively large storage with a short accumulator value. The accumulator is designed in such a way that, given the last accumulator value and some new modification to the storage, a new accumulator value can be computed efficiently. While the accumulator value does not contain all the information about the storage, a “helper” algorithm allows the (untrusted) storage party who is maintaining the full storage to help the (restricted) computation party that has the accumulator value recover any data stored in arbitrary location. A positional accumulator for message space $\mathcal{M}_\lambda$ consists of the following algorithms.

Syntax.

- $	ext{Acc.Setup}(1^\lambda, S)$: The setup algorithm takes as input the security parameter $\lambda$ (in unary), and an integer bound $S$ (in binary) on the number of iterations. It outputs public parameters $\mathsf{pp}_{\text{Acc}}$ and an initial accumulator value $w^0$ and an initial storage value $\text{store}^0$.

- $	ext{Acc.SetupEnforceRead}(1^\lambda, S, (m_1, \text{index}_1), \ldots, (m_k, \text{index}_k), \text{index}^*)$: The setup enforce-read algorithm takes as input the security parameter $\lambda$ (in unary), an integer bound $S$ (in binary) representing the maximum number of values that can be stored, and a vector of symbol-index pairs where each index is in \{0, \ldots, S - 1\}, and an additional index* also in \{0, \ldots, S - 1\}. It outputs public parameters $\mathsf{pp}_{\text{Acc}}$ and an initial accumulator value $w^0$ and an initial storage value $\text{store}^0$.

- $	ext{Acc.SetupEnforceWrite}(1^\lambda, S, (m_1, \text{index}_1), \ldots, (m_k, \text{index}_k))$: The setup enforce-write algorithm takes as input the security parameter $\lambda$ (in unary), an integer bound $S$ (in binary) representing the maximum number of values that can be stored, and a vector of symbol-index pairs where each index is in \{0, \ldots, S - 1\}. It outputs public parameters $\mathsf{pp}_{\text{Acc}}$ and an initial accumulator value $w^0$ and an initial storage value $\text{store}^0$.

- $	ext{Acc.PrepRead}(\mathsf{pp}_{\text{Acc}}, \text{store}^\text{in}, \text{index})$: The prep-read algorithm takes as input the public parameters $\mathsf{pp}_{\text{Acc}}$, a storage value $\text{store}^\text{in}$, and an index $\in \{0, \ldots, S - 1\}$. It outputs a symbol $m$ (that can be $\emptyset$) and a value $\pi$.

- $	ext{Acc.PrepWrite}(\mathsf{pp}_{\text{Acc}}, \text{store}^\text{in}, \text{index})$: The prep-write algorithm takes as input the public parameters $\mathsf{pp}_{\text{Acc}}$, a storage value $\text{store}^\text{in}$, and an index $\in \{0, \ldots, S - 1\}$. It outputs an auxiliary value $\text{aux}$.

- $	ext{Acc.VerifyRead}(\mathsf{pp}_{\text{Acc}}, \text{w}^\text{in}, \text{m}^\text{read}, \text{index}, \pi)$: The verify-read algorithm takes as input the public parameters $\mathsf{pp}_{\text{Acc}}$, a accumulator value $\text{w}^\text{in}$, a symbol $\text{m}^\text{read}$, an index $\in \{0, \ldots, S - 1\}$, and a value $\pi$. It outputs True or False.

- $	ext{Acc.WriteStore}(\mathsf{pp}_{\text{Acc}}, \text{store}^\text{in}, \text{index}, m)$: The write-store algorithm takes as input the public parameters $\mathsf{pp}_{\text{Acc}}$, a storage value $\text{store}^\text{in}$, an index $\in \{0, \ldots, S - 1\}$, and a symbol $m$. It outputs a storage value $\text{store}^\text{out}$.

- $	ext{Acc.Update}(\mathsf{pp}_{\text{Acc}}, \text{w}^\text{in}, \text{m}^\text{write}, \text{index}, \pi)$: The update algorithm takes as input the public parameters $\mathsf{pp}_{\text{Acc}}$, an accumulator value $\text{w}^\text{in}$, a symbol $\text{m}^\text{write}$, an index $\in \{0, \ldots, S - 1\}$, and an auxiliary value $\text{aux}$. It outputs an accumulator value $\text{w}^\text{out}$ or Reject.

- $	ext{Acc.Combine}(\mathsf{pp}_{\text{Acc}}, h_1, h_2, \text{index})$: The update algorithm takes as input the public parameters $\mathsf{pp}_{\text{Acc}}$, two hashes $h_1, h_2 \in \{0, 1\}^\ell$, an index $\in \{0, 1\}^{\lfloor \log S \rfloor}$. It outputs another hash value $h^\text{out} \in \{0, 1\}^\ell$, which must be consistent with the output of Acc.Update after iterating over the whole storage $\text{store}$.
Security. Let Acc = Acc\{Setup, SetupEnforceRead, SetupEnforceWrite, PrepRead, PrepWrite, VerifyRead, WriteStore, Update\} be an accumulator with message space $\mathcal{M}_\lambda$ and state space $S_\lambda$. We require the following notions of security.

**Definition A.3** (Indistinguishability of Read-Setup). A positional accumulator Acc is said to satisfy indistinguishability of Read-Setup phase if any PPT adversary $\mathcal{A}$’s advantage in the security game Exp-Setup-Read$(1^\lambda, ltr, \mathcal{A})$ at most is negligible in $\lambda$, where Exp-Setup-Read is defined as follows.

\[
\text{Exp-Setup-Read}(1^\lambda, \text{Acc}, \mathcal{A})
\]

- The adversary $\mathcal{A}$ chooses a bound $S \in \Theta(2^\lambda)$ and sends it to challenger.
- $\mathcal{A}$ sends $k$ messages $m^1, \ldots, m^k \in \mathcal{M}_\lambda$ and $k$ indexes $\text{index}^1, \ldots, \text{index}^k \in \{0, \ldots, S - 1\}$.
- The challenger chooses a bit $b$. If $b = 0$, the challenger outputs $(\text{pp}_{\text{Acc}}, w^0, \text{store}^0) \leftarrow \text{Acc.Setup}(1^\lambda, S)$.
  - Else, it outputs $(\text{pp}_{\text{Acc}}, w^0, \text{store}^0) \leftarrow \text{Acc.SetupEnforceRead}(1^\lambda, S, (m^1, \text{index}^1), \ldots, (m^k, \text{index}^k))$.
- $\mathcal{A}$ sends a bit $b'$.
  - $\mathcal{A}$ wins the security game if $b = b'$.

**Definition A.4** (Indistinguishability of Write-Setup). A positional accumulator Acc is said to satisfy indistinguishability of Write-Setup phase if any PPT adversary $\mathcal{A}$’s advantage in the security game Exp-Setup-Write$(1^\lambda, ltr, \mathcal{A})$ at most is negligible in $\lambda$, where Exp-Setup-Write is defined as follows.

\[
\text{Exp-Setup-Write}(1^\lambda, \text{Acc}, \mathcal{A})
\]

- The adversary $\mathcal{A}$ chooses a bound $S \in \Theta(2^\lambda)$ and sends it to challenger.
- $\mathcal{A}$ sends $k$ messages $m^1, \ldots, m^k \in \mathcal{M}_\lambda$ and $k$ indexes $\text{index}^1, \ldots, \text{index}^k \in \{0, \ldots, S - 1\}$.
- The challenger chooses a bit $b$. If $b = 0$, the challenger outputs $(\text{pp}_{\text{Acc}}, w^0, \text{store}^0) \leftarrow \text{Acc.Setup}(1^\lambda, S)$.
  - Else, it outputs $(\text{pp}_{\text{Acc}}, w^0, \text{store}^0) \leftarrow \text{Acc.SetupEnforceWrite}(1^\lambda, S, (m^1, \text{index}^1), \ldots, (m^k, \text{index}^k))$.
- $\mathcal{A}$ sends a bit $b'$.
  - $\mathcal{A}$ wins the security game if $b = b'$.

**Definition A.5** (Read-Enforcing). Consider any $\lambda \in \mathbb{N}, S \in \Theta(2^\lambda), m^1, \ldots, m^k \in \mathcal{M}_\lambda, \text{index}^1, \ldots, \text{index}^k \in \{0, \ldots, S - 1\}$, and any $\text{index}^*$ $\notin \{\text{index}^1, \ldots, \text{index}^k\}$ and $m = \emptyset$, or $m = m^i$ for the largest $i \in [k]$ such that $\text{index}^i = \text{index}^*$. Then, Acc is said to be read-enforcing if VerifyRead(\text{pp}_{\text{Acc}}, w^k, m, \text{index}^*, \pi) = 1, then either $\text{index}^* \notin \{\text{index}^1, \ldots, \text{index}^k\}$ and $m = \emptyset, \text{or m} = m^i$ for the largest $i \in [k]$ such that $\text{index}^i = \text{index}^*$. Note that this is an information-theoretic property. We are requiring that for all other symbols $m$, values of $\pi$ that would cause VerifyRead to output 1 at $\text{index}^*$ do not exist.

**Definition A.6** (Write-Enforcing). Consider any $\lambda \in \mathbb{N}, S \in \Theta(2^\lambda), m^1, \ldots, m^k \in \mathcal{M}_\lambda, \text{index}^1, \ldots, \text{index}^k \in \{0, \ldots, S - 1\}$, and any $\text{index}^* \in \{0, \ldots, S - 1\}$.

\[
\text{Let (pp}_{\text{Acc}}, w^0, \text{store}^0) \leftarrow \text{Acc.SetupEnforceRead}(1^\lambda, S, (m^1, \text{index}^1), \ldots, (m^k, \text{index}^k), \text{index}^*).
\]

For all $j \in [k]$, we defined $\text{store}^j$ iteratively as $\text{store}^j := \text{WriteStore}(\text{pp}_{\text{Acc}}, \text{store}^j-1, \text{index}^j, m^j)$. We similarly define $\text{aux}^j$ and $w^j$ iteratively as $\text{aux}^j := \text{PrepWrite}(\text{pp}_{\text{Acc}}, \text{store}^j-1, \text{index}^j)$ and $w^j := \text{Update}(\text{pp}_{\text{Acc}}, w^j-1, m^j, \text{index}^j, \text{aux}^j)$.

Then, Acc is said to be write-enforcing if $\text{VerifyWrite}(\text{pp}_{\text{Acc}}, w^k, m, \text{index}^*, \pi) = 1$, then either $\text{index}^* \notin \{\text{index}^1, \ldots, \text{index}^k\}$ and $m = \emptyset, \text{or m} = m^i$ for the largest $i \in [k]$ such that $\text{index}^i = \text{index}^*$. Note that this is an information-theoretic property. We are requiring that for all other symbols $m$, values of $\pi$ that would cause VerifyWrite to output 1 at $\text{index}^*$ do not exist.
A.3.3 Splittable Signatures

Splittable signatures [KLW15] are normal signatures with additional algorithms and properties. In particular, the following keys are introduced:

- “All but one” keys function normally except for a particular message \( m^* \)
- “One” keys function only for a particular message \( m^* \)
- Reject-verification keys reject all signatures when used for verification

The security requirement of splittable signatures is weaker than that of normal signatures in the sense that no signing oracle is provided to the adversary. This weaker requirement is sufficient for applications and enables us to argue the indistinguishability between different types of verification keys.

Syntax. A splittable signature scheme Spl for message space \( \mathcal{M}_\lambda \) consists of the following algorithms:

- Setup: The setup algorithm is a randomized algorithm that takes as input the security parameter \( \lambda \) and outputs a signing key \( sk \), a verification key \( vk \), and reject-verification key \( vk_{rej} \)
- Sign: The signing algorithm is a deterministic algorithm that takes as input a signing key \( sk \), and a message \( m \in \mathcal{M}_\lambda \). It outputs a signature \( \sigma \).
- Verify: The verification algorithm is a deterministic algorithm that takes as input a verification key \( vk \), signature \( \sigma \), and a message \( m \). It outputs either 0 or 1.
- Split: The splitting algorithm is randomized. It takes as input a secret key \( sk \) and a message \( m^* \in \mathcal{M}_\lambda \). It outputs a signature \( \sigma_{one} \leftarrow \text{Sign}(sk, m^*) \), a one-message verification key \( vk_{one} \), an all-but-one signing key \( sk_{abo} \) and an all-but-one verification key \( vk_{abo} \).
- AboSign: The all-but-one signing algorithm is deterministic. It takes as input an all-but-one signing key \( sk_{abo} \) and a message \( m \), and outputs a signature \( \sigma \).

Correctness. Let \( m^* \in \mathcal{M}_\lambda \) be any message. Let \((sk, vk, vk_{rej}) \leftarrow \text{Spl.Setup}(1^\lambda) \) and \((\sigma_{one}, vk_{one}, sk_{abo}, vk_{abo}) \leftarrow \text{Spl.Split}(sk, m^*) \). Then, we require the following correctness properties:

1. For all \( m \in \mathcal{M}_\lambda \), \( \text{Spl.Verify}(vk, m, \text{Spl.Sign}(sk, m)) = 1 \).
2. For all \( m \in \mathcal{M}_\lambda \), \( m \neq m^* \), \( \text{Spl.Sign}(sk, m) = \text{Spl.AboSign}(sk_{abo}, m) \).
3. For all \( \sigma \), \( \text{Spl.Verify}(vk, m^*, \sigma) = \text{Spl.Verify}(vk, m^*, \sigma) \).
4. For all \( m \neq m^* \) and \( \sigma \), \( \text{Spl.Verify}(vk, m, \sigma) = \text{Spl.Verify}(vk_{abo}, m, \sigma) \).
5. For all \( m \neq m^* \) and \( \sigma \), \( \text{Spl.Verify}(vk_{one}, m, \sigma) = 0 \).
6. For all \( \sigma \) and all \( m \in \mathcal{M}_\lambda \), \( \text{Spl.Verify}(vk_{rej}, m, \sigma) = 0 \).
7. For all \( \sigma \) and all \( m \in \mathcal{M}_\lambda \), \( \text{Spl.Verify}(vk_{rej}, m, \sigma) = 0 \).

Security. We will now define the security notions for splittable signature schemes. Each security notion is defined in terms of a security game between a challenger and an adversary \( \mathcal{A} \).

Definition A.7 (\( vk_{rej} \) indistinguishability). A splittable signature scheme Spl is said to be \( vk_{rej} \) indistinguishable if any PPT adversary \( \mathcal{A} \) has negligible advantage in the following security game:

\( \text{Exp-}vk_{rej}(1^\lambda, \text{Spl}, \mathcal{A}) \)

- The challenger computes \((sk, vk, vk_{rej}) \leftarrow \text{Setup} \). It chooses a bit \( b \in \{0, 1\} \). If \( b = 0 \), the challenger sends \( vk \) to \( \mathcal{A} \). Else, it sends \( vk_{rej} \) to \( \mathcal{A} \).

81
– \(A\) sends a bit \(b'\).
\(A\) wins if \(b = b'\).

**Definition A.8** (\(\text{vk}_{\text{one}}\) indistinguishability). A splittable signature scheme \(\text{Spl}\) is said to be \(\text{vk}_{\text{one}}\) indistinguishable if any PPT adversary \(A\) has negligible advantage in the following security game:

\[
\text{Exp-}\text{vk}_{\text{one}}(1^\lambda, \text{Spl}, A)
\]

– \(A\) sends a message \(m^* \in M\).
– The challenger computes \((\text{sk}, \text{vk}, \text{vk}_{\text{rej}}) \leftarrow \text{Setup}\), and computes \((\sigma_{\text{one}}, \text{vk}_{\text{one}}, \text{sk}_{\text{abo}}, \text{vk}_{\text{abo}}) \leftarrow \text{Split}(\text{sk}, m^*)\).
  It chooses a bit \(b \in \{0, 1\}\). If \(b = 0\), the challenger sends \((\sigma_{\text{one}}, \text{vk}_{\text{one}})\) to \(A\). Else, it sends \((\sigma_{\text{one}}, \text{vk})\) to \(A\).
– \(A\) sends a bit \(b'\).
\(A\) wins if \(b = b'\).

**Definition A.9** (\(\text{vk}_{\text{abo}}\) indistinguishability). A splittable signature scheme \(\text{Spl}\) is said to be \(\text{vk}_{\text{abo}}\) indistinguishable if any PPT adversary \(A\) has negligible advantage in the following security game:

\[
\text{Exp-}\text{vk}_{\text{abo}}(1^\lambda, \text{Spl}, A)
\]

– \(A\) sends a message \(m^* \in M\).
– The challenger computes \((\text{sk}, \text{vk}, \text{vk}_{\text{rej}}) \leftarrow \text{Setup}\), and computes \((\sigma_{\text{one}}, \text{vk}_{\text{one}}, \text{sk}_{\text{abo}}, \text{vk}_{\text{abo}}) \leftarrow \text{Split}(\text{sk}, m^*)\).
  It chooses a bit \(b \in \{0, 1\}\). If \(b = 0\), the challenger sends \((\text{sk}_{\text{abo}}, \text{vk}_{\text{abo}})\) to \(A\). Else, it sends \((\text{sk}_{\text{abo}}, \text{vk})\) to \(A\).
– \(A\) sends a bit \(b'\).
\(A\) wins if \(b = b'\).

**Definition A.10** (Splitting indistinguishability). A splittable signature scheme \(\text{Spl}\) is said to be splitting indistinguishable if any PPT adversary \(A\) has negligible advantage in the following security game:

\[
\text{Exp-}\text{vk}_{\text{abo}}(1^\lambda, \text{Spl}, A)
\]

– \(A\) sends a message \(m^* \in M\).
– The challenger computes \((\text{sk}, \text{vk}, \text{vk}_{\text{rej}}) \leftarrow \text{Setup}(1^\lambda), (\text{sk}', \text{vk}', \text{vk}'_{\text{rej}}) \leftarrow \text{Setup}(1^\lambda), \) and computes \((\sigma_{\text{one}}, \text{vk}_{\text{one}}, \text{sk}_{\text{abo}}, \text{vk}_{\text{abo}}) \leftarrow \text{Split}(\text{sk}, m^*), (\sigma'_{\text{one}}, \text{vk}'_{\text{one}}, \text{sk}'_{\text{abo}}, \text{vk}'_{\text{abo}}) \leftarrow \text{Split}(\text{sk}', m^*)\).
  It chooses a bit \(b \in \{0, 1\}\). If \(b = 0\), the challenger sends \((\sigma_{\text{one}}, \text{vk}_{\text{one}}, \text{sk}_{\text{abo}}, \text{vk}_{\text{abo}})\) to \(A\). Else, it sends \((\sigma'_{\text{one}}, \text{vk}'_{\text{one}}, \text{sk}'_{\text{abo}}, \text{vk}'_{\text{abo}})\) to \(A\).
– \(A\) sends a bit \(b'\).
\(A\) wins if \(b = b'\).

**A.3.4 Indistinguishability Obfuscation for Circuits**

**Definition A.11** (Indistinguishability Obfuscation for Circuits [GGH+13, SW14]). Let \(C = \{C_\lambda\}_{\lambda \in \mathbb{N}}\) be a family of polynomial-size circuits. Let \(i\mathcal{O}\) be a uniform PPT algorithm that takes as input the security parameter \(\lambda\), a circuit \(C \in C_\lambda\) and outputs a circuit \(C'\). \(i\mathcal{O}\) is called an indistinguishability obfuscator for a circuit class \(\{C_\lambda\}_{\lambda \in \mathbb{N}}\) if it satisfies the following conditions:

– (Preserving Functionality.) For all security parameters \(\lambda \in \mathbb{N}\), for all circuits \(C \in C_\lambda\), for all inputs \(x\), we have that \(C'(x) = C(x)\) where \(C' \leftarrow i\mathcal{O}(1^\lambda, C)\).

– (Indistinguishability of Obfuscation.) For any (not necessarily uniform) PPT distinguisher \(B = (\text{Samp}, \mathcal{D})\), there exists a negligible function \(\text{negl}(\cdot)\) such that the following holds: if for all security parameters \(\lambda \in \mathbb{N}\),
  \[
  \Pr[\forall x, C_0(x) = C_1(x) : (C_0; C_1; \sigma) \leftarrow \text{Samp}(1^\lambda)] > 1 - \text{negl}(\lambda),
  \]
  then
  \[
  \Pr[\mathcal{D}(\sigma, i\mathcal{O}(1^\lambda, C_0))] = 1 : (C_0; C_1; \sigma) \leftarrow \text{Samp}(1^\lambda)]
  \]
  \[
  \Pr[\mathcal{D}(\sigma, i\mathcal{O}(1^\lambda, C_1))] = 1 : (C_0; C_1; \sigma) \leftarrow \text{Samp}(1^\lambda)] \leq \text{negl}(\lambda).
  \]
In addition, we require the efficiency of the input circuit to be preserved.

- (Preserving Efficiency.) For all security parameters \( \lambda \in \mathbb{N} \), for all circuits \( C \in \mathcal{C}_\lambda \), we have that \( |C'| = \text{poly}(\lambda)|C| \) where \( C' \leftarrow \mathcal{O}(1^\lambda, C) \).

### A.3.5 Puncturable Pseudorandom Functions

Puncturable Pseudorandom Functions [BW13, BGI14, KPTZ13, SW14] since introduced, have proven to be very powerful. We here review the definition.

#### Syntax.
A function \( \text{PRF} : \mathcal{K} \times \mathcal{X} \rightarrow \mathcal{Y} \) is a puncturable pseudorandom function if there is an additional key space \( \mathcal{K}_{\text{punct}} \) and three polynomial time algorithms \( \text{PPRF.Setup}, \text{PPRF.Puncture}, \) and \( \text{PPRF.Eval} \) as follows:

- \( \text{PPRF.Setup}(1^\lambda) \) is a randomized algorithm that takes the security parameter \( \lambda \) as input, and outputs a description of the key space \( \mathcal{K} \), the punctured key space \( \mathcal{K}_{\text{punct}} \), and the function \( \text{PRF} \).
- \( \text{PPRF.Puncture}(K, x) \) is a randomized algorithm that takes as input a PRF key \( K \in \mathcal{K} \) and \( x \in \mathcal{X} \), and outputs a key \( K \{x\} \in \mathcal{K}_{\text{punct}} \).
- \( \text{PPRF.Eval}(K \{x\}, x') \) is a deterministic algorithm that takes as input a punctured key \( K \{x\} \in \mathcal{K}_{\text{punct}} \) and \( x' \in \mathcal{X} \). Let \( K \in \mathcal{K} \), \( x \in \mathcal{X} \) and \( K \{x\} \leftarrow \text{PPRF.Puncture}(K, x) \). For correctness, we require:

\[
\text{PPRF.Eval}(K \{x\}, x') = \begin{cases} 
\text{PRF}(K, x') & \text{if } x' \neq x \\
\bot & \text{otherwise}
\end{cases}
\]

For convenience, we simply write \( \text{PRF}(K \{x\}, x') \) to denote \( \text{PPRF.Eval}(K \{x\}, x') \) when the context is clear.

#### Security.
We now define the selective security for puncturable PRFs.

**Definition A.12 (Selective Security).** We say a puncturable PRF scheme \( \text{PPRF} \) is selectively secure if for all probabilistic polynomial time adversaries \( A \), its advantage \( \text{Adv}_{A, \text{PPRF}}(\lambda) \) in the following security game is negligible in \( \lambda \):

**Challenge Phase.** \( A \) sends a challenge \( x^* \in \mathcal{X} \). The challenger chooses uniformly at random a PRF key \( K \leftarrow \mathcal{K} \) and a bit \( b \leftarrow \{0, 1\} \). It computes \( K \{x^*\} \leftarrow \text{PPRF.Puncture}(K, x^*) \). If \( b = 0 \), the challenger sets \( y = \text{PRF}(K, x^*) \), else it chooses uniformly at random \( y \leftarrow \mathcal{Y} \). It sends \( K \{x^*\}, y \) to \( A \).

**Guess Phase.** \( A \) outputs a guess \( b' \) of \( b \).

\( A \) wins if \( b = b' \). The advantage of \( A \) is defined to be \( \text{Adv}_{A, \text{PPRF}}(\lambda) = \Pr[A \text{ wins}] - \frac{1}{2} \).
B Security Proofs

B.1 Proof of Theorem 6.2 (Security for CiO-RAM)

Proof. Let Adv\(_A^x\) denote the advantage of the adversary A in the hybrid Hyb\(_x\). We first define the first-layer hybrids Hyb\(_i\) for \(i \in \{0, 1\}\).

Hyb\(_i\) for \(i \in \{0, 1\}\). In this hybrid, the challenger outputs an obfuscation computation system of \(\Pi^i\) where stateful algorithm \(\hat{F}_i\) is defined in Algorithm 23.

Let us assume the obfuscated computation system terminates at time \(t^* < T\). We argue that \(|\text{Adv}_A^0 - \text{Adv}_A^1| \leq \text{negl}(\lambda)|\). To show this, we define the second-layer hybrids Hyb\(_{0,1}\), Hyb\(_{0,2}\), Hyb\(_{0,3}\) and Hyb\(_{0,4}\). We also define important third-layer hybrids Hyb\(_{0,2,i}\) and Hyb\(_{0,2',i}\) for \(0 \leq i < t^*\).

Hyb\(_{0,0}\). This hybrid is identical to Hyb\(_0\) in the first layer.

Hyb\(_{0,1}\). In this hybrid, the challenger outputs an obfuscation of \(\hat{F}^{0,1}\) defined in Algorithm 25. This program is similar to \(\hat{F}^0\) except that it has PRF key \(K_2\) hardwired, accepts both ‘A’ and ‘B’ type signatures for \(t < t^*\). The type of the outgoing signature follows the type of the incoming signature. Also, if the incoming signature is ‘B’ type and \(t < t^*\), then the program uses \(F_1\) to compute the output.

Hyb\(_{0,2}\). This hybrid is identical to Hyb\(_{0,2,0}\) defined below.

Hyb\(_{0,2,i}\). In this hybrid, based on the initial configuration \((\text{mem}^0, \text{st}^0, a^0_{i=0}, \text{mem}^0_0, \text{st}^0_0 = \bot, a^0_{i=\bot} = \bot)\), the challenger computes \(m_i\) as follows:

Then the challenger outputs an obfuscation of \(\hat{F}^{0,2,i}\) defined in Algorithm 26. This program is similar to \(\hat{F}^{0,1}\) except that it accepts ‘B’ type signatures only for inputs corresponding to \(i + 1 \leq t \leq t^* - 1\). It also has the correct output message \(m_i\) for step \(i\) hardwired. For \(i + 1 \leq t \leq t^* - 1\), the type of the outgoing signature follows the type of the incoming signature. At \(t = i\), it outputs an ‘A’ type signature if \(m^{\text{out}} = m_i\), and outputs ‘B’ type signature otherwise.

Hyb\(_{0,2',i}\). In this hybrid, the challenger outputs an obfuscation of \(\hat{F}^{0,2',i}\) defined in Algorithm 27. This program is similar to \(\hat{F}^{0,2,i}\) except that it accepts ‘B’ type signatures only for inputs corresponding to \(i + 2 \leq t \leq t^* - 1\). It also has the correct input message \(m_i\) for step \(i + 1\) hardwired. For \(i + 2 \leq t \leq t^* - 1\), the type of the outgoing signature follows the type of the incoming signature. At \(t = i + 1\), it outputs an ‘A’ type signature if \(m^{\text{in}} = m_i\), and outputs ‘B’ type signature otherwise.

Hyb\(_{0,3}\). In this hybrid, the challenger outputs an obfuscation of \(\hat{F}^{0,3}\) defined in Algorithm 28. This program is similar to \(\hat{F}^{0,2',t^*-1}\), except that it does not output ‘B’ type signatures.

Hyb\(_{0,4}\). In this hybrid, the challenger outputs the obfuscation of \(\hat{F}^{0,4}\) defined in Algorithm 29. This program outputs Reject for all \(t > t^*\) including the case when the signature is a valid ‘A’ type signature.
Analysis. In the remaining of this subsection, we prove Lemmas B.1, B.9, B.23, B.33, and B.37.

By Lemma B.1, we have $|\text{Adv}_A^0 - \text{Adv}_A^{0,1}| \leq \text{negl}(\lambda)$. Since $\hat{F}^{0,1}$ and $\hat{F}^{0,2,0}$ have identical functionality, we have $|\text{Adv}_A^{0,1} - \text{Adv}_A^{0,2,0}| \leq \text{negl}(\lambda)$. By Lemma B.9, we have $|\text{Adv}_A^{0,2,i} - \text{Adv}_A^{0,2,i-1}| \leq \text{negl}(\lambda)$ for $0 \leq i \leq t^* - 1$. By Lemma B.23, we have $|\text{Adv}_A^{0,2,i} - \text{Adv}_A^{0,2,i+1}| \leq \text{negl}(\lambda)$ for $0 \leq i \leq t^* - 2$. By Lemma B.33, we have $|\text{Adv}_A^{0,3} - \text{Adv}_A^{0,4}| \leq \text{negl}(\lambda)$. Summarizing the above, we have $|\text{Adv}_A^0 - \text{Adv}_A^1| \leq \text{negl}(\lambda)$.

Symmetrically, we can show that $|\text{Adv}_A^0 - \text{Adv}_A^1| \leq \text{negl}(\lambda)$. Finally, we can conclude that $|\text{Adv}_A^0 - \text{Adv}_A^1| \leq \text{negl}(\lambda)$, which completes the proof.

$\square$

Algorithm 23: $\hat{F}^i$

<table>
<thead>
<tr>
<th>Input</th>
<th>$st^\text{in} = (t, st^\text{in}, v^\text{in}, w^\text{in}, \sigma^\text{in})$, $\overline{a}<em>{\text{sk}-M} = (a</em>{\text{sk}-M}^\text{in}, \pi^\text{in})$ where $a_{\text{sk}-M}^\text{in} = (I^\text{in}, B^\text{in})$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>$T$, $pp_{\text{Acc}}, p_{\text{Itr}}, K_A$</td>
</tr>
<tr>
<td>1</td>
<td>If Acc.VerifyRead($pp_{\text{Acc}}, w^\text{in}, I^\text{in}, B^\text{in}, \pi^\text{in}$) = 0 output Reject;</td>
</tr>
<tr>
<td>2</td>
<td>Compute $r_A = \text{PRF}(K_A, t - 1)$;</td>
</tr>
<tr>
<td>3</td>
<td>Compute $(sk_A, vk_A, vk_{A,\text{rej}}) = \text{Spl.Setup}(1^\lambda; r_A)$;</td>
</tr>
<tr>
<td>4</td>
<td>Set $m^\text{in} = (v^\text{in}, st^\text{in}, w^\text{in}, I^\text{in})$;</td>
</tr>
<tr>
<td>5</td>
<td>If Spl.Verify($vk_A, m^\text{in}, \sigma^\text{in}$) = 0 output Reject;</td>
</tr>
<tr>
<td>6</td>
<td>Compute $(st^\text{out}, a_{\text{Mk}^{-\text{A}}}^\text{out}) \leftarrow F^i(st^\text{in}, a_{\text{Mk}^{-\text{A}}}^\text{in})$;</td>
</tr>
<tr>
<td>7</td>
<td>If $st^\text{out} = \text{Reject}$, output Reject;</td>
</tr>
<tr>
<td>8</td>
<td>$w^\text{out} = \text{Acc.Update}(pp_{\text{Acc}}, w^\text{in}, B^\text{out}, \pi^\text{in})$;</td>
</tr>
<tr>
<td>9</td>
<td>If $w^\text{out} = \text{Reject}$ output Reject;</td>
</tr>
<tr>
<td>10</td>
<td>Compute $\overline{v}^\text{out} = \text{Itr.Iterate}(pp_{\text{Itr}}, t^\text{in}, (st^\text{in}, w^\text{in}, I^\text{in}))$;</td>
</tr>
<tr>
<td>11</td>
<td>If $\overline{v}^\text{out} = \text{Reject}$ output Reject;</td>
</tr>
<tr>
<td>12</td>
<td>Compute $r'_A = \text{PRF}(K_A, t)$;</td>
</tr>
<tr>
<td>13</td>
<td>Compute $(sk'_A, vk'<em>A, vk'</em>{A,\text{rej}}) = \text{Spl.Setup}(1^\lambda; r'_A)$;</td>
</tr>
<tr>
<td>14</td>
<td>Set $m^\text{out} = (v^\text{out}, st^\text{out}, w^\text{out}, I^\text{out})$;</td>
</tr>
<tr>
<td>15</td>
<td>Compute $\sigma^\text{out} = \text{Spl.Sign}(sk'_A, m^\text{out})$;</td>
</tr>
<tr>
<td>16</td>
<td>Output $\overline{st}^\text{out} = (t + 1, st^\text{out}, v^\text{out}, w^\text{out}, \sigma^\text{out})$, $\overline{a}<em>{\text{Mk}^{-\text{A}}}^\text{out} = a</em>{\text{Mk}^{-\text{A}}}^\text{out}$;</td>
</tr>
</tbody>
</table>

Algorithm 24: This algorithm is used in $\text{Hyb}_{0,2,i}$

<table>
<thead>
<tr>
<th>for $j \in {1, \ldots, i}$ do</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
</tbody>
</table>
Algorithm 25: $\hat{F}^{0,1}$

\textbf{Input}: \(\tilde{\text{st}}^\text{in} = (t, \text{st}^\text{in}, v^\text{in}, w^\text{in}, \sigma^\text{in})\), \(\tilde{\alpha}^\text{in} = (\alpha^\text{in}_{k-M}, \pi^\text{in})\) where \(\alpha^\text{in}_{k-M} = (\Gamma^\text{in}, \Theta^\text{in})\)

\textbf{Data}: \(T, \text{pp}_{\text{Acc}}, \text{pp}_{\text{Itr}}, K_A, K_B\)

1. If \(\text{Acc}\.\text{VerifyRead}(\text{pp}_{\text{Acc}}, w^\text{in}, \Gamma^\text{in}, \Theta^\text{in}, \pi^\text{in}) = 0\) output \text{Reject};
2. Compute \(r_A = \text{PRF}(K_A, t - 1), r_B = \text{PRF}(K_B, t - 1);\)
3. Compute \((\text{sk}_A, \text{vk}_A, \text{vk}_{A,\text{rej}}) = \text{Spl.Setup}(1^\lambda; r_A), (\text{sk}_B, \text{vk}_B, \text{vk}_{B,\text{rej}}) = \text{Spl.Setup}(1^\lambda; r_B);\)
4. Set \(m^\text{in} = (v^\text{in}, \text{st}^\text{in}, w^\text{in}, \Gamma^\text{in})\) and \(\alpha = \text{\_\_\_\_};\)
5. If \(\text{Spl.Verify}(\text{vk}_A, m^\text{in}, \sigma^\text{in}) = 1\) set \(\alpha = \text{A};\)
6. If \(\alpha = \text{\_\_\_\_} \) and \(t > t^*\) output \text{Reject};
7. If \(\alpha \neq \text{A} \) and \(\text{Spl.Verify}(\text{vk}_B, m^\text{in}, \sigma^\text{in}) = 1\) set \(\alpha = \text{B};\)
8. If \(\alpha = \text{\_\_\_\_} \) output \text{Reject};

9. if \(\alpha = \text{B} \) then
10. \hspace{1em} Compute \((\text{st}^\text{out}, a^\text{out}_{k-A}) \leftarrow F^1(\text{st}^\text{in}, a^\text{in}_{k-M})\)
11. else
12. \hspace{1em} Compute \((\text{st}^\text{out}, a^\text{out}_{k-A}) \leftarrow F^0(\text{st}^\text{in}, a^\text{in}_{k-M})\)
13. If \(\text{st}^\text{out} = \text{Reject}, \text{output} \text{Reject};\)

14. \(w^\text{out} = \text{Acc.Update}(\text{pp}_{\text{Acc}}, w^\text{in}, \Theta^\text{out}, \pi^\text{in});\)
15. If \(w^\text{out} = \text{Reject} \) output \text{Reject};
16. Compute \(u^\text{out} = \text{Itr}\_\text{Itrate}(\text{pp}_{\text{Itr}}, v^\text{in}, (\text{st}^\text{in}, w^\text{in}, \Gamma^\text{in}));\)
17. If \(\text{u}^\text{out} = \text{Reject} \) output \text{Reject};
18. Compute \(r'_A = \text{PRF}(K_A, t), r'_B = \text{PRF}(K_B, t);\)
19. Compute \((\text{sk}'_A, \text{vk}'_A, \text{vk}'_{A,\text{rej}}) = \text{Spl.Setup}(1^\lambda; r'_A), (\text{sk}'_B, \text{vk}'_B, \text{vk}'_{B,\text{rej}}) = \text{Spl.Setup}(1^\lambda; r'_B);\)
20. Set \(m'^\text{out} = (u^\text{out}, \text{st}^\text{out}, w^\text{out}, \Gamma^\text{out});\)
21. Compute \(\sigma^\text{out} = \text{Spl.Sign}(\text{sk}'_A, m'^\text{out});\)
22. Output \(\tilde{\text{st}}^\text{out} = (t + 1, \text{st}^\text{out}, u^\text{out}, w^\text{out}, \sigma^\text{out} ), \tilde{\alpha}^\text{out}_{k-A} = a^\text{out}_{k-A};\)
Algorithm 26: $\hat{F}_{0,2,i}$

Input: $\hat{\sigma}^\text{in} = (t, \hat{s}^\text{in}, v^\text{in}, w^\text{in}, \sigma^\text{in})$, $\overrightarrow{\alpha}^\text{in}_{\text{out}} = (\overrightarrow{a}^\text{in}_{\text{out}}, \overrightarrow{\pi}^\text{in})$ where $\overrightarrow{a}^\text{in}_{\text{out}} = (\overrightarrow{I}^\text{in}, \overrightarrow{B}^\text{in})$

Data: $T, \text{pp}_{\text{Acc}}, \text{pp}_{\text{itr}}, K_A, K_B, m^i$

1. If $\text{Acc.\!VerifyRead} (\text{pp}_{\text{Acc}}, w^\text{in}, \overrightarrow{I}^\text{in}, \overrightarrow{B}^\text{in}, \overrightarrow{\pi}^\text{in}) = 0$ output Reject;
2. Compute $r_A = \text{PRF}(K_A, t - 1), r_B = \text{PRF}(K_B, t - 1)$;
3. Compute $(\text{sk}_A, \text{vk}_A, \text{vk}_{A,\text{rej}}) = \text{Spl.\!Setup}(1^\lambda; r_A), (\text{sk}_B, \text{vk}_B, \text{vk}_{B,\text{rej}}) = \text{Spl.\!Setup}(1^\lambda; r_B)$;
4. Set $m^\text{in} = (v^\text{in}, \hat{s}^\text{in}, w^\text{in}, \overrightarrow{I}^\text{in})$ and $\alpha = \text{\textquoteleft\textquoteleft}$;
5. If $\text{Spl.\!Verify}(\text{vk}_A, m^\text{in}, \sigma^\text{in}) = 1$ set $\alpha = \text{\textquoteleft}A\textquoteright$;
6. If $\alpha = \text{\textquoteleft}\text{\textquoteleft}$ and $(t > t^* \text{ or } t < i)$ output Reject;
7. If $\alpha \neq \text{\textquoteleft}A\textquoteright$ and $\text{Spl.\!Verify}(\text{vk}_B, m^\text{in}, \sigma^\text{in}) = 1$ set $\alpha = \text{\textquoteleft}B\textquoteright$;
8. If $\alpha = \text{\textquoteleft}\text{\textquoteleft}$ output Reject;

9. If $\alpha = \text{\textquoteleft}B\textquoteright$ or $t < i$ then
10. Compute $(\text{st}^\text{out}, \overrightarrow{a}^\text{out}_{\text{out}}) \leftarrow F^1(\hat{s}^\text{in}, \alpha^\text{in}_{\text{out}})$
11. Else
12. Compute $(\text{st}^\text{out}, \overrightarrow{a}^\text{out}_{\text{out}}) \leftarrow F^0(\hat{s}^\text{in}, \alpha^\text{in}_{\text{out}})$
13. If $\text{st}^\text{out} = \text{Reject}$ output Reject;

14. $w^\text{out} = \text{Acc.\!Update}(\text{pp}_{\text{Acc}}, w^\text{in}, \overrightarrow{B}^\text{out}, \overrightarrow{\pi}^\text{in})$;
15. If $w^\text{out} = \text{Reject}$ output Reject;
16. Compute $v^\text{out} = \text{itr.\!Detect}(\text{pp}_{\text{itr}}, v^\text{in}, (\text{st}^\text{in}, w^\text{in}, \overrightarrow{I}^\text{in}))$;
17. If $v^\text{out} = \text{Reject}$ output Reject;
18. Compute $r'_A = \text{PRF}(K_A, t), r'_B = \text{PRF}(K_B, t)$;
19. Compute $(\text{sk}'_A, \text{vk}'_A, \text{vk}_{A,\text{rej}}) = \text{Spl.\!Setup}(1^\lambda; r'_A), (\text{sk}'_B, \text{vk}'_B, \text{vk}_{B,\text{rej}}) = \text{Spl.\!Setup}(1^\lambda; r'_B)$;
20. Set $m^\text{out} = (v^\text{out}, \text{st}^\text{out}, w^\text{out}, \overrightarrow{I}^\text{out})$;
21. If $t = i$ and $m^\text{out} = m^i$ then
22. Compute $\sigma^\text{out} = \text{Spl.\!Sign}(\text{sk}'_A, m^\text{out})$;
23. Else if $t = i$ and $m^\text{out} \neq m^i$ then
24. Compute $\sigma^\text{out} = \text{Spl.\!Sign}(\text{sk}'_B, m^\text{out})$;
25. Else
26. Compute $\sigma^\text{out} = \text{Spl.\!Sign}(\text{sk}'_A, m^\text{out})$;

27. Output $\text{st}^\text{out} = (t + 1, \text{st}^\text{out}, v^\text{out}, w^\text{out}, \sigma^\text{out})$, $\overrightarrow{a}^\text{out}_{\text{out}} = \overrightarrow{a}^\text{out}_{\text{out}}$.
Algorithm 27: $\tilde{F}_{0,2',i}$

**Input**: $s^n = (t, s^{in}, v^{in}, w^{in}, \sigma^{in})$, $\tilde{a}^{in}_{H-M} = (a^{in}_{H-M}, \pi^{in})$ where $a^{in}_{H-M} = (I^{in}, B^{in})$

**Data**: $T, pp_{Acc}, pp_{Itr}, K_A, K_B, m^i$

1. If $Acc\cdot VerifyRead(pp_{Acc}, w^{in}, I^{in}, B^{in}, \pi^{in}) = 0$ output Reject;
2. Compute $r_A = PRF(K_A, t - 1), r_B = PRF(K_B, t - 1)$;
3. Compute $(sk_A, vk_A, vk_{A, rej}) = Spl.Setup(1^{\lambda}; r_A), (sk_B, vk_B, vk_{B, rej}) = Spl.Setup(1^{\lambda}; r_B)$;
4. Set $m^{in} = (v^{in}, st^{in}, w^{in}, I^{in})$ and $\alpha = \cdot$;
5. If $Spl.Verify(vk_A, m^{in}, \sigma^{in}) = 1$ set $\alpha = 'A'$;
6. If $\alpha = \cdot$ and ($t > t^* \text{ or } t \leq i + 1$) output Reject;
7. If $\alpha \neq 'A'$ and $Spl.Verify(vk_B, m^{in}, \sigma^{in}) = 1$ set $\alpha = 'B'$;
8. If $\alpha = \cdot$ output Reject;
9. if $\alpha = 'B'$ or $t \leq i + 1$ then
   10. Compute $(st^{out}, a_{H-M}^{out}) \leftarrow F^1(st^{in}, a_{H-M}^{in})$
   else
   11. Compute $(st^{out}, a_{H-M}^{out}) \leftarrow F^0(st^{in}, a_{H-M}^{in})$
12. If $(st^{out} = Reject, output Reject$;
13. $w^{out} = Acc\cdot Update(pp_{Acc}, w^{in}, B^{out}, \pi^{in})$;
14. If $w^{out} = Reject$ output Reject;
15. Compute $v^{out} = Itr\cdot Iterate(pp_{Itr}, v^{in}, (st^{in}, w^{in}, I^{in}))$;
16. If $v^{out} = Reject$ output Reject;
17. Compute $r'_A = PRF(K_A, t), r'_B = PRF(K_B, t)$;
18. Compute $(sk'_A, vk'_A, vk'_{A, rej}) = Spl.Setup(1^{\lambda}; r'_A), (sk'_B, vk'_B, vk'_{B, rej}) = Spl.Setup(1^{\lambda}; r'_B)$;
19. Set $m^{out} = (v^{out}, st^{out}, w^{out}, I^{out})$;
20. if $t = i + 1 \text{ and } m^{in} = m^i$ then
   21. Compute $\sigma^{out} = Spl\cdot Sign(sk'_A, m^{out})$;
   else if $t = i + 1 \text{ and } m^{in} \neq m^i$ then
   22. Compute $\sigma^{out} = Spl\cdot Sign(sk'_B, m^{out})$;
   else
   23. Compute $\sigma^{out} = Spl\cdot Sign(sk'_A, m^{out})$;
24. Output $st^{out} = (t + 1, st^{out}, v^{out}, w^{out}, \sigma^{out}), a_{H-M}^{out} = a_{H-M}^{out}$.
Algorithm 28: $\tilde{F}^{0.3}$

Input: $\tilde{\text{st}}^{in} = (t, \text{st}^{in}, v^{in}, w^{in}, \sigma^{in})$, $\tilde{a}_{a^k-M}^{in} = (a_{a^k-M}^{in}, \pi^{in})$ where $a_{a^k-M}^{in} = (I^{in}, B^{in})$

Data: $T$, $\text{pp}_{\text{Acc}}$, $\text{pp}_{\text{itr}}$, $K_A$, $K_B$, $t^*$

1. If $\text{Acc}.\text{VerifyRead}(\text{pp}_{\text{Acc}}, w^{in}, I^{in}, B^{in}, \pi^{in}) = 0$ output Reject;
2. Compute $r_A = \text{PRF}(K_A, t - 1)$, $r_B = \text{PRF}(K_B, t - 1)$;
3. Compute $(\text{sk}_A, \text{vk}_A, \text{vk}_A, \text{rej}) = \text{Spl}.\text{Setup}(1^\lambda; r_A)$, $(\text{sk}_B, \text{vk}_B, \text{vk}_B, \text{rej}) = \text{Spl}.\text{Setup}(1^\lambda; r_B)$;
4. Set $m^{in} = (v^{in}, \text{st}^{in}, w^{in}, I^{in})$;
5. If $\text{Spl}.\text{Verify}(\text{vk}_A, m^{in}, \sigma^{in}) = 0$ output Reject;
6. if $t \leq t^*$ then
   7. Compute $(\text{st}^{out}, a_{a^k-M}^{out}) \leftarrow F^1(\text{st}^{in}, a_{a^k-M}^{in})$
   8. else
   9. Compute $(\text{st}^{out}, a_{a^k-M}^{out}) \leftarrow F^0(\text{st}^{in}, a_{a^k-M}^{in})$
10. If $\text{st}^{out} = \text{Reject}$, output Reject;
11. $w^{out} = \text{Acc}.\text{Update}(\text{pp}_{\text{Acc}}, w^{in}, B^{out}, \pi^{in})$;
12. If $w^{out} = \text{Reject}$ output Reject;
13. Compute $v^{out} = \text{itr}.\text{Iterate}(\text{pp}_{\text{itr}}, v^{in}, (\text{st}^{in}, w^{in}, I^{in}))$;
14. If $v^{out} = \text{Reject}$ output Reject;
15. Compute $r'_A = \text{PRF}(K_A, t)$, $r'_B = \text{PRF}(K_B, t)$;
16. Compute $(\text{sk}'_A, \text{vk}'_A, \text{vk}'_A, \text{rej}) = \text{Spl}.\text{Setup}(1^\lambda; r'_A)$, $(\text{sk}'_B, \text{vk}'_B, \text{vk}'_B, \text{rej}) = \text{Spl}.\text{Setup}(1^\lambda; r'_B)$;
17. Set $m^{out} = (v^{out}, \text{st}^{out}, w^{out}, I^{out})$;
18. if $t = t^*$ then
   19. Compute $\sigma^{out} = \text{Spl}.\text{Sign}(\text{sk}'_B, m^{out})$;
   20. else
   21. Compute $\sigma^{out} = \text{Spl}.\text{Sign}(\text{sk}'_A, m^{out})$;

22. Output $\tilde{\text{st}}^{out} = (t + 1, \text{st}^{out}, v^{out}, w^{out}, \sigma^{out})$, $\tilde{a}_{a^k-M}^{out} = a_{a^k-M}^{out}$;
Algorithm 29: $\hat{F}^{0,4}$

\textbf{Input}: $\tilde{\text{st}}^\text{in} = (t, \text{st}^\text{in}, v^\text{in}, w^\text{in}, \sigma^\text{in})$, $\tilde{a}^\text{in}_{M} = (a^\text{in}_{M}, \pi^\text{in})$ where $a^\text{in}_{M} = (\text{I}^\text{in}, \text{B}^\text{in})$

\textbf{Data}: $T$, $\text{pp}_{\text{Acc}}$, $\text{pp}_{\text{Itr}}$, $K_{A}$, $K_{B}$, $t^*$

1. If $t > t^*$ output \text{Reject};
2. If $\text{Acc.\,Verify\,Read}(\text{pp}_{\text{Acc}}, w^\text{in}, \text{I}^\text{in}, \text{B}^\text{in}, \pi^\text{in}) = 0$ output \text{Reject};
3. Compute $r_{A} = \text{PRF}(K_{A}, t - 1)$, $r_{B} = \text{PRF}(K_{B}, t - 1)$;
4. Compute $(\text{sk}_{A}, \text{vk}_{A}, \text{vk}_{A,\text{rej}}) = \text{Spl.\,Setup}(1^\lambda; r_{A})$, $(\text{sk}_{B}, \text{vk}_{B}, \text{vk}_{B,\text{rej}}) = \text{Spl.\,Setup}(1^\lambda; r_{B})$;
5. Set $m^\text{in} = (v^\text{in}, \text{st}^\text{in}, w^\text{in}, \text{I}^\text{in})$;
6. If $\text{Spl.\,Verify}(\text{vk}_{A}, m^\text{in}, \sigma^\text{in}) = 0$ output \text{Reject};
7. if $t \leq t^*$ then
8. \hspace{1em} Compute $(\text{st}^\text{out}, a^\text{out}_{M}) \leftarrow F^1(\text{st}^\text{in}, a^\text{in}_{M})$
9. \hspace{1em} If $\text{st}^\text{out} = \text{Reject}$, output \text{Reject};
10. $w^\text{out} = \text{Acc.\,Update}(\text{pp}_{\text{Acc}}, w^\text{in}, \text{B}^\text{out}, \pi^\text{in})$;
11. If $w^\text{out} = \text{Reject}$ output \text{Reject};
12. Compute $v^\text{out} = \text{Itr.\,Iterate}(\text{pp}_{\text{Itr}}, v^\text{in}, (\text{st}^\text{in}, w^\text{in}, \text{I}^\text{in}))$;
13. If $v^\text{out} = \text{Reject}$ output \text{Reject};
14. Compute $r'_{A} = \text{PRF}(K_{A}, t)$, $r'_{B} = \text{PRF}(K_{B}, t)$;
15. Compute $(\text{sk}'_{A}, \text{vk}'_{A}, \text{vk}'_{A,\text{rej}}) = \text{Spl.\,Setup}(1^\lambda; r'_{A})$, $(\text{sk}'_{B}, \text{vk}'_{B}, \text{vk}'_{B,\text{rej}}) = \text{Spl.\,Setup}(1^\lambda; r'_{B})$;
16. Set $m^\text{out} = (v^\text{out}, \text{st}^\text{out}, w^\text{out}, \text{I}^\text{out})$;
17. if $t = t^*$ then
18. \hspace{1em} Compute $\sigma^\text{out} = \text{Spl.\,Sign}(\text{sk}'_{B}, m^\text{out})$;
19. \hspace{1em} else
20. \hspace{2em} Compute $\sigma^\text{out} = \text{Spl.\,Sign}(\text{sk}'_{A}, m^\text{out})$;
21. Output $\tilde{\text{st}}^\text{out} = (t + 1, \text{st}^\text{out}, v^\text{out}, w^\text{out}, \sigma^\text{out})$, $\tilde{a}^\text{out}_{M} = a^\text{out}_{M}$;
B.1.1 From Hyb\(_{0,0}\) to Hyb\(_{0,1}\):

**Lemma B.1.** Let iO be a secure indistinguishability obfuscator, PRF be a selectively secure puncturable PRF and Spl be a secure splittable signature scheme. Then for any PPT adversary \(A\), \(|\text{Adv}\_A^0 - \text{Adv}\_A^{0,1}| \leq \text{negl}(\lambda)|.\)

**Proof:** We define third layer hybrids \(\text{Hyb}_{0,i}\) where \(i \in \{0, 1, \ldots, t^*\}\).

\(\text{Hyb}_{0,i}\). In this hybrid, the challenger outputs an obfuscation of \(\tilde{\mathcal{F}}_{0,i}\) defined in Algorithm 30. This program is similar to \(\tilde{\mathcal{F}}_0\) except that it has PRF key \(K_B\) hardwired, accepts both ‘A’ and ‘B’ type signatures for \(i < t \leq t^*\). The type of the outgoing signature follows the type of the incoming signature.

We observe that hybrids \(\text{Hyb}_{0,0,0}\) and \(\text{Hyb}_{0,1}\) are identical. In addition, hybrids \(\text{Hyb}_{0,i,t}\) and \(\text{Hyb}_{0,0}\) are functionally identical, since the difference between these two hybrids is a dummy code which has never been executed. Therefore, it suffices to show that \(\text{Hyb}_{0,0,i}\) and \(\text{Hyb}_{0,0,i-1}\) are computationally indistinguishable for \(0 \leq i \leq t^*\), which is implied by Lemma B.2.

\[ \square \]

---

**Algorithm 30:** \(\tilde{\mathcal{F}}_{0,i}\)

\[
\begin{align*}
\text{Input} & : \tilde{\mathcal{I}}^\text{in} = (t, \tilde{s}^\text{in}_\text{A}, \tilde{v}^\text{in}_\text{A}, \tilde{w}^\text{in}, \sigma^\text{in}), \tilde{\alpha}^\text{in}_\text{A} = (\tilde{a}^\text{in}_\text{A}, \pi^\text{in}) \quad \text{where} \quad \tilde{a}^\text{in}_\text{A} = (\tilde{I}^\text{in}, \tilde{B}^\text{in}) \\
\text{Data} & : T, \text{pp}_\text{Acc}, \text{pp}_\text{itr}, K_A, K_B \\
1 & \text{If Acc.VerifyRead}((\text{pp}_\text{Acc}, \tilde{w}^\text{in}, \tilde{I}^\text{in}, \tilde{B}^\text{in}, \pi^\text{in}) = 0 \text{ output Reject}; \\
2 & \text{Compute } r_A = \text{PRF}(K_A, t - 1), r_B = \text{PRF}(K_B, t - 1); \\
3 & \text{Compute } (\text{sk}_A, \text{vk}_A, \text{vk}_A) = \text{Spl.Setup}(1^\lambda; r_A), (\text{sk}_B, \text{vk}_B, \text{vk}_B) = \text{Spl.Setup}(1^\lambda; r_B); \\
4 & \text{Set } m^\text{in} = (\tilde{v}^\text{in}, \tilde{s}^\text{in}_\text{A}, \tilde{w}^\text{in}, \tilde{I}^\text{in}) \text{ and } \alpha = \tilde{\alpha}; \\
5 & \text{If Spl.Verify}(\text{vk}_A, m^\text{in}, \sigma^\text{in}) = 1 \text{ set } \alpha = \text{‘A’ } ; \\
6 & \text{If } \alpha = \tilde{\alpha} \text{ and } (t > t^* \text{ or } t \leq i) \text{ output Reject}; \\
7 & \text{If } \alpha = \tilde{\alpha} \text{ and } \text{Spl.Verify}(\text{vk}_B, m^\text{in}, \sigma^\text{in}) = 1 \text{ set } \alpha = \text{‘B’ } ; \\
8 & \text{If } \alpha = \tilde{\alpha} \text{ output Reject}; \\
9 & \text{if } \alpha = \text{‘B’ then} \\
10 & \quad \text{Compute } (\text{st}^\text{out}, \text{a}^\text{out}_\text{A-\text{B}}) \leftarrow F^1(\text{st}^\text{in}, \text{a}^\text{in}_\text{A-\text{B}}) \\
11 & \text{else} \\
12 & \quad \text{Compute } (\text{st}^\text{out}, \text{a}^\text{out}_\text{A-\text{B}}) \leftarrow F^0(\text{st}^\text{in}, \text{a}^\text{in}_\text{A-\text{B}}) \\
13 & \text{if } \text{st}^\text{out} = \text{Reject, output } \text{Reject} ; \\
14 & \quad \text{w}^\text{out} = \text{Acc.Update}((\text{pp}_\text{Acc}, \tilde{w}^\text{in}, \tilde{B}^\text{out}, \pi^\text{in}) ; \\
15 & \quad \text{if } \text{w}^\text{out} = \text{Reject output } \text{Reject} ; \\
16 & \quad \text{compute } \text{b}^\text{out} = \text{itr.iterate}((\text{pp}_\text{itr}, \tilde{v}^\text{in}, \text{st}^\text{in}, \tilde{w}^\text{in}, \tilde{I}^\text{in}) ; \\
17 & \quad \text{if } \text{b}^\text{out} = \text{Reject output } \text{Reject} ; \\
18 & \quad \text{compute } r_A' = \text{PRF}(K_A, t), r_B' = \text{PRF}(K_B, t) ; \\
19 & \quad \text{compute } (\text{sk}_A', \text{vk}_A', \text{vk}_A') = \text{Spl.Setup}(1^\lambda; r_A'), (\text{sk}_B', \text{vk}_B', \text{vk}_B') = \text{Spl.Setup}(1^\lambda; r_B') ; \\
20 & \quad \text{set } m^\text{out} = (\text{b}^\text{out}, \text{st}^\text{out}, \text{w}^\text{out}, \tilde{I}^\text{out}) ; \\
21 & \quad \text{compute } \sigma^\text{out} = \text{Spl.Sign}(\text{sk}_A', m^\text{out}) ; \\
22 & \text{output } \tilde{\text{st}}^\text{out} = (t + 1, \text{st}^\text{out}, \text{b}^\text{out}, \text{w}^\text{out}, \sigma^\text{out}) \quad \text{where } \tilde{a}^\text{out}_\text{A-\text{B}} = \text{a}^\text{out}_\text{A-\text{B}} ;
\end{align*}
\]
Lemma B.2. Let $iO$ be a secure indistinguishability obfuscator, PRF be a selectively secure puncturable PRF and Spl be a secure splittable signature scheme. Then for any PPT adversary $\mathcal{A}$, $|\text{Adv}_\mathcal{A}^{0,0,i} - \text{Adv}_\mathcal{A}^{0,0,i-1}| \leq \text{negl}(\lambda)$.

Proof. We define fourth-layer hybrids $\text{Hyb}_{0,0,i,a}$, \ldots, $\text{Hyb}_{0,0,i,f}$.

$\text{Hyb}_{0,0,i,a}$. In this hybrid, the challenger outputs an obfuscation of $\hat{F}^{0,0,i,a}$ defined in Algorithm 31. This program is similar to $\hat{F}^{0,0,i}$ except that when $t = i$, it verifies the signature using $\text{vk}_{B,\text{rej}}$ if it is not accepted as ‘A’ type signature.

$\text{Hyb}_{0,0,i,b}$. In this hybrid, the challenger first punctures the PRF key $K_B$ on input $i - 1$ by computing $K_B\{i - 1\} \leftarrow \text{PRF.Puncture}(K_B, i - 1)$. Next, it computes $r_C = \text{PRF}(K_B, i - 1)$ and $(\text{sk}_C, \text{vk}_C, \text{vk}_{C,\text{rej}}) = \text{Spl.Setup}(1^\lambda; r_C)$. It outputs an obfuscation of $\hat{F}^{0,0,i,a}$ except that it has $K_B\{i - 1\}$ and $\text{vk}_{C,\text{rej}}$ hardwired, and when $t = i$, it replaces $\text{vk}_{B,\text{rej}}$ by $\text{vk}_{C,\text{rej}}$.

$\text{Hyb}_{0,0,i,c}$. This hybrid is similar to $\text{Hyb}_{0,0,i,b}$, except that $r_C$ is now chosen uniformly at random from $\{0,1\}^\lambda$.

$\text{Hyb}_{0,0,i,d}$. This hybrid is similar to $\text{Hyb}_{0,0,i,c}$, except that $\text{vk}_C$ instead of $\text{vk}_{C,\text{rej}}$ is hardwired to the program.

$\text{Hyb}_{0,0,i,e}$. This hybrid is similar to $\text{Hyb}_{0,0,i,d}$, except that $r_C = \text{PRF}(K_B, i - 1)$ is now pseudorandom.

$\text{Hyb}_{0,0,i,f}$. This hybrid is identical to $\text{Hyb}_{0,0,i-1}$.

Analysis. In the remaining we prove the following claims:

Claim B.3. Let $iO$ be a secure indistinguishability obfuscator. Then for any PPT adversary $\mathcal{A}$, $|\text{Adv}_\mathcal{A}^{0,0,i} - \text{Adv}_\mathcal{A}^{0,0,i,a}| \leq \text{negl}(\lambda)$.

Proof. Observe that $\hat{F}^{0,0,i}$ and $\hat{F}^{0,0,i,a}$ have identical functionality. Therefore $\text{Hyb}_{0,0,i}$ and $\text{Hyb}_{0,0,i,a}$ are computationally indistinguishable under the assumption that $iO$ is a secure indistinguishability obfuscation scheme.

Claim B.4. Let $iO$ be a secure indistinguishability obfuscator. Then for any PPT adversary $\mathcal{A}$, $|\text{Adv}_\mathcal{A}^{0,0,i,a} - \text{Adv}_\mathcal{A}^{0,0,i,b}| \leq \text{negl}(\lambda)$.

Proof. Note that the only difference between $\hat{F}^{0,0,i,a}$ and $\hat{F}^{0,0,i,b}$ is that the later uses a punctured PRF key $K_B\{i - 1\}$ to compute the verification key for time $t - 1$ and the signing key for time $t$. For verification, the functionality is preserved since $\text{vk}_{C,\text{rej}}$ is hardwired to the circuit. For signing, ‘B’ type key is never used to sign at time $t = i - 1$. Therefore $\text{Hyb}_{0,0,i,a}$ and $\text{Hyb}_{0,0,i,b}$ are computationally indistinguishable.

Claim B.5. Let PRF be a selectively secure puncturable PRF. Then for any PPT adversary $\mathcal{A}$, $|\text{Adv}_\mathcal{A}^{0,0,i,b} - \text{Adv}_\mathcal{A}^{0,0,i,c}| \leq \text{negl}(\lambda)$.

Proof. Since both $\hat{F}^{0,0,i,b}$ and $\hat{F}^{0,0,i,c}$ depend only on $K_B\{i - 1\}$, by the security of indistinguishability obfuscation, the value of PRF($K_B, i - 1$) can be replaced by a random value. Therefore $\text{Hyb}_{0,0,i,b}$ and $\text{Hyb}_{0,0,i,c}$ are computationally indistinguishable under the assumption that PRF is selectively secure puncturable PRF.
Claim B.6. Let Spl be a splittable signature scheme which satisfies \( \text{vk}_{\text{rej}} \) indistinguishability (Definition A.7). Then for any PPT adversary \( \mathcal{A} \), \( |\text{Adv}^{0,0,i,c}_{\mathcal{A}} - \text{Adv}^{0,0,i,d}_{\mathcal{A}}| \leq \text{negl}(\lambda) \).

Proof. Note that \( \text{sk}_C \) is not hardwired in either \( \hat{F}^{0,0,i,c} \) or \( \hat{F}^{0,0,i,d} \). Based on the \( \text{vk}_{\text{rej}} \) indistinguishability property of splittable signature scheme Spl, given only \( \text{vk}_C \) or \( \text{vk}_{C,\text{rej}} \), the two hybrids are computationally indistinguishable. \( \square \)

Claim B.7. Let PRF be a selectively secure puncturable PRF. Then for any PPT adversary \( \mathcal{A} \), \( |\text{Adv}^{0,0,i,d}_{\mathcal{A}} - \text{Adv}^{0,0,i,e}_{\mathcal{A}}| \leq \text{negl}(\lambda) \).

Proof. Since both \( \hat{F}^{0,0,i,d} \) and \( \hat{F}^{0,0,i,e} \) depend only on \( K_B \{i - 1\} \), by the security of indistinguishability obfuscation, the random value can be switched back to \( \text{PRF}(K_B, i - 1) \). Therefore \( \text{Hyb}_{0,0,i,d} \) and \( \text{Hyb}_{0,0,i,e} \) are computationally indistinguishable. \( \square \)

Claim B.8. Let \( iO \) be a secure indistinguishability obfuscator. Then for any PPT adversary \( \mathcal{A} \), \( |\text{Adv}^{0,0,i,e}_{\mathcal{A}} - \text{Adv}^{0,0,i,f}_{\mathcal{A}}| \leq \text{negl}(\lambda) \).

Proof. Finally, observe that \( \hat{F}^{0,0,i,e} \) and \( \hat{F}^{0,0,i,f} \) have identical functionality. To conclude, we have for all PPT \( \mathcal{A} \), \( |\text{Adv}^{0,0,i}_{\mathcal{A}} - \text{Adv}^{0,0,i-1}_{\mathcal{A}}| \leq \text{negl}(\lambda) \) as required. \( \square \)

B.1.2 From Hyb\(_{0,2,i}\) to Hyb\(_{0,2',i}\)

Lemma B.9. Let \( 1 \leq i < t^* \). Assume \( iO \) is a secure indistinguishability obfuscator, PRF is a selectively secure puncturable PRF, Spl is a secure splittable signature scheme, and Acc is a secure positional accumulator scheme. Then for any PPT adversary \( \mathcal{A} \), \( |\text{Adv}^{0,2,i}_{\mathcal{A}} - \text{Adv}^{0,2',i}_{\mathcal{A}}| \leq \text{negl}(\lambda) \).

Proof. We define fourth layer hybrids \( \text{Hyb}_{0,2,i,0}, \text{Hyb}_{0,2,i,1}, \ldots, \text{Hyb}_{0,2,i,13} \). The first hybrid corresponds to \( \text{Hyb}_{0,2,i,0} \), and the last one corresponds to \( \text{Hyb}_{0,2',i} \).

\textbf{Hyb}_{0,2,i,0}. This hybrid corresponds to \( \text{Hyb}_{0,2,i} \).

\textbf{Hyb}_{0,2,i,1}. In this experiment, the challenger punctures key \( K_A, K_B \) at input \( i \), uses \( \text{PRF}(K_A, i) \) and \( \text{PRF}(K_B, i) \) to compute \( (\text{sk}_C, \text{vk}_C) \) and \( (\text{sk}_D, \text{vk}_D) \) respectively. More formally, it computes \( K_A \{i\} \leftarrow \text{PRF}.\text{Puncture}(K_A, i), \ r_C = \text{PRF}(K, i), \ (\text{sk}_C, \text{vk}_C, \text{vk}_{C,\text{rej}}) = \text{Spl.Setup}(1^{\lambda}; r_C) \) and \( K_B \{i\} \leftarrow \text{PRF}.\text{Puncture}(K_B, i), \ r_D = \text{PRF}(K, i), \ (\text{sk}_D, \text{vk}_D, \text{vk}_{D,\text{rej}}) = \text{Spl.Setup}(1^{\lambda}; r_D) \).

In this hybrid, the challenger outputs an obfuscation of \( \hat{F}^{0,2,i,1} \) defined in Algorithm 34. Here \( \hat{F}^{0,2,i,1} \) is identical to \( \hat{F}^{0,2,i} \) defined in Algorithm 26 except that it uses a punctured PRF key \( K_A \{i\} \) instead of \( K_A \), and \( K_B \{i\} \) instead of \( K_B \).

\textbf{Hyb}_{0,2,i,2}. In this hybrid, the challenger chooses \( r_C, r_D \) uniformly at random instead of computing them using \( \text{PRF}(K_A, i) \) and \( \text{PRF}(K_B, i) \). In other words, the secret key/verification key pairs are sampled as \( (\text{sk}_C, \text{vk}_C) \leftarrow \text{Spl.Setup}(1^{\lambda}) \) and \( (\text{sk}_D, \text{vk}_D) \leftarrow \text{Spl.Setup}(1^{\lambda}) \).
Algorithm 31: \( \tilde{F}^{0,0,1,1} \)

Input : \( \tilde{s}^{\text{in}} = (t, s^{\text{in}}, w^{\text{in}}, \sigma^{\text{in}}), \tilde{a}^{\text{in}}_{k-M} = (a^{\text{in}}_{k-M}, \pi^{\text{in}}) \) where \( a^{\text{in}}_{k-M} = (I^{\text{in}}, B^{\text{in}}) \)

Data: \( T, pp_{\text{Acc}}, pp_{\text{Itr}}, K_A, K_B \)

1. If \( \text{Acc.VerifyRead}(pp_{\text{Acc}}, w^{\text{in}}, I^{\text{in}}, B^{\text{in}}, \pi^{\text{in}}) = 0 \) output \( \text{Reject} \);
2. Compute \( r_A = \text{PRF}(K_A, t - 1), r_B = \text{PRF}(K_B, t - 1) \);
3. Compute \( (sk_A, vk_A, vk_{A,\text{rej}}) = \text{Split}(1^{\lambda}; r_A), (sk_B, vk_B, vk_{B,\text{rej}}) = \text{Split}(1^{\lambda}; r_B) \);
4. Set \( v_k = vk_{B,\text{rej}} \);
5. Set \( m^{\text{in}} = (v^{\text{in}}, s^{\text{in}}, w^{\text{in}}, I^{\text{in}}) \) and \( \alpha = \mu^* \);
6. If \( \text{Spl.Verify}(vk_A, m^{\text{in}}, \sigma^{\text{in}}) = 1 \) set \( \alpha = A' \);
7. If \( \alpha = \mu^* \) and \( (t > t^* \text{ or } t < i - 1) \) output \( \text{Reject} \);
8. If \( \alpha = \mu^* \) and \( t = i \) and \( \text{Spl.Verify}(vk, m^{\text{in}}, \sigma^{\text{in}}) = 0 \) output \( \text{Reject} \);
9. If \( \alpha = \mu^* \) and \( \text{Spl.Verify}(vk_B, m^{\text{in}}, \sigma^{\text{in}}) = 1 \) set \( \alpha = B' \);
10. If \( \alpha = \mu^* \) output \( \text{Reject} \);

11. If \( \alpha = B' \) then
12. \( \) Compute \( (s^{\text{out}}, a^{\text{out}}_{M-k}) \leftarrow F^1(s^{\text{in}}, a^{\text{in}}_{k-M}) \)
13. else
14. \( \) Compute \( (s^{\text{out}}, a^{\text{out}}_{M-k}) \leftarrow F^0(s^{\text{in}}, a^{\text{in}}_{k-M}) \)
15. If \( s^{\text{out}} = \text{Reject}, \text{output} \text{Reject} \);
16. \( w^{\text{out}} = \text{Acc.Update}(pp_{\text{Acc}}, w^{\text{in}}, B^{\text{out}}, \pi^{\text{in}}) \);
17. If \( w^{\text{out}} = \text{Reject} \) output \( \text{Reject} \);
18. Compute \( v^{\text{out}} = \text{Itr.Iterate}(pp_{\text{Itr}}, v^{\text{in}}, (s^{\text{in}}, w^{\text{in}}, I^{\text{in}})) \);
19. If \( v^{\text{out}} = \text{Reject} \) output \( \text{Reject} \);
20. Compute \( r'_A = \text{PRF}(K_A, t), r'_B = \text{PRF}(K_B, t) \);
21. Compute \( (sk'_A, vk'_A, vk'_{A,\text{rej}}) = \text{Spl.Setup}(1^{\lambda}; r'_A), (sk'_B, vk'_B, vk'_{B,\text{rej}}) = \text{Spl.Setup}(1^{\lambda}; r'_B) \);
22. Set \( m^{\text{out}} = (v^{\text{out}}, s^{\text{out}}, w^{\text{out}}, I^{\text{out}}) \);
23. Compute \( \sigma^{\text{out}} = \text{Spl.Sign}(sk'_A, m^{\text{out}}) \);
24. Output \( \tilde{s}^{\text{out}} = (t + 1, s^{\text{out}}, w^{\text{out}}, \sigma^{\text{out}}), \tilde{a}^{\text{out}}_{M-k} = a^{\text{out}}_{M-k} \).
Algorithm 32: $\tilde{F}^{0,0,i,b}$

Input : $\sigma_{in} = (t, st_{in}, v_{in}, w_{in}, \sigma_{in})$, $\tilde{\sigma}_{in} = (a_{in}^M, \pi_{in})$ where $a_{in}^M = (I_{in}, B_{in})$

Data: $T$, $pp_{Acc}$, $pp_{Itr}$, $K_A$, $K_B\{i-1\}$, $vk_{C,\text{ rej}}$

1. If $\text{Acc}$.VerifyRead($pp_{Acc}, w_{in}, I_{in}, B_{in}, \pi_{in}$) = 0 output Reject;
2. Compute $r_A = \text{PRF}(K_A, t - 1)$;
3. Compute $(sk_A, vk_A, vk_{A, \text{ rej}}) = \text{Spl.Setup}(1^\lambda; r_A)$;
4. If $t \neq i$ then
   5. Compute $r_B = \text{PRF}(K_B\{i-1\}, t - 1)$;
   6. Compute $(sk_B, vk_B, vk_{B, \text{ rej}}) = \text{Spl.Setup}(1^\lambda; r_B)$;
   7. Set $vk = vk_{B, \text{ rej}}$;
8. else
   9. Set $vk = vk_{C, \text{ rej}}$;
10. Set $m_{in} = (v_{in}, st_{in}, w_{in}, I_{in})$ and $\alpha = \alpha'$;
11. If $\text{Spl}.\text{Verify}(vk_A, m_{in}, \sigma_{in}) = 1$ set $\alpha = \alpha'$;
12. If $\alpha = \alpha'$ and $(t > t^* \text{ or } t \leq i - 1)$ output Reject;
13. If $\alpha = \alpha'$ and $t = i$ and $\text{Spl}.\text{Verify}(vk, m_{in}, \sigma_{in}) = 0$ output Reject;
14. If $\alpha = \alpha'$ and $\text{Spl}.\text{Verify}(vk_B, m_{in}, \sigma_{in}) = 1$ set $\alpha = \alpha'B$;
15. If $\alpha = \alpha'$ output Reject;
16. if $\alpha = \alpha'B$ then
17. Compute $(st_{out}^{\alpha'}, a_{M_{i-1}}^{\alpha'}) \leftarrow F^1(st_{in}, a_{i-1}^{\alpha})$
18. else
19. Compute $(st_{out}^{\alpha'}, a_{M_{i-1}}^{\alpha'}) \leftarrow F^0(st_{in}, a_{i-1}^{\alpha})$
20. If $st_{out} = \text{Reject}$, output Reject;
21. $w_{out} = \text{Acc}.\text{Update}(pp_{Acc}, w_{in}, B_{out}, \pi_{in})$;
22. If $w_{out} = \text{Reject}$ output Reject;
23. Compute $v_{out} = \text{Itr}.\text{Iterate}(pp_{Itr}, v_{in}, (st_{in}, w_{in}, I_{in}))$;
24. If $v_{out} = \text{Reject}$ output Reject;
25. Compute $r_A' = \text{PRF}(K_A, t), r_B' = \text{PRF}(K_B\{i-1\}, t)$;
26. Compute $(sk_A', vk_A', vk_{A, \text{ rej}}') = \text{Spl.Setup}(1^\lambda; r_A'), (sk_B', vk_B', vk_{B, \text{ rej}}') = \text{Spl.Setup}(1^\lambda; r_B')$;
27. Set $m_{out} = (v_{out}, st_{out}, w_{out}, I_{out})$;
28. Compute $\sigma_{out} = \text{Spl}.\text{Sign}(sk_{\alpha', M}, m_{out})$;
29. Output $st_{out} = (t + 1, st_{out}, v_{out}, w_{out}, \sigma_{out})$, $\tilde{\sigma}_{out}^{\alpha'} = a_{M_{i-1}}^{\alpha'}$. 

95
**Hyb_{0,2,i,3}** In this hybrid, the challenger computes constrained signing keys using the Spl.Split algorithm. As in the previous hybrids, the challenger first computes the i-th message $m^i$. Then, it computes the following: $(σ_{C,one}, vk_{C,one}, sk_{C,abo}, vk_{C,abo}) = \text{Spl.Split}(sk_C, m^i)$ and $(σ_{D,one}, vk_{D,one}, sk_{D,abo}, vk_{D,abo}) = \text{Spl.Split}(sk_D, m^i)$.

In this hybrid, the challenger outputs an obfuscation of $\hat{F}^{0,2,i,2}$ defined in Algorithm 35. Note that the only difference between $\hat{F}^{0,2,i,2}$ and $\hat{F}^{0,2,i,1}$ is that in $\hat{F}^{0,2,i,1}$, on input corresponding to step $i$, signs the outgoing message $m$ using $sk_C$ if $m = m^i$, else it signs using $sk_D$. On the other hand, at step $i$, $\hat{F}^{0,2,i,2}$ outputs $σ_{C,one}$ if the outgoing message $m = m^i$, else it signs using $sk_{C,abo}$.

**Hyb_{0,2,i,4}** This hybrid is similar to the previous one, except that the challenger hardwires $vk_{C,one}$ in $\hat{F}^{0,2,i,2}$ instead of $vk_C$.

**Hyb_{0,2,i,5}** This hybrid is similar to the previous one, except that the challenger hardwires $vk_{D,abo}$ instead of $vk_D$. As in the previous hybrid, the challenger uses Spl.Split to compute $(σ_{C,one}, vk_{C,one}, sk_{C,abo}, vk_{C,abo})$ and $(σ_{D,one}, vk_{D,one}, sk_{D,abo}, vk_{D,abo})$ from $sk_C$ and $sk_D$ respectively.

**Hyb_{0,2,i,6}** In this hybrid, the challenger outputs an obfuscation of $\hat{F}^{0,2,i,3}$ defined in Algorithm 36. This program performs extra checks before computing the signature. In particular, the program additionally checks if the input corresponds to step $i + 1$. If so, it checks whether $m^i_{in} = m^i$ or not, and accordingly outputs either ‘A’ or ‘B’ type signature.

**Hyb_{0,2,i,7}** In this hybrid, the challenger makes the accumulator ‘read enforcing’. It computes the first $i$ number of ‘correct inputs’ for the accumulator. Based on the initial configuration, we first obtain $\left\{ (j, \text{mem}^0[j]) \right\}^{|\text{mem}^0|}_{j=1}$. Then we run the following algorithm to obtain $\{ a^i_{\text{mem}^0} \}_{j=0}$.

**Algorithm 33:** This algorithm is for $\textbf{Hyb}_{0,2,i,7}$

1. for $j \in \{1, \ldots, i\}$ do
2.  Compute $(st^j, a^j_{\text{mem}^0}) \leftarrow F^0(st^{j-1}, a^{j-1}_{\text{mem}^0})$ ; \hspace{1cm} // $a^{j-1}_{\text{mem}^0} = (I^{j-1}, B^{j-1})$
3.  $(\text{mem}^j, a^j_{\text{mem}^0}) \leftarrow \text{access}(\text{mem}^{j-1}, a^{j-1}_{\text{mem}^0})$ ; \hspace{1cm} // $a^j_{\text{mem}^0} = (I^j, B^j)$

Let $\ell = |\text{mem}^0|$. Now we set

$$\text{enf} = \left( (1, \text{mem}^0[1]), \ldots, (\ell, \text{mem}^0[\ell]), (I^0, B^0), \ldots, (I^{i-1}, B^{i-1}) \right)$$

Finally, the challenger computes $(pp_{\text{Acc}}, w_0, st_{\text{read}}) \leftarrow \text{Acc.SetupEnforceRead}(1^\lambda; T, \text{enf}, I^\lambda)$.

**Hyb_{0,2,i,8}** In this hybrid, the challenger outputs an obfuscation of $\hat{F}^{0,2,i,4}$ defined in Algorithm 37. This program runs $F^1$ instead of $F^0$, if on $(i + 1)$-st step, the input signature ‘A’ verifies. Note that the accumulator is ‘read enforced’ in this hybrid.

**Hyb_{0,2,i,9}** In this hybrid, the challenger uses normal setup for the accumulator related parameters; that is, it computes $(pp_{\text{Acc}}, w_0, st_{\text{read}}) \leftarrow \text{Acc.Setup}(1^\lambda; T)$. The remaining steps are exactly identical to the corresponding ones in the previous hybrid.
\textbf{Hyb}_{0,2,i,10}. In this hybrid, the challenger computes \((\sigma_{C,\text{one}}, \vk_{C,\text{one}}, \sk_{C,\text{abo}}, \vk_{C,\text{abo}}) = \text{Spl.Split}(\sk_C, m^i)\), but does not compute \((\sk_D, \vk_D)\). Instead, it outputs an obfuscation of Note that the hardwired keys for verification/signing (that is, \(\sigma_{C,\text{one}}, \vk_{C,\text{one}}, \sk_{C,\text{abo}}, \vk_{C,\text{abo}}\)) are all derived from the same signing key \(\sk_C\), whereas in the previous hybrid, the first two components were derived from \(\sk_C\) while the next two from \(\sk_D\).

\textbf{Hyb}_{0,2,i,11}. In this hybrid, the challenger outputs an obfuscation of \(\hat{F}^{0,2,i,5}\) defined in Algorithm 35.

\textbf{Hyb}_{0,2,i,12}. In this hybrid, the challenger chooses the randomness \(r_C\) used to compute \((\sk_C, \vk_C)\) pseudo-randomly; that is, it sets \(r_C = \text{PRF}(K_A, i)\).

\textbf{Hyb}_{0,2,i,13}. This corresponds to \(\text{Hyb}_{0,2',i}\).

\textbf{Analysis.} In the remaining we prove the following claims.

\textbf{Claim B.10.} Let \(iO\) be a secure indistinguishability obfuscator. Then for any PPT adversary \(A\), \(|\text{Adv}_{A}^{0,2,i} - \text{Adv}_{A}^{0,2,i,1}| \leq \text{negl}(\lambda)|\).

\textit{Proof.} The only difference between \(\text{Hyb}_{0,2,i}\) and \(\text{Hyb}_{0,2,i,1}\) is that \(\text{Hyb}_{0,2,i}\) uses program \(\hat{F}^{0,2,i}\), while \(\text{Hyb}_{0,2,i,1}\) uses \(\hat{F}^{0,2,i,1}\). From the correctness of puncturable PRFs, it follows that both programs have identical functionality for \(t \neq i\). For \(t = i\), the two programs have identical functionality because \((\sk_C, \vk_C)\) and \((\sk_D, \vk_D)\) are correctly computed using \(\text{PRF}(K_A, i)\) and \(\text{PRF}(K_B, i)\) respectively. Therefore, by the security of \(iO\), it follows that the obfuscations of the two programs are computationally indistinguishable.

\textbf{Claim B.11.} Let \(\text{PRF}\) be a selectively secure puncturable PRF. Then for any PPT adversary \(A\), \(|\text{Adv}_{A}^{0,2,i,1} - \text{Adv}_{A}^{0,2,i,2}| \leq \text{negl}(\lambda)|\).

\textit{Proof.} We will construct an intermediate experiment \(\text{Hyb}\), where \(r_C\) is chosen uniformly at random, while \(r_D = \text{PRF}(K_B, i)\). Now, if an adversary can distinguish between \(\text{Hyb}_{0,2,i,1}\) and \(\text{Hyb}\), then we can construct a reduction algorithm that breaks the security of \(\text{PRF}\). The reduction algorithm sends \(i\) as the challenge, and receives \(K_A\{i\}, r\). It then uses \(r\) to compute \((\sk_C, \vk_C) = \text{Spl.Setup}(1^\lambda, r)\). Depending on whether \(r\) is truly random or not, \(B\) simulates either hybrid \(\text{Hyb}\) or \(\text{Hyb}_{0,2,i,1}\). Clearly, if \(A\) can distinguish between \(\text{Hyb}_{0,2,i,1}\) and \(\text{Hyb}\) with advantage non-negl, then \(B\) breaks the \(\text{PRF}\) security with advantage non-negl.

\textbf{Claim B.12.} Let \(iO\) be a secure indistinguishability obfuscator. Then for any PPT adversary \(A\), \(|\text{Adv}_{A}^{0,2,i,2} - \text{Adv}_{A}^{0,2,i,3}| \leq \text{negl}(\lambda)|\).

\textit{Proof.} The correctness property of \(\text{Spl}\) ensures that \(\hat{F}^{0,2,i,1}\) and \(\hat{F}^{0,2,i,2}\) have identical functionality.

\textbf{Claim B.13.} Let \(\text{Spl}\) be a secure splittable signature scheme which satisfies \(\vk_{\text{one}}\) indistinguishability (Definition A.8). Then for any PPT adversary \(A\), \(|\text{Adv}_{A}^{0,2,i,3} - \text{Adv}_{A}^{0,2,i,4}| \leq \text{negl}(\lambda)|\).

\textit{Proof.} Suppose there exists an adversary \(A\) such that \(|\text{Adv}_{A}^{0,2,i,3} - \text{Adv}_{A}^{0,2,i,4}| \neq \text{non-negl}\). Then we can construct a reduction algorithm \(B\) that breaks the \(\vk_{\text{one}}\) indistinguishability of splittable signature scheme \(\text{Spl}\). \(B\) sends \(m^t\) to the challenger. The challenger chooses \((\sk_C, \vk_C, \vk_{C,\text{rej}}) \leftarrow \text{Spl.Setup}(1^\lambda)\), \((\sigma_{C,\text{one}}, \vk_{C,\text{one}}, \sk_{D,\text{abo}}, \vk_{D,\text{abo}})\) and receives \((\sigma, \vk)\), where \(\sigma = \sigma_{C,\text{one}}\) and \(\vk = \vk_C\) or \(\vk_{C,\text{one}}\). It chooses the remaining components (including \(\sk_{D,\text{abo}}\) and \(\vk_D\)) and computes \(\hat{F}^{0,2,i,2}\) where \((T, \pp_{\text{Acc}}, \pp_{\text{itr}}, K_A\{i\}, K_B\{i\}, \sigma_{C,\text{one}}, \sk_{D,\text{abo}}, \vk, \vk_{D, m^t})\) is hardwired.

Now, note that \(B\) perfectly simulates either \(\text{Hyb}_{0,2,i,3}\) or \(\text{Hyb}_{0,2,i,4}\), depending on whether the challenge message was \((\sigma_{C,\text{one}}, \vk_C)\) or \((\sigma_{C,\text{one}}, \vk_{C,\text{one}})\).
Claim B.14. Let $\text{Spl}$ be a secure splittable signature scheme which satisfies $\text{vk}_{\text{abo}}$ indistinguishability (Definition A.9). Then for any PPT adversary $A$, $|\text{Adv}_{A}^{0,2,i,4} - \text{Adv}_{A}^{0,2,i,5}| \leq \text{negl}(\lambda)$.

Proof. This proof is similar to the previous one. Suppose there exists an adversary $A$ such that $|\text{Adv}_{A}^{0,2,i,4} - \text{Adv}_{A}^{0,2,i,5}|$ is non-negligible. Then there exists a reduction algorithm $B$ that breaks the $\text{vk}_{\text{abo}}$ security of $\text{Spl}$ with advantage non-negligible. In this case, the reduction algorithm uses the challenger’s output to set up $\text{sk}_{D,\text{abo}}$ and $\text{vk}$, which is either $\text{vk}_{D}$ or $\text{vk}_{D,\text{abo}}$.

□

Claim B.15. Let $\text{iO}$ be a secure indistinguishability obfuscator. Then for any PPT adversary $A$, $|\text{Adv}_{A}^{0,2,i,6} - \text{Adv}_{A}^{0,2,i,7}| \leq \text{negl}(\lambda)$.

Proof. Let $P_0$ be $\hat{F}^{0,2,i,2}$ and $P_1$ be $\hat{F}^{0,2,i,3}$ respectively with identically computed constants $T, \text{pp}_{\text{Acc}}, \text{pp}_{\text{tr}}, K_A\{i\}, K_B\{i\}, \sigma_{\text{C,one}}, \text{sk}_{D,\text{abo}}, \text{vk}_{\text{C,one}}, \text{vk}_{D,\text{abo}}, m^i$.

It suffices to show that $P_0$ and $P_1$ have identical functionality. Note that the only inputs where $P_0$ and $P_1$ can possibly differ correspond to step $i + 1$. Fix any input in step $i + 1$. Let us consider two cases:

\(- m^{\text{in}} = m^i\). In this case, using the correctness properties of $\text{Spl}$ we can argue that for both programs, $\alpha = 'A'$. Now, $P_0$ outputs $\text{Spl.Sign}(\text{sk}_{\text{A},i}^{',m^{\text{out}}})$, while $P_1$ is hardwired to output $\text{Spl.Sign}(\text{sk}_{\text{A},i}^{',m^{\text{out}}})$.

Therefore, both programs have the same output in this case.

\(- m^{\text{in}} \neq m^i\). Here, we use the correctness properties of $\text{Spl}$ to argue that $\alpha \neq 'A'$, and conclude that $\alpha = 'B'$. $P_1$ is hardwired to output $\text{Spl.Sign}(\text{sk}_{\text{B},i}^{',m^{\text{out}}})$, while $P_0$ outputs $\text{Spl.Sign}(\text{sk}_{\text{A},i}^{',m^{\text{out}}})$.

□

Claim B.16. Let $\text{Acc}$ be a positional accumulator which satisfies indistinguishability of Read Setup (Definition A.3). Then for any PPT adversary $A$, $|\text{Adv}_{A}^{0,2,i,6} - \text{Adv}_{A}^{0,2,i,7}| \leq \text{negl}(\lambda)$.

Proof. Suppose there exists an adversary $A$ such that $|\text{Adv}_{A}^{0,2,i,6} - \text{Adv}_{A}^{0,2,i,7}|$ is non-negligible. We will construct an algorithm $B$ that uses $A$ to break the Read Setup indistinguishability of $\text{Acc}$. Here $B$ computes the first $i$ tuples to be accumulated. It computes $(B_j', I'_j)$ for $j \leq i$ as described in $\text{Hyb}_{0,2,i,7}$, and sends $(B_j', I'_j)$ for $j < i$, and $I'$ to the challenger, and receives $(\text{pp}_{\text{Acc}}, w_0, \text{store}_0)$. $B$ uses these components to compute the encoding. Note that the remaining steps are identical in both hybrids, and therefore, $B$ can simulate them perfectly. Finally, using $A$’s guess, $B$ guesses whether the setup was normal or read-enforced.

□

Claim B.17. Let $\text{iO}$ be a secure indistinguishability obfuscator, and $F^0$ and $F^1$ be functionally equivalent. Then for any PPT adversary $A$, $|\text{Adv}_{A}^{0,2,i,7} - \text{Adv}_{A}^{0,2,i,8}| \leq \text{negl}(\lambda)$.

Proof. Let $P_0$ be $\hat{F}^{0,2,i,3}$ and $P_1$ be $\hat{F}^{0,2,i,4}$ respectively with identically computed constants $T, \text{pp}_{\text{Acc}}, \text{pp}_{\text{tr}}, K_A\{i\}, K_B\{i\}, \sigma_{\text{C,one}}, \text{sk}_{D,\text{abo}}, \text{vk}_{\text{C,one}}, \text{vk}_{D,\text{abo}}, m^i$.

We need to show that $P_0$ and $P_1$ have identical functionality. Note that in this case, $F^0$ and $F^1$ are used in $\hat{F}^{0,2,i,3}$ and in $\hat{F}^{0,2,i,4}$ to compute the output respectively. Based on the assumption that $F^0$ and $F^1$ are functionally equivalent, now the only difference could be in the case where $t = i + 1$. If $\text{Spl.Verify}(\text{vk}_{\text{C,one}}, m^{\text{in}}, \sigma^{\text{in}}) = 1$ and $\text{st}^{\text{out}} = \text{Reject}$, the two programs could have different functionality. Next we argue this case cannot happen.

From the correctness of $\text{Spl}$, we have that if $\text{Spl.Verify}(\text{vk}_{\text{C,one}}, m^{\text{in}}, \sigma^{\text{in}}) = 1$, then $m^{\text{in}} = m^i$. As a result, $w^{\text{in}} = w^i$, $I^{\text{in}} = I'$, $\text{st}^{\text{in}} = \text{st}^i$. Therefore, $(\text{B}^{\text{in}} = \bot$ or $\text{Acc.VerifyRead}(\text{pp}_{\text{Acc}}, \text{B}^{\text{in}}, w^i, I', \pi) = 1) \Rightarrow \text{B}^{\text{in}} = \text{B}'$, which implies $\text{st}^{\text{out}} = \text{st}^{i+1}$. However, $\text{st}^{i+1} \neq \text{Reject}$. Therefore, $t = i + 1$ and $\text{Spl.Verify}(\text{vk}_{\text{C,one}}, m^{\text{in}}, \sigma^{\text{in}}) = 1$ and $\text{st}^{\text{out}} = \text{Reject}$ cannot take place.

□
Claim B.18. Let $\text{Acc}$ be a positional accumulator which satisfies indistinguishability of Read Setup (Definition A.3). Then for any PPT adversary $\mathcal{A}$, $|\text{Adv}_{\mathcal{A}}^{0,2,i,8} - \text{Adv}_{\mathcal{A}}^{0,2,i,9}| \leq \text{negl}(\lambda)$.

Proof. The proof is similar to that for Claim B.16.

Claim B.19. Let $\text{Spl}$ be a secure splittable signature scheme which satisfies splitting indistinguishability (Definition A.10). Then for any PPT adversary $\mathcal{A}$, $|\text{Adv}_{\mathcal{A}}^{0,2,i,9} - \text{Adv}_{\mathcal{A}}^{0,2,i,10}| \leq \text{negl}(\lambda)$.

Proof. Suppose there exists an adversary $\mathcal{A}$ such that $|\text{Adv}_{\mathcal{A}}^{0,2,i,9} - \text{Adv}_{\mathcal{A}}^{0,2,i,10}| = \text{non-negl}$. We will construct an algorithm $B$ that uses $\mathcal{A}$ to break the splitting indistinguishability of $\text{Spl}$. $B$ first receives as input from the challenger a tuple $(\sigma_{\text{one}}, v_{k_{\text{one}}}, s_{k_{\text{abo}}}, v_{k_{\text{abo}}})$, where either all components are derived from the same secret key, or the first two are from one secret key, and the last two from another secret key. Using this tuple, $B$ can define the constants required for $\mathcal{F}^{0,2,i,4}$. It computes $K_A\{i\}, K_B\{i\}, pp_{\text{Acc}}, pp_{\text{itr}}, m_i$ as described in hybrid $\text{Hyb}_{0,2,i,9}$ and hardwires $\sigma_{\text{one}}, v_{k_{\text{one}}}, s_{k_{\text{abo}}}, v_{k_{\text{abo}}}$ in the program. In this way, $B$ can simulate either $\text{Hyb}_{0,2,i,9}$ or $\text{Hyb}_{0,2,i,10}$, and therefore, use $\mathcal{A}$’s advantage to break the splitting indistinguishability.

Claim B.20. Let $iO$ be a secure indistinguishability obfuscator. Then for any PPT adversary $\mathcal{A}$, $|\text{Adv}_{\mathcal{A}}^{0,2,i,10} - \text{Adv}_{\mathcal{A}}^{0,2,i,11}| \leq \text{negl}(\lambda)$.

Proof. This claim follows from correctness properties of $\text{Spl}$. Note that the programs $\mathcal{F}^{0,2,i,4}$ and $\mathcal{F}^{0,2,i,5}$ can possibly differ only if $t = i + 1$. We argue that in this case, the two programs are identical as follows:

First, if signatures verify and $st_{in} = \text{Reject}$, then both programs output $\text{Reject}$. Second, if $\text{Spl}$.Verify$(v_{k_{\text{C,one}}}, m_{in}, \sigma_{\text{in}}) = 1$, and $st_{out} \neq \text{Reject}$, then both programs output $\text{Spl}$.Sign$(s_{k_{\text{abo}}}^{'}, m_{out})$. Third, if $\text{Spl}$.Verify$(v_{k_{\text{C,one}}}, m_{in}, \sigma_{\text{in}}) = 0$ but $\text{Spl}$.Verify$(v_{k_{\text{abo}}}, m_{in}, \sigma_{\text{in}}) = 1$, then both programs output $\text{Spl}$.Sign$(s_{k_{\text{all}}}^{'}$). Finally, if signatures do not verify at both steps, then both programs output $\text{Reject}$.

Claim B.21. Let $\text{PRF}$ be a selectively secure puncturable PRF. Then for any PPT adversary $\mathcal{A}$, $|\text{Adv}_{\mathcal{A}}^{0,2,i,11} - \text{Adv}_{\mathcal{A}}^{0,2,i,12}| \leq \text{negl}(\lambda)$.

Proof. The proof is similar to that for Claim B.11.

Claim B.22. Let $iO$ be a secure indistinguishability obfuscator. Then for any PPT adversary $\mathcal{A}$, $|\text{Adv}_{\mathcal{A}}^{0,2,i,12} - \text{Adv}_{\mathcal{A}}^{0,2,i,13}| \leq \text{negl}(\lambda)$.

Proof. The proof is similar to that for Claim B.10.

B.1.3 From $\text{Hyb}_{0,2,i}$ to $\text{Hyb}_{0,2,i+1}$

Lemma B.23. Let $i \in \{0, \ldots, l^* - 1\}$. Let $iO$ be a secure indistinguishability obfuscator, $\text{PRF}$ be a selectively secure puncturable PRF and $\text{Spl}$ be a secure splittable signature scheme. Then for any PPT adversary $\mathcal{A}$, $|\text{Adv}_{\mathcal{A}}^{0,2,i} - \text{Adv}_{\mathcal{A}}^{0,2,i+1}| \leq \text{negl}(\lambda)$.

Proof. We define fourth layer hybrids $\text{Hyb}_{0,2,i,0}$, $\text{Hyb}_{0,2,i,1}$, \ldots, $\text{Hyb}_{0,2,i,8}$. The first hybrid corresponds to $\text{Hyb}_{0,2,i}$, and the last one corresponds to $\text{Hyb}_{0,2,i+1}$.

$\text{Hyb}_{0,2,i,0}$. This hybrid corresponds to $\text{Hyb}_{0,2,i}$.
Algorithm 34: $\tilde{F}^{0,2,\lambda}$

- **Input**: $s^{in} \leftarrow (t, s^{in}, v^{in}, w^{in}, \sigma^{in})$, $a^{in}_{\text{Acc}} = (a^{in}_{\text{Acc}}, \pi^{in})$ where $a^{in}_{\text{Acc}} = (I^{in}, B^{in})$
- **Data**: $T, p_{\text{Acc}}, p_{\text{Ptr}}, K_A\{i\}, K_B\{i\}, s_C, s_D, v_k, v_k'$, $m^i$

1. If $\text{Acc.VerifyRead}(pp_{\text{Acc}}, w^{in}, I^{in}, B^{in}, \pi^{in}) = 0$ output $\text{Reject}$;
2. if $t \neq i + 1$ then
3. 
4. Compute $a^{in}_{\text{Acc}} = \text{Spl.Setup}(\lambda; r^{A})$, $(v_k, v_k', v_k^{\prime\prime}) = \text{Spl.Setup}(\lambda; r^{B})$;
5. else
6. Set $v_k = v_k'$, $v_k = v_k'$;
7. Set $m^{in} = (v^{in}, s^{in}, w^{in}, I^{in})$ and $\alpha = \text{‘-’}$;
8. If $\text{Spl.Verify}(v_k, m^{in}, \sigma^{in}) = 1$ set $\alpha = \text{‘A’}$;
9. If $\alpha = \text{‘-’}$ and $(t > t^* \ or \ t \leq i)$ output $\text{Reject}$;
10. If $\alpha \neq \text{‘A’}$ and $\text{Spl.Verify}(v_k, m^{in}, \sigma^{in}) = 1$ set $\alpha = \text{‘B’}$;
11. If $\alpha = \text{‘-’}$ output $\text{Reject}$;
12. if $\alpha = \text{‘B’} \ or \ t \leq i$ then
13. Compute $(s^{out^{out}}, a^{in}_{\text{Acc}}) \leftarrow F^{1}(s^{in}, a^{in}_{\text{Acc}})$
14. else
15. Compute $(s^{out^{out}}, a^{in}_{\text{Acc}}) \leftarrow F^{0}(s^{in}, a^{in}_{\text{Acc}})$
16. If $s^{out^{out}} = \text{Reject}$, output $\text{Reject}$;
17. $w^{out} = \text{Acc.Update}(pp_{\text{Acc}}, w^{in}, B^{out}, \pi^{in})$;
18. If $w^{out} = \text{Reject}$ output $\text{Reject}$;
19. Compute $\nu^{out} = \text{itr.Iterate}(pp_{\text{Ptr}}, v^{in}, (s^{in}, w^{in}, I^{in}))$;
20. If $\nu^{out} = \text{Reject}$ output $\text{Reject}$;
21. if $t \neq i$ then
22. Set $r^{A'} = \text{PRF}(K_A\{i\}, t)$, $r^{B'} = \text{PRF}(K_B\{i\}, t)$;
23. Compute $(sk^{A'}, v^{\prime A'}, v^{\prime A', rej}) = \text{Spl.Setup}(\lambda; r^{A'})$, $(sk^{B'}, v^{A'}, v^{A', rej}) = \text{Spl.Setup}(\lambda; r^{B'})$;
24. else
25. Set $sk^{A'} = s_C$, $sk^{B'} = s_D$;
26. Set $m^{out} = (\nu^{out}, s^{out^{out}})$;
27. if $t = i$ and $m^{out} = m^i$ then
28. Compute $\sigma^{out} = \text{Spl.Sign}(sk^{A'}, m^{out})$;
29. else if $t = i$ and $m^{out} \neq m^i$ then
30. Compute $\sigma^{out} = \text{Spl.Sign}(sk^{B'}, m^{out})$;
31. else
32. Compute $\sigma^{out} = \text{Spl.Sign}(sk^{A'}, m^{out})$;
33. Output $s^{out^{out}} = (t + 1, s^{out^{out}}, v^{out}, w^{out}, \sigma^{out})$, $a^{out}_{\text{Acc}} = a^{out}_{\text{Acc}}$.
Algorithm 35: $F^{0,2,1,2}$

**Input:** $s_{\overline{t}}^{in} = (t, s_{\overline{t}}^{in}, v^{in}, w^{in}, \sigma^{in})$, $\overline{a}_{\lambda \leftarrow \Pi}^{in} = (a_{\lambda \leftarrow \Pi}^{in}, \pi^{in})$ where $a_{\lambda \leftarrow \Pi}^{in} = (I^{in}, B^{in})$

**Data:** $T$, $\text{pp}_{\text{Acc}}$, $\text{pp}_{\text{Init}}$, $K_{A}(i)$, $K_{B}(i)$, $\sigma_{C,one}$, $\text{sk}_{D,abo}$, $vk_{C}$, $vk_{D}$, $m^{t}$

1. If $\text{Acc.\ VerifyRead}(\text{pp}_{\text{Acc}}, w^{in}, I^{in}, B^{in}, \pi^{in}) = 0$ output Reject;
2. if $t \neq i + 1$ then
   3. Compute $r_{A} = \text{PRF}(K_{A}(i), t - 1)$, $r_{B} = \text{PRF}(K_{B}(i), t - 1)$;
   4. Compute $(\text{sk}_{A}, vk_{A}, vk_{A, \text{rej}}) = \text{Spl.\ Setup}(1^{\lambda}; r_{A})$, $(sk_{B}, vk_{B}, vk_{B, \text{rej}}) = \text{Spl.\ Setup}(1^{\lambda}; r_{B})$;
5. else
   6. Set $vk_{A} = vk_{C}$, $vk_{B} = vk_{D}$;
   7. Set $m^{in} = (v^{in}, s_{\overline{t}}^{in}, w^{in}, I^{in})$ and $\alpha = \text{‘‘-‘‘}$;
   8. If $\text{Spl.\ Verify}(vk_{A}, m^{in}, \sigma^{in}) = 1$ set $\alpha = \text{‘‘A‘‘}$;
   9. if $\alpha = \text{‘‘-‘‘}$ and ($t > t^{*}$ or $t \leq i$) output Reject;
10. if $\alpha \neq \text{‘‘A‘‘}$ and $\text{Spl.\ Verify}(vk_{B}, m^{in}, \sigma^{in}) = 1$ set $\alpha = \text{‘‘B‘‘}$;
11. if $\alpha = \text{‘‘-‘‘}$ output Reject;
12. if $\alpha = \text{‘‘B‘‘}$ or $t \leq i$ then
   13. Compute $(s_{\overline{t}}^{out}, \sigma_{\overline{t} \leftarrow \Pi}^{out}) \leftarrow F^{1}(s_{\overline{t}}^{in}, a_{\lambda \leftarrow \Pi}^{in})$
   14. else
   15. Compute $(s_{\overline{t}}^{out}, \sigma_{\overline{t} \leftarrow \Pi}^{out}) \leftarrow F^{0}(s_{\overline{t}}^{in}, a_{\lambda \leftarrow \Pi}^{in})$
16. if $s_{\overline{t}}^{out} = \text{Reject}$ output Reject;
17. $w^{out} = \text{Acc.\ Update}(\text{pp}_{\text{Acc}}, w^{in}, B^{out}, \pi^{in})$;
18. if $w^{out} = \text{Reject}$ output Reject;
19. Compute $v^{out} = \text{itr.\ Iterate}(\text{pp}_{\text{Init}}, v^{in}, (s_{\overline{t}}^{in}, w^{in}, I^{in}))$;
20. if $v^{out} = \text{Reject}$ output Reject;
21. if $t \neq i$ then
   22. Set $r'_{A} = \text{PRF}(K_{A}(i), t)$, $r'_{B} = \text{PRF}(K_{B}(i), t)$;
   23. Compute $(\text{sk}'_{A}, vk'_{A}, vk'_{A, \text{rej}}) = \text{Spl.\ Setup}(1^{\lambda}; r'_{A})$, $(sk'_{B}, vk'_{B}, vk'_{B, \text{rej}}) = \text{Spl.\ Setup}(1^{\lambda}; r'_{B})$;
24. else
   25. Set $\text{sk}'_{A} = \sigma_{C,one}$, $sk'_{B} = \text{sk}_{D,abo}$;
   26. Set $m^{out} = (v^{out}, s_{\overline{t}}^{out}, w^{out}, I^{out})$;
   27. if $t = i$ and $m^{out} = m^{t}$ then
   28. Compute $\sigma^{out} = \sigma_{C,one}$;
29. else if $t = i$ and $m^{out} \neq m^{t}$ then
   30. Compute $\sigma^{out} = \text{Spl.\ AboSign}(\text{sk}'_{D,abo}, m^{out})$;
31. else
   32. Compute $\sigma^{out} = \text{Spl.\ Sign}(\text{sk}'_{\lambda}, m^{out})$;
33. Output $\overline{s}_{\overline{t}}^{out} = (t + 1, s_{\overline{t}}^{out}, v^{out}, w^{out}, \sigma^{out})$, $\overline{a}_{\lambda \leftarrow \Pi}^{out} = a_{\lambda \leftarrow \Pi}^{out}$.
Algorithm 36: $\tilde{F}_{0,2,1,3}^{\alpha}$

Input : $\tilde{st}^{in} = (t, st^{in}, u^{in}, w^{in}, \sigma^{in})$, $\tilde{a}^{in}_{A-M} = (a^{in}_{A-M}, \pi^{in})$ where $a^{in}_{A-M} = (I^{in}, B^{in})$

Data: $T$, $pp_{Acc}$, $pp_{itr}$, $K_A\{i\}$, $K_B\{i\}$, $\sigma_{C,one}$, $sk_{D,abo}$, $vk_C$, $vk_D$, $m^i$

1. If Acc.VerifyRead($pp_{Acc}$, $u^{in}$, $I^{in}$, $B^{in}$, $\pi^{in}$) = 0 output Reject;
2. if $t \neq i + 1$ then
   3. Compute $r_A = \text{PRF}(K_A\{i\}, t - 1)$, $r_B = \text{PRF}(K_B\{i\}, t - 1)$;
   4. Compute $(sk_A, vk_A, vk_{A, rej}) = \text{Spl.Setup}(1^\lambda; r_A)$, $(sk_B, vk_B, vk_{B, rej}) = \text{Spl.Setup}(1^\lambda; r_B)$;
else
   5. Set $vk_A = vk_C$, $vk_B = vk_D$;
   6. Set $m^{in} = (v^{in}, st^{in}, w^{in}, I^{in})$ and $\alpha = \text{‘} -$ ‘;
   7. If Spl.Verify($vk_A$, $m^{in}$, $\sigma^{in}$) = 1 set $\alpha = \text{‘} A’$;
   8. If $\alpha = \text{‘} -$ and ($t > t^*$ or $t \leq i$) output Reject;
   9. If $\alpha \neq \text{‘} A’$ and Spl.Verify($vk_B$, $m^{in}$, $\sigma^{in}$) = 1 set $\alpha = \text{‘} B’$;
10. If $\alpha = \text{‘} -$ output Reject;
11. if $\alpha = \text{‘} B’$ or $t < i$ then
   12. Compute $(st^{out}, a_{\tilde{r}^{in}-A}) \leftarrow F^1(st^{in}, a^{in}_{A-M})$
   13. else
   14. Compute $(st^{out}, a_{\tilde{r}^{in}-A}) \leftarrow F^0(st^{in}, a^{in}_{A-M})$
15. if $st^{out} = \text{Reject}$, output Reject;
16. $w^{out} = \text{Acc.Update}(pp_{Acc}, u^{in}, B^{out}, \pi^{in})$
17. if $w^{out} = \text{Reject}$ output Reject;
18. Compute $\pi^{out} = \text{Itr.Iteate}(pp_{itr}, v^{in}, (st^{in}, w^{in}, I^{in}))$
19. if $\pi^{out} = \text{Reject}$ output Reject;
20. if $t \neq i$ then
21. Set $r_A' = \text{PRF}(K_A\{i\}, t), r_B' = \text{PRF}(K_B\{i\}, t)$;
22. Compute $(sk_A', vk_A', vk_{A, rej}) = \text{Spl.Setup}(1^\lambda; r_A'), (sk_B', vk_B', vk_{B, rej}) = \text{Spl.Setup}(1^\lambda; r_B')$;
else
23. Set $sk_A' = \sigma_{C,one}$, $sk_B' = sk_{D,abo}$;
24. Set $m^{out} = (\pi^{out}, st^{out}, w^{out}, I^{out})$;
25. if $t = i$ and $m^{out} \neq m^i$ then
26. Compute $\sigma^{out} = \sigma_{C,one}$;
27. else if $t = i$ and $m^{out} \neq m^i$ then
28. Compute $\sigma^{out} = \text{Spl.AboSign}(sk_{D,abo}, m^{out})$;
29. else if $t = i + 1$ and $m^{in} = m^i$ then
30. Compute $\sigma^{out} = \text{Spl.Sign}(sk_A', m^{out})$;
31. else if $t = i + 1$ and $m^{in} \neq m^i$ then
32. Compute $\sigma^{out} = \text{Spl.Sign}(sk_B', m^{out})$;
33. else
34. Compute $\sigma^{out} = \text{Spl.Sign}(sk_{\alpha}', m^{out})$;
35. Output $\tilde{st}^{out} = (t + 1, st^{out}, u^{out}, w^{out}, \sigma^{out})$, $\tilde{a}^{out}_{M-A} = a^{out}_{M-A}$;
Algorithm 37: $F_{0,2,\cdot,4}$

Input : $s^{\text{in}} = (t, s^{\text{in}}_t, v^{\text{in}}, w^{\text{in}}, \sigma^{\text{in}}_t)$, $\alpha^{\text{in}}_{\text{A}k-M} = (a^{\text{in}}_{\text{A}k-M}, \pi^{\text{in}})$ where $a^{\text{in}}_{\text{A}k-M} = (1^{\text{in}}, B^{\text{in}})$

Data: $T$, $\text{pp}_{\text{Acc}}$, $\text{pp}_{\text{itr}}$, $K_A(i)$, $K_B(i)$, $\sigma_{\text{C, one}}$, $\text{sk}_{\text{D, abo}}$, $\text{vk}_C$, $\text{vk}_D$, $m^i$

1. If Acc.VerifyRead($\text{pp}_{\text{Acc}}, w^{\text{in}}, I^{\text{in}}, B^{\text{in}}, \pi^{\text{in}}$) = 0 output `Reject`;
2. if $t \neq i + 1$ then
   3. Compute $r_A = \text{PRF}(K_A(i), t - 1)$, $r_B = \text{PRF}(K_B(i), t - 1)$;
   4. Compute ($\text{sk}_A$, $\text{vk}_A$, $\text{vk}_{A, \text{rej}}$) = $\text{Spl.Setup}(1^\lambda, r_A)$, ($\text{sk}_B$, $\text{vk}_B$, $\text{vk}_{B, \text{rej}}$) = $\text{Spl.Setup}(1^\lambda, r_B)$;
5. else
   6. Set $\text{vk}_A = \text{vk}_C$, $\text{vk}_B = \text{vk}_D$;
   7. Set $m^{\text{in}} = (v^{\text{in}}, s^{\text{in}}_t, w^{\text{in}}, I^{\text{in}})$ and $\alpha = \cdot$;
   8. If $\text{Spl.Verify}(\text{vk}_A, m^{\text{in}}, \sigma^{\text{in}}) = 1$ set $\alpha = \cdot$;
   9. If $\alpha = \cdot$ and $(t > t^* \text{ or } t \leq i)$ output `Reject`;
10. If $\alpha \neq \cdot$ and $\text{Spl.Verify}(\text{vk}_B, m^{\text{in}}, \sigma^{\text{in}}) = 1$ set $\alpha = \cdot$;
11. If $\alpha = \cdot$ output `Reject`;
12. if $\alpha = \cdot$ or $t \leq i + 1$ then
   13. Compute ($s^{\text{out}}_{\cdot}^{\text{in}}, \alpha^{\text{out}}_{\text{A}k-M}$) $\leftarrow F^1(s^{\text{in}}_t, \alpha^{\text{in}}_{\text{A}k-M})$
   14. else
   15. Compute ($s^{\text{out}}_{\cdot}^{\text{in}}, \alpha^{\text{out}}_{\text{A}k-M}$) $\leftarrow F^0(s^{\text{in}}_t, \alpha^{\text{in}}_{\text{A}k-M})$
16. if $s^{\text{out}} = \text{Reject}$, output `Reject`;
17. $w^{\text{out}} = \text{Acc.Update}(\text{pp}_{\text{Acc}}, w^{\text{in}}, B^{\text{out}}, \pi^{\text{out}})$;
18. if $w^{\text{out}} = \text{Reject}$ output `Reject`;
19. Compute $w^{\text{out}} = \text{itr.Iterate}(\text{pp}_{\text{itr}}, v^{\text{in}}, (s^{\text{in}}, w^{\text{in}}, I^{\text{in}}))$;
20. if $w^{\text{out}} = \text{Reject}$ output `Reject`;
21. if $t \neq i$ then
22. Set $r'_A = \text{PRF}(K_A(i), t)$, $r'_B = \text{PRF}(K_B(i), t)$;
23. Compute ($\text{sk}'_A$, $\text{vk}'_A$, $\text{vk}'_{A, \text{rej}}$) = $\text{Spl.Setup}(1^\lambda, r'_A)$, ($\text{sk}'_B$, $\text{vk}'_B$, $\text{vk}'_{B, \text{rej}}$) = $\text{Spl.Setup}(1^\lambda, r'_B)$;
24. else
25. Set $\text{sk}'_A = \sigma_{\text{C, one}}$, $\text{sk}'_B = \text{sk}_{\text{D, abo}}$;
26. Set $m^{\text{out}} = (w^{\text{out}}, s^{\text{out}}_{\cdot}^{\text{in}}, w^{\text{out}}, I^{\text{out}})$;
27. if $t = i$ and $m^{\text{out}} \neq m^i$ then
28. Compute $\sigma^{\text{out}} = \sigma_{\text{C, one}}$;
29. else if $t = i$ and $m^{\text{out}} \neq m^i$ then
30. Compute $\sigma^{\text{out}} = \text{Spl.AboSign}(\text{sk}'_{\text{D, abo}}, m^{\text{out}})$;
31. else if $t = i + 1$ and $m^{\text{in}} = m^i$ then
32. Compute $\sigma^{\text{out}} = \text{Spl.Sign}(\text{sk}'_A, m^{\text{out}})$;
33. else if $t = i + 1$ and $m^{\text{in}} \neq m^i$ then
34. Compute $\sigma^{\text{out}} = \text{Spl.Sign}(\text{sk}'_B, m^{\text{out}})$;
35. else
36. Compute $\sigma^{\text{out}} = \text{Spl.Sign}(\text{sk}'_{\cdot}, m^{\text{out}})$;
37. Output $s^{\text{out}} = (t + 1, s^{\text{out}}_t, v^{\text{out}}, w^{\text{out}}, \sigma^{\text{out}})$, $\sigma^{\text{out}}_{\text{A}k-M} = \sigma^{\text{out}}_{\text{A}k-M}$;

103
Algorithm 38: $F^{0,2,3,5}$

**Input:** $st^{in} = (t, st^{in}, v^{in}, w^{in}, \sigma^{in})$, $\tilde{a}_{\alpha-M}^{in} = (a_{\alpha-M}^{in}, \pi^{in})$ where $a_{\alpha-M}^{in} = (I^{in}, B^{in})$

**Data:** $T, pp_{\text{Acc}}, pp_{\text{Pitr}}, K_A\{i\}, K_B\{i\}, sk_C, vk_C, m^i$

1. If $\text{Acc}.\text{VerifyRead}(pp_{\text{Acc}}, w^{in}, I^{in}, B^{in}, \pi^{in}) = 0$ output Reject;
2. if $t \neq i + 1$ then
3. Compute $r_A = \text{PRF}(K_A\{i\}, t - 1), r_B = \text{PRF}(K_B\{i\}, t - 1)$;
4. Compute $(sk_A, vk_A, vk_{A,\text{rej}}) = \text{Spl.Setup}(1^\lambda; r_A), (sk_B, vk_B, vk_{B,\text{rej}}) = \text{Spl.Setup}(1^\lambda; r_B)$;
5. else
6. Set $vk_A = vk_C$;
7. Set $m^{in} = (v^{in}, st^{in}, w^{in}, I^{in})$ and $\alpha = \text{‘‘-‘'‘;}$
8. If Spl.Verify$(vk_A, m^{in}, \sigma^{in}) = 1$ set $\alpha = \text{‘‘A‘'}$
9. if $\alpha = \text{‘‘-‘'‘;}$ and $(t > t^* \text{ or } t \leq i + 1)$ output Reject;
10. if $\alpha \neq \text{‘‘A‘'}$ and Spl.Verify$(vk_B, m^{in}, \sigma^{in}) = 1$ set $\alpha = \text{‘‘B‘'}$
11. if $\alpha = \text{‘‘-‘'‘;}$ output Reject;
12. if $\alpha = \text{‘‘B‘'}$ or $t \leq i + 1$ then
13. Compute $(st^{out}, a_{\alpha-M}^{out}) \leftarrow F^1(st^{in}, a_{\alpha-M}^{in})$
14. else
15. Compute $(st^{out}, a_{\alpha-M}^{out}) \leftarrow F^0(st^{in}, a_{\alpha-M}^{in})$
16. If $st^{out} = \text{Reject}$, output Reject;
17. $w^{out} = \text{Acc.Update}(pp_{\text{Acc}}, w^{in}, B^{out}, \pi^{in})$;
18. If $w^{out} = \text{Reject}$ output Reject;
19. Compute $u^{out} \leftarrow \text{itr.Iterate}(pp_{\text{Pitr}}, v^{in}, (st^{in}, w^{in}, I^{in}))$;
20. If $u^{out} = \text{Reject}$ output Reject;
21. if $t \neq i$ then
22. Set $r_A' = \text{PRF}(K_A\{i\}, t), r_B' = \text{PRF}(K_B\{i\}, t)$;
23. Compute $(sk_A', vk_A', vk_{A,\text{rej}}) = \text{Spl.Setup}(1^\lambda; r_A'), (sk_B', vk_B', vk_{B,\text{rej}}) = \text{Spl.Setup}(1^\lambda; r_B')$;
24. else
25. Set $sk_A' = sk_C$;
26. Set $m^{out} = (w^{out}, st^{out}, u^{out}, I^{out})$;
27. if $t = i$ then
28. Compute $\sigma^{out} = \text{Spl.Sign}(sk_A', m^{out})$;
29. else if $t = i + 1$ and $m^{in} = m^i$ then
30. Compute $\sigma^{out} = \text{Spl.Sign}(sk_A', m^{out})$;
31. else if $t = i + 1$ and $m^{in} \neq m^i$ then
32. Compute $\sigma^{out} = \text{Spl.Sign}(sk_B', m^{out})$;
33. else
34. Compute $\sigma^{out} = \text{Spl.Sign}(sk_A', m^{out})$;
35. Output $st^{out} = (t + 1, st^{out}, v^{out}, u^{out}, \sigma^{out}), \tilde{a}_{\alpha-M}^{out} = a_{\alpha-M}^{out}$.
Hyb\(_{0,2',i,1}\). In this hybrid, the challenger makes the accumulator ‘read enforcing’.

Based on the initial configuration, we first obtain \(\{(j, \text{mem}^0[j])\}_{j=1}^{\text{mem}^0[i]}\). Let \(\ell = |\text{mem}^0|\). It computes the first \(\ell + i\) ‘correct inputs’ for the accumulator. Then we run the following algorithm to obtain \(\{a^j_{\ell-i}\}_{j=0}^i\).

**Algorithm 39:** This algorithm is for Hyb\(_{0,2',i,1}\)

1. for \(j \in \{1, \ldots, i\}\) do
2. \(\text{Compute } (st^j, a^j_{\ell-i}) \leftarrow F^0(st^{j-1}, a^j_{\ell-i}); \quad /\!/ a^{j-\ell}_i = (I^{j-1}, B^{j-1})\)
3. \((\text{mem}^j, a^j_{\ell-i}) \leftarrow \text{access(\text{mem}^{j-1}, a^j_{\ell-i});} \quad /\!/ a^{j-i}_{\ell} = (I^j, B^j)\)

Now we set

\[
\text{enf} = \left((1, \text{mem}^0[1]), \ldots, (\ell, \text{mem}^0[\ell]), (I^0, B^0), \ldots, (I^{i-1}, B^{i-1})\right)
\]

Finally, the challenger computes \((pp_{\text{Acc}}, w_0, \text{store}_0) \leftarrow \text{Acc.SetupEnforceRead}(1^{\lambda}; T, \text{enf}, I^j)\).

Hyb\(_{0,2',i,2}\). In this hybrid, the challenger uses program \(\hat{F}^{0,2',i,2}\) (defined in Algorithm 42), which is similar to \(\hat{F}^{0,2,i}\). However, in addition to checking if \(m^i = m^\text{in}\), it also checks if \((v'^{\text{out}}, s'^{\text{out}}, I'^{\text{out}}) = (v^{i+1}, s^{i+1}, I^{i+1})\).

Hyb\(_{0,2',i,3}\). In this experiment, the challenger uses normal setup instead of ‘read enforced’ setup for the accumulator.

Hyb\(_{0,2',i,4}\). In this hybrid, the challenger ‘write enforces’ the accumulator. As in Hyb\(_{0,2',i,1}\), based on the initial configuration, we first obtain \(\{(j, \text{mem}^0[j])\}_{j=1}^{\text{mem}^0[i]}\). But now it computes the first \(\ell + i + 1\) ‘correct inputs’ for the accumulator. We run the following algorithm to obtain \(\{a^j_{\ell-i}\}_{j=0}^{i+1}\).

**Algorithm 40:** This algorithm is for Hyb\(_{0,2',i,4}\)

1. for \(j \in \{1, \ldots, i\}\) do
2. \(\text{Compute } (st^j, a^j_{\ell-i}) \leftarrow F^0(st^{j-1}, a^j_{\ell-i}); \quad /\!/ a^{j-\ell}_i = (I^{j-1}, B^{j-1})\)
3. \((\text{mem}^j, a^j_{\ell-i}) \leftarrow \text{access(\text{mem}^{j-1}, a^j_{\ell-i});} \quad /\!/ a^{j-i}_{\ell} = (I^j, B^j)\)

Now we set

\[
\text{enf} = \left((1, \text{mem}^0[1]), \ldots, (\ell, \text{mem}^0[\ell]), (I^0, B^0), \ldots, (I^i, B^i)\right)
\]

Finally, the challenger computes \((pp_{\text{Acc}}, w_0, \text{store}_0) \leftarrow \text{Acc.SetupEnforceRead}(1^{\lambda}; T, \text{enf})\).

Hyb\(_{0,2',i,5}\). In this experiment, the challenger outputs an obfuscation of \(\hat{F}^{0,2',i,5}\) in Algorithm 43, which is very similar to \(\hat{F}^{0,2',i,2}\). However, on input where \(t = i + 1\), before computing signature, it also checks if \(w^\text{out} = w^{i+1}\). Therefore, it checks whether \(m^\text{in} = m^i\) and \(m^\text{out} = m^{i+1}\).

Hyb\(_{0,2',i,6}\). This experiment is similar to the previous one, except that the challenger uses normal setup for accumulator instead of ‘enforcing write’.

105
Hyb\textsubscript{0,2',i,7}. This experiment is similar to the previous one, except that the challenger uses enforced setup for iterator instead of normal setup. It first computes pp\textsubscript{Acc}, w\textsuperscript{0}, store\textsuperscript{0} as in the previous hybrid. Next, it computes the first i + 1 ‘correct messages’ for the iterator.

Based on the initial configuration mem\textsuperscript{0}, st\textsuperscript{0}, a\textsubscript{H \leftarrow A} = \perp, a\textsubscript{H \leftarrow A} = \perp), the challenger computes enf = (\langle st\textsuperscript{0}, w\textsuperscript{0}, F\rangle, (st\textsuperscript{i}, w\textsuperscript{i}, F\textsuperscript{i}), \ldots, (st\textsuperscript{i}, w\textsuperscript{i}, F\textsuperscript{i})\rangle as follows:

Algorithm 41: This algorithm is for Hyb\textsubscript{0,2',i,7}

\begin{verbatim}
for j ∈ \{1, \ldots, i + 1\} do
  Compute (st\textsuperscript{j}, a\textsubscript{H \leftarrow A}\textsuperscript{j−1}) ← F\textsuperscript{0}(st\textsuperscript{j−1}, a\textsubscript{H \leftarrow A}\textsuperscript{j−1});
  (a\textsubscript{H \leftarrow A}\textsuperscript{j}, \pi\textsuperscript{j}) ← Acc.WriteStore(pp\textsubscript{Acc}, store\textsuperscript{j−1}, a\textsubscript{H \leftarrow A}\textsuperscript{j});
  M\textsuperscript{j} ← Acc.Update(pp\textsubscript{Acc}, w\textsuperscript{j−1}, a\textsubscript{H \leftarrow A}\textsuperscript{j}, \pi\textsuperscript{j});
\end{verbatim}

Then the challenger computes (pp\textsubscript{Iter}, v\textsuperscript{0}) ← Itr.SetupEnforceIterate(1\^{\lambda}; T, enf).

Hyb\textsubscript{0,2',i,8}. In this experiment, the challenger outputs an obfuscation of \tilde{F}\textsuperscript{0,2',i,8} in Algorithm 44, which is similar to \tilde{F}\textsuperscript{0,2',i,5}, except that it only checks if m\textsuperscript{out} = m\textsuperscript{i+1}.

Hyb\textsubscript{0,2',i,9}. This corresponds to Hyb\textsubscript{0,2,i+1}. The only difference between this experiment and the previous one is that this uses normal Setup for iterator.

Analysis.

Claim B.24. Let Acc be a positional accumulator which satisfies indistinguishability of Read Setup (Definition A.3). Then for any PPT adversary \mathcal{A}, |Adv\textsubscript{\mathcal{A}}\textsuperscript{0,2',i} - Adv\textsubscript{\mathcal{A}}\textsuperscript{0,2',i,1}| ≤ negl(\lambda).

Proof. The proof is very similar that for Claim B.16.

Claim B.25. Let Acc be a positional accumulator which is Read-enforcing (Definition A.5), and iO be a secure indistinguishability obfuscator. Then for any PPT adversary \mathcal{A}, |Adv\textsubscript{\mathcal{A}}\textsuperscript{0,2',i,1} - Adv\textsubscript{\mathcal{A}}\textsuperscript{0,2',i,2}| ≤ negl(\lambda).

Proof. In order to prove the claim, it suffices to show that P\textsubscript{0} = \tilde{F}\textsuperscript{0,2',i} and P\textsubscript{1} = \tilde{F}\textsuperscript{0,2,i}, which are functionally equivalent. These two programs are functionally identical if m\textsuperscript{in} = m\textsuperscript{i} ⇒ (v\textsuperscript{out}, st\textsuperscript{i, out}) = (v\textsuperscript{i+1}, st\textsuperscript{i+1, out}), which is implied by the read-enforcing property of the accumulator.

Claim B.26. Let Acc be a positional accumulator which satisfies indistinguishability of Read Setup (Definition A.3). Then for any PPT adversary \mathcal{A}, |Adv\textsubscript{\mathcal{A}}\textsuperscript{0,2',i,2} - Adv\textsubscript{\mathcal{A}}\textsuperscript{0,2',i,3}| ≤ negl(\lambda).

Proof. The proof is very similar that for Claim B.16.

Claim B.27. Let Acc be a positional accumulator which satisfies indistinguishability of Write Setup (Definition A.4). Then for any PPT adversary \mathcal{A}, |Adv\textsubscript{\mathcal{A}}\textsuperscript{0,2',i,3} - Adv\textsubscript{\mathcal{A}}\textsuperscript{0,2',i,4}| ≤ negl(\lambda).
Proof. Suppose there exists an adversary $A$ such that $|\Adv_{\mathcal{A}}^{0,2',i,3,4} - \Adv_{\mathcal{A}}^{0,2',i,4}| = \text{non-negl}$. We will construct an algorithm $B$ that uses $A$ to break the Write Setup indistinguishability of Acc. Here $B$ computes the first $\ell_{\text{input}} + i + 1$ tuples to be accumulated, i.e., enf. It then sends enf to the challenger, and receives $(\text{pp}_{\text{Acc}}, \hat{w}_0, \text{store}_0)$. Note that the remaining steps are identical in both hybrids, and therefore, $B$ can simulate them perfectly. Finally, using $A$’s guess, $B$ guesses whether the setup was normal or write-enforced.

Claim B.28. Let Acc be a positional accumulator which is Write-enforcing (Definition A.6), and iO be a secure indistinguishability obfuscator. Then for any PPT adversary $A$, $|\Adv_{\mathcal{A}}^{0,2',i,4} - \Adv_{\mathcal{A}}^{0,2',i,5}| \leq \text{negl}(\lambda)$.

Proof. In order to prove the claim, it suffices to show that $\hat{F}^{0,2,i,b}$ and $\hat{F}^{0,2,i,c}$ are functionally equivalent. These two programs are functionally identical iff $m_{\text{in}} = m^i$ and $(v_{\text{out}}, y_{\text{out}}, z_{\text{out}}) = (v^{i+1}, y^{i+1}, z^{i+1}) \Rightarrow w_{\text{out}} = w_i$, which is implied by the read-enforcing property of the accumulator.

Claim B.29. Let Acc be a positional accumulator which satisfies indistinguishability of Write Setup (Definition A.4). Then for any PPT adversary $A$, $|\Adv_{\mathcal{A}}^{0,2',i,5} - \Adv_{\mathcal{A}}^{0,2',i,6}| \leq \text{negl}(\lambda)$.

Proof. The proof is very similar that for Claim B.27.

Claim B.30. Let $\text{itr}$ be an iterator which satisfies indistinguishability of Setup (Definition A.1). Then for any PPT adversary $A$, $|\Adv_{\mathcal{A}}^{0,2',i,6} - \Adv_{\mathcal{A}}^{0,2',i,7}| \leq \text{negl}(\lambda)$.

Proof. Suppose there exists an adversary $A$ such that $|\Adv_{\mathcal{A}}^{0,2',i,6} - \Adv_{\mathcal{A}}^{0,2',i,7}| = \text{non-negl}$. We will construct an algorithm $B$ that uses $A$ to break the Setup indistinguishability of $\text{itr}$. Here $B$ computes the first $i + 1$ tuples to be iterated on, i.e., $\text{enf} = \left( (\text{st}^0, w^0, I^0), (\text{st}^1, w^1, I^1), \ldots, (\text{st}^i, w^i, I^i) \right)$. It then sends $\text{enf}$ to the challenger, and receives $(\text{pp}_{\text{itr}}, v_0)$. Note that the remaining steps are identical in both hybrids, and therefore, $B$ can simulate them perfectly. Finally, using $A$’s guess, $B$ guesses whether the setup was normal or enforced.

Claim B.31. Let $\text{itr}$ be an iterator which is enforcing (Definition A.2), and iO be a secure indistinguishability obfuscator. Then for any PPT adversary $A$, $|\Adv_{\mathcal{A}}^{0,2',i,7} - \Adv_{\mathcal{A}}^{0,2',i,8}| \leq \text{negl}(\lambda)$.

Proof. In order to prove the claim, it suffices to show that $P_0 = P^{0,2',i,8}$ and $P_1 = \hat{F}^{0,2,i,8}$ are functionally equivalent. Note that the only difference between $P_0$ and $P_1$ is that, in $P_0$ we check if $(m_{\text{in}} = m^i)$ and $(m_{\text{out}} = m^{i+1})$, while in $P_1$ we only check if $(m_{\text{out}} = m^{i+1})$. Therefore, we need to show that $m_{\text{out}} = m^{i+1} \Rightarrow m_{\text{in}} = m^i$. This follows directly from the enforcing property of the iterator.

Claim B.32. Let $\text{itr}$ be an iterator which satisfies indistinguishability of Setup (Definition A.1). Then for any PPT adversary $A$, $|\Adv_{\mathcal{A}}^{0,2',i,8} - \Adv_{\mathcal{A}}^{0,2',i,9}| \leq \text{negl}(\lambda)$.

Proof. The proof is very similar that for Claim B.30.

B.1.4 From $\text{Hyb}_{0,2',i^*-1}$ to $\text{Hyb}_{0,3}$

Lemma B.33. Let iO be a secure indistinguishability obfuscator, and Acc be a secure positional accumulator. Then for any PPT adversary $A$, $|\Adv_{\mathcal{A}}^{0,2',i^*-1} - \Adv_{\mathcal{A}}^{0,3}| \leq \text{negl}(\lambda)$.

107
Algorithm 42: $\tilde{F}^{0,2';2}$

**Input**: $st^i = (t, st^i, v^i, w^i, \sigma^i), \tilde{a}^i_{\text{in}-M} = (\tilde{a}^i_{\text{in}-M}, \pi^i)$ where $a^i_{\text{in}-M} = (I^i, B^i)$

**Data**: $T, pp_{\text{Acc}}, pp_{\text{itr}}, K_A, K_B, m', v^{i+1}, st^{i+1}, I^{i+1}$

1. If Acc.VerifyRead($pp_{\text{Acc}}, w^i, I^i, B^i, \pi^i$) = 0 output Reject;
   2. Compute $r_A = \text{PRF}(K_A, t - 1), r_B = \text{PRF}(K_B, t - 1)$;
   3. Compute $(sk_A, vk_A, vk_{A,\text{rej}}) = \text{Spl.Setup}(1^\lambda; r_A), (sk_B, vk_B, vk_{B,\text{rej}}) = \text{Spl.Setup}(1^\lambda; r_B)$;
   4. Set $m^i = (v^i, st^i, w^i, I^i)$ and $\alpha = \cdot$;
   5. If Spl.Verify($vk_A, m^i, \sigma^i$) = 1 set $\alpha = 'A'$;
   6. If $\alpha = \cdot$ and $(t > t^* \text{ or } t \leq i + 1)$ output Reject;
   7. If $\alpha \neq 'A'$ and Spl.Verify($vk_B, m^i, \sigma^i$) = 1 set $\alpha = 'B'$;
   8. If $\alpha = \cdot$ output Reject;

9. if $\alpha = 'B'$ or $t \leq i + 1$ then
   10. Compute $(st^{out}, a^{out}_{st^-\cdot\cdot}) \leftarrow F^1(st^i, a^i_{\text{in}-M})$
   11. else
   12. Compute $(st^{out}, a^{out}_{st^-\cdot\cdot}) \leftarrow F^0(st^i, a^i_{\text{in}-M})$
   13. If $st^{out} = \text{Reject}$, output Reject;

14. $w^{out} = \text{Acc}.\text{Update}(pp_{\text{Acc}}, w^i, B^{out}, \pi^i)$;
15. If $w^{out} = \text{Reject}$ output Reject;
16. Compute $v^{out} = \text{itr}.\text{iterate}(pp_{\text{itr}}, v^i, (st^i, w^i, I^i))$;
17. If $v^{out} = \text{Reject}$ output Reject;
18. Compute $r'_A = \text{PRF}(K_A, t), r'_B = \text{PRF}(K_B, t)$;
19. Compute $(sk'_A, vk'_A, vk'_{A,\text{rej}}) = \text{Spl.Setup}(1^\lambda; r'_A), (sk'_B, vk'_B, vk'_{B,\text{rej}}) = \text{Spl.Setup}(1^\lambda; r'_B)$;
20. Set $m^{out} = (v^{out}, st^{out}, w^{out}, I^{out})$;
21. if $t = i + 1$ and $(m^i = m^i$ and $(v^{out}, st^{out}, I^{out}) = (v^{i+1}, st^{i+1}, I^{i+1}))$ then
   22. Compute $\sigma^{out} = \text{Spl}.\text{Sign}(sk'_A, m^{out})$;
23. else if $t = i + 1$ and $(m^i \neq m^i$ or $(v^{out}, st^{out}, I^{out}) \neq (v^{i+1}, st^{i+1}, I^{i+1}))$ then
   24. Compute $\sigma^{out} = \text{Spl}.\text{Sign}(sk'_B, m^{out})$;
25. else
   26. Compute $\sigma^{out} = \text{Spl}.\text{Sign}(sk'_A, m^{out})$;

27. Output $st^{out} = (t + 1, st^{out}, v^{out}, w^{out}, \sigma^{out}), a^{out}_{st^-\cdot\cdot} = a^{out}_{st^-\cdot\cdot}$. 

108
Algorithm 43: $\tilde{F}_{0,2',i,5}$

Input: $\tilde{\mathbf{st}} = (t, \mathbf{st}_t, \mathbf{v}_t, \mathbf{w}_t, \sigma_t)$, $\tilde{\mathbf{a}}_{a_t-\mathbf{M}} = (a_{a_t-\mathbf{M}}, \pi_t)$ where $a_{a_t-\mathbf{M}} = (\mathbf{I}_t, \mathbf{B}_t)$

Data: $T, \mathbb{PP}_{\mathbb{Acc}}, \mathbb{PP}_{\mathbb{Itr}}, K_A, K_B, \mathbf{m}_i, \mathbf{m}_{i+1}$

1. If Acc.VerifyRead$(\mathbb{PP}_{\mathbb{Acc}}, \mathbf{w}_t, \mathbf{I}_t, \mathbf{B}_t, \pi_t) = 0$ output Reject;
2. Compute $r_A = \text{PRF}(K_A, t - 1)$, $r_B = \text{PRF}(K_B, t - 1)$;
3. Compute $(\mathbf{sk}_A, \mathbf{vk}_A, \mathbf{vk}_{A, \text{rej}}) = \text{Spl.Setup}(1^\lambda; r_A)$, $(\mathbf{sk}_B, \mathbf{vk}_B, \mathbf{vk}_{B, \text{rej}}) = \text{Spl.Setup}(1^\lambda; r_B)$;
4. Set $\mathbf{m}_t = (\mathbf{v}_t, \mathbf{st}_t, \mathbf{w}_t, \mathbf{I}_t)$ and $\alpha = \leftarrow$;
5. If $\text{Spl.Verify}(\mathbf{vk}_A, \mathbf{m}_t, \pi_t) = 1$ set $\alpha = \leftarrow$;
6. If $\alpha = \leftarrow$ and $(t > t^* \text{ or } t < i + 1)$ output Reject;
7. If $\alpha \neq \leftarrow$ and $\text{Spl.Verify}(\mathbf{vk}_B, \mathbf{m}_t, \pi_t) = 1$ set $\alpha = \leftarrow$;
8. If $\alpha = \leftarrow$ output Reject;

9. if $\alpha = \leftarrow$ or $t < i + 1$ then
   $\quad$ Compute $(\mathbf{st}_t, a_{a_t-\mathbf{M}}) \leftarrow F^1(\mathbf{st}_t, a_{a_t-\mathbf{M}})$
10. else
    $\quad$ Compute $(\mathbf{st}_t, a_{a_t-\mathbf{M}}) \leftarrow F^0(\mathbf{st}_t, a_{a_t-\mathbf{M}})$
11. If $\mathbf{st}_t = \text{Reject}$, output Reject;

14. $\mathbf{w}_t = \text{Acc.Update}(\mathbb{PP}_{\mathbb{Acc}}, \mathbf{w}_t, \mathbf{B}_t, \pi_t)$;
15. If $\mathbf{w}_t = \text{Reject}$ output Reject;
16. Compute $\mathbf{v}_t = \text{Itr.\,\,Iterate}(\mathbb{PP}_{\mathbb{Itr}}, \mathbf{v}_t, (\mathbf{st}_t, \mathbf{w}_t, \mathbf{I}_t))$;
17. If $\mathbf{v}_t = \text{Reject}$ output Reject;
18. Compute $r'_A = \text{PRF}(K_A, t)$, $r'_B = \text{PRF}(K_B, t)$;
19. Compute $(\mathbf{sk}'_A, \mathbf{vk}'_A, \mathbf{vk}'_{A, \text{rej}}) = \text{Spl.Setup}(1^\lambda; r'_A)$, $(\mathbf{sk}'_B, \mathbf{vk}'_B, \mathbf{vk}'_{B, \text{rej}}) = \text{Spl.Setup}(1^\lambda; r'_B)$;
20. Set $\mathbf{m}_t = (\mathbf{v}_t, \mathbf{st}_t, \mathbf{w}_t, \mathbf{I}_t)$;
21. if $t = i + 1$ and $(\mathbf{m}_t = \mathbf{m}_i \text{ and } \mathbf{m}_t = \mathbf{m}_i + 1)$ then
   $\quad$ Compute $\sigma_t = \text{Spl.Sign}(\mathbf{sk}'_A, \mathbf{m}_t)$;
22. else if $t = i + 1$ and $(\mathbf{m}_t = \mathbf{m}_i \text{ or } \mathbf{m}_t = \mathbf{m}_i + 1)$ then
    $\quad$ Compute $\sigma_t = \text{Spl.Sign}(\mathbf{sk}'_B, \mathbf{m}_t)$;
23. else
    $\quad$ Compute $\sigma_t = \text{Spl.Sign}(\mathbf{sk}'_A, \mathbf{m}_t)$;
27. Output $\tilde{\mathbf{st}}_t = (t + 1, \mathbf{st}_t, \mathbf{v}_t, \mathbf{w}_t, \sigma_t)$, $\tilde{\mathbf{a}}_{a_t-\mathbf{M}} = a_{a_t-\mathbf{M}}$;
Algorithm 44: \( \tilde{F}^{0,2_t,i_8} \)

**Input**: \( \text{st}^{\text{in}} = (t, \text{st}^{\text{in}}, v^{\text{in}}, w^{\text{in}}, \sigma^{\text{in}}), \) \( \text{out}^{\text{in}} = (a^{\text{in}}_{k^{\text{in}}}, \pi^{\text{in}}) \) where \( a^{\text{in}}_{k^{\text{in}}} = (\text{I}^{\text{in}}, \text{B}^{\text{in}}) \)

**Data**: \( T, \text{pp}_{\text{Acc}}, \text{pp}_{\text{Itr}}, K_A, K_B, m^{i+1} \)

1. If \( \text{Acc. VerifyRead}(\text{pp}_{\text{Acc}}, w^{\text{in}}, \text{I}^{\text{in}}, \text{B}^{\text{in}}, \pi^{\text{in}}) = 0 \) output \text{Reject};
2. Compute \( r_A = \text{PRF}(K_A, t - 1), r_B = \text{PRF}(K_B, t - 1); \)
3. Compute \( (\text{sk}_A, \text{vk}_A, \text{vk}_A, \text{rej}) = \text{Spl. Setup}(1^\lambda; r_A), (\text{sk}_B, \text{vk}_B, \text{vk}_B, \text{rej}) = \text{Spl. Setup}(1^\lambda; r_B); \)
4. Set \( m^{\text{in}} = (v^{\text{in}}, \text{st}^{\text{in}}, w^{\text{in}}, \text{I}^{\text{in}}) \) and \( \alpha = \cdot A; \)
5. If \( \text{Spl. Verify}(\text{vk}_A, m^{\text{in}}, \sigma^{\text{in}}) = 1 \) set \( \alpha = \cdot A; \)
6. If \( \alpha = \cdot A; \) and \( (t > t^* \text{ or } t \leq i + 1) \) output \text{Reject};
7. If \( \alpha \neq \cdot A; \) and \( \text{Spl. Verify}(\text{vk}_B, m^{\text{in}}, \sigma^{\text{in}}) = 1 \) set \( \alpha = \cdot B; \)
8. If \( \alpha = \cdot A; \) output \text{Reject};
9. If \( \alpha = \cdot B; \) or \( t \leq i + 1 \) then
   10. Compute \( (\text{st}^{\text{out}}, \text{out}^{\text{out}}_{k^{\text{in}}}) \leftarrow F^1(\text{st}^{\text{in}}, a^{\text{in}}_{k^{\text{in}}}); \)
11. else
   12. Compute \( (\text{st}^{\text{out}}, \text{out}^{\text{out}}_{k^{\text{in}}}) \leftarrow F^0(\text{st}^{\text{in}}, a^{\text{in}}_{k^{\text{in}}}); \)
13. If \( \text{st}^{\text{out}} = \text{Reject}, \) output \text{Reject};
14. \( w^{\text{out}} = \text{Acc. Update}(\text{pp}_{\text{Acc}}, w^{\text{in}}, \text{B}^{\text{out}}, \pi^{\text{in}}); \)
15. If \( w^{\text{out}} = \text{Reject} \) output \text{Reject};
16. Compute \( v^{\text{out}} = \text{Itr. Iterate}(\text{pp}_{\text{Itr}}, v^{\text{in}}, (\text{st}^{\text{in}}, w^{\text{in}}, \text{I}^{\text{in}})); \)
17. If \( v^{\text{out}} = \text{Reject} \) output \text{Reject};
18. Compute \( r'_A = \text{PRF}(K_A, t), r'_B = \text{PRF}(K_B, t); \)
19. Compute \( (\text{sk}'_A, \text{vk}'_A, \text{vk}'_A, \text{rej}) = \text{Spl. Setup}(1^\lambda; r'_A), (\text{sk}'_B, \text{vk}'_B, \text{vk}'_B, \text{rej}) = \text{Spl. Setup}(1^\lambda; r'_B); \)
20. Set \( m^{\text{out}} = (v^{\text{out}}, \text{st}^{\text{out}}, w^{\text{out}}, \text{I}^{\text{out}}); \)
21. if \( t = i + 1 \) and \( (m^{\text{out}} = m^{i+1}) \) then
   22. Compute \( \sigma^{\text{out}} = \text{Spl. Sign}(\text{sk}'_A, m^{\text{out}}); \)
23. else if \( t = i + 1 \) and \( (m^{\text{out}} \neq m^{i+1}) \) then
   24. Compute \( \sigma^{\text{out}} = \text{Spl. Sign}(\text{sk}'_B, m^{\text{out}}); \)
25. else
   26. Compute \( \sigma^{\text{out}} = \text{Spl. Sign}(\text{sk}'_A, m^{\text{out}}); \)
27. Output \( \tilde{\text{st}}^{\text{out}} = (t + 1, \text{st}^{\text{out}}, v^{\text{out}}, w^{\text{out}}, \sigma^{\text{out}}), \) \( \tilde{\text{out}}^{\text{out}}_{k^{\text{in}}} = \text{out}^{\text{out}}_{k^{\text{in}}}; \)
Hyb\(_{0,2',t^*-1,1}\). In this hybrid, the challenger makes the accumulator ‘read enforcing’. Based on the initial configuration, we first obtain \(\{(j, \text{mem}^0[j])\}_{j=1}^{\text{mem}^0}\). Let \(\ell = |\text{mem}^0|\). It computes the first \(t^* - 1\) ‘correct inputs’ for the accumulator. Then we run the following algorithm to obtain \(\{a_j^0\}_{j=0}^{t^*-1}\).

**Algorithm 45:** This algorithm is for Hyb\(_{0,2',t^*-1,1}\).

\[
\begin{array}{ll}
\text{for } j \in \{1, \ldots, t^* - 1\} & \\
\text{Compute } (st^j, a_{H^\leftarrow A}^j) \leftarrow F^0(st^{j-1}, a_{H^\leftarrow A}^{j-1}) ; & // a_{H^\leftarrow A}^{j-1} = (V^{-1}, B^{j-1}) \\
\text{(mem}^j, a_{H^\leftarrow A}^j) \leftarrow \text{access}(\text{mem}^{j-1}, a_{H^\leftarrow A}^{j-1}) ; & // a_{H^\leftarrow A}^{j} = (V, B^j)
\end{array}
\]

Now we set

\[
\text{enf} = \left( (1, \text{mem}^0[1]), \ldots, (\ell, \text{mem}^0[\ell]), (I^0, B^0), \ldots, (I^{t^*-2}, B^{t^*-2}) \right)
\]

Finally, the challenger computes \((pp_{\text{Acc}}, \hat{w}_0, \text{store}_0) \leftarrow \text{Acc.SetupEnforceRead}(1^\lambda; T, \text{enf}, I^{t^*-1})\).

Hyb\(_{0,2',t^*-1,2}\). In this hybrid, the challenger outputs an obfuscation of \(\hat{F}^{0,3}\).

Hyb\(_{0,2',t^*-1,3}\). In this hybrid, the challenger uses Acc.Setup instead of using Acc.SetupEnforceRead

**Claim B.34.** Let Acc be an accumulator which satisfies indistinguishability of Read Setup (Definition A.3). Then for any PPT adversary \(A\), \(|\text{Adv}_{A}^{0,2',t^*-1,1} - \text{Adv}_{A}^{0,2',t^*-1,1}| \leq \text{negl}(\lambda)\).

*Proof.* This proof is similar to that for Claim B.16.

**Claim B.35.** Let iO be a secure indistinguishability obfuscator. Then for any PPT adversary \(A\), \(|\text{Adv}_{A}^{0,2',t^*-1,1} - \text{Adv}_{A}^{0,2',t^*-1,1}| \leq \text{negl}(\lambda)\).

**Claim B.36.** Let Acc be an accumulator which satisfies indistinguishability of Read Setup (Definition 4.1). Then for any PPT adversary \(A\), \(|\text{Adv}_{A}^{0,2',t^*-1,2} - \text{Adv}_{A}^{0,2',t^*-1,3}| \leq \text{negl}(\lambda)\).

*Proof.* This proof is similar to that for Claim B.16.

### B.1.5 From Hyb\(_{0,3}\) to Hyb\(_{0,4}\)

**Lemma B.37.** Let iO be a secure indistinguishability obfuscator, PRF be a selectively secure puncturable PRF and Spl be a secure splitting signature scheme. Then for any PPT adversary \(A\), \(|\text{Adv}_{A}^{0,3} - \text{Adv}_{A}^{0,4}| \leq \text{negl}(\lambda)\).

*Proof.* We will define \(T - t^* + 1\) hybrids, and show they are computationally indistinguishable.

Hyb\(_{0,3,i}\). In this hybrid, the challenger outputs an obfuscation of \(\hat{F}^{0,3,i}\) defined in Algorithm 46 for \(t^* \leq i \leq T\).

Clearly, programs \(\hat{F}^{0,3,i}\) and \(\hat{F}^{0,3,i'}\) are functionally identical, and therefore Hyb\(_{0,3}\) and Hyb\(_{0,3,i'}\) are computationally indistinguishable. In addition, hybrids Hyb\(_{0,3,T}\) and Hyb\(_{0,4}\) are functionally identical, since the difference between these two hybrids is a dummy code which has never been executed. In order to show that Hyb\(_{0,3,i}\) and Hyb\(_{0,3,i+1}\) are computationally indistinguishable, we define intermediate hybrid experiments Hyb\(_{0,3,i,a}\), Hyb\(_{0,3,i,a}\), ..., Hyb\(_{0,3,i,f}\) as follows. Note that Hyb\(_{0,3,i,a}\) corresponds to Hyb\(_{0,3,i}\) and Hyb\(_{0,3,i,f}\) corresponds to Hyb\(_{0,3,i+1}\).
\textbf{Hyb}_{0,3,i,a}. This hybrid corresponds to \textbf{Hyb}_{0,3,i}.

\textbf{Hyb}_{0,3,i,b}. In this hybrid, the challenger first punctures the PRF key $K_A$ on input $i$ by computing $K_A \{i\} \leftarrow \text{PRF}.\text{Puncture}(K_A, i)$. Next, it computes $r_C = \text{PRF}(K_A, i)$ and $(sk_C, vk_C, vk_{C, \text{rej}}) = \text{Spl}.\text{Setup}(1^\lambda; r_C)$. It outputs an obfuscation of $\widehat{F}^{0,3,i,b}$ defined in Algorithm 47. This program is similar to $\widehat{F}^{0,3,i,a}$ except that it has $K_A \{i\}$ and $vk_{C, \text{rej}}$ hardwired, and when $t = i$, it replaces $vk_{A, \text{rej}}$ by $vk_{C, \text{rej}}$.

\textbf{Hyb}_{0,3,i,c}. This hybrid is similar to \textbf{Hyb}_{0,3,i,b}, except that $r_C$ is now chosen uniformly at random from $\{0, 1\}^\lambda$.

\textbf{Hyb}_{0,3,i,d}. This hybrid is similar to \textbf{Hyb}_{0,3,i,c}, except that $vk_{C, \text{rej}}$ is hardwired to the program.

\textbf{Hyb}_{0,3,i,e}. This hybrid is similar to \textbf{Hyb}_{0,3,i,d}, except that $r_C = \text{PRF}(K_B, i)$ is now pseudorandom.

\textbf{Hyb}_{0,3,i,f}. This hybrid corresponds to \textbf{Hyb}_{0,3,i+1}.

\textbf{Claim B.38}. Let $iO$ be a secure indistinguishability obfuscator. Then for any PPT adversary $A$, $|\text{Adv}_A^{0,3,i} - \text{Adv}_A^{0,3,i,a}| \leq \text{negl}(\lambda)$.

\textit{Proof.} Observe that $\widehat{F}^{0,3,i}$ and $\widehat{F}^{0,3,i,a}$ have identical functionality. Therefore \textbf{Hyb}_{0,3,i} and \textbf{Hyb}_{0,3,i,a} are computationally indistinguishable under the assumption that $iO$ is a secure indistinguishability obfuscation scheme.

\textbf{Claim B.39}. Let $iO$ be a secure indistinguishability obfuscator. Then for any PPT adversary $A$, $|\text{Adv}_A^{0,3,i,a} - \text{Adv}_A^{0,3,i,b}| \leq \text{negl}(\lambda)$.

\textit{Proof.} Note that the only difference between $\widehat{F}^{0,3,i,a}$ and $\widehat{F}^{0,3,i,b}$ is that the later uses a punctured PRF key $K_A \{i\}$ to compute the verification key for time $t - 1$ and the signing key for time $t$. For verification, the functionality is preserved since $vk_{C, \text{rej}}$ is hardwired to the circuit. For signing, the type key is never used to sign at time $t = i$. Therefore \textbf{Hyb}_{0,3,i,a} and \textbf{Hyb}_{0,3,i,b} are computationally indistinguishable.

\textbf{Claim B.40}. Let PRF be a selectively secure puncturable PRF. Then for any PPT adversary $A$, $|\text{Adv}_A^{0,3,i,b} - \text{Adv}_A^{0,3,i,c}| \leq \text{negl}(\lambda)$.

\textit{Proof.} Since both $\widehat{F}^{0,3,i,b}$ and $\widehat{F}^{0,3,i,c}$ depend only on $K_A \{i\}$, by the security of indistinguishability obfuscation, the value of PRF$(K_A, i)$ can be replaced by a random value. Therefore \textbf{Hyb}_{0,3,i,b} and \textbf{Hyb}_{0,3,i,c} are computationally indistinguishable under the assumption that PRF is selectively secure puncturable PRF.

\textbf{Claim B.41}. Let Spl be a splittable signature scheme which satisfies $vk_{\text{rej}}$ indistinguishability (Definition A.7). Then for any PPT adversary $A$, $|\text{Adv}_A^{0,3,i,c} - \text{Adv}_A^{0,3,i,d}| \leq \text{negl}(\lambda)$.

\textit{Proof.} Note that $sk_C$ is not hardwired in either $\widehat{F}^{0,3,i,c}$ or $\widehat{F}^{0,3,i,d}$. Based on the $vk_{\text{rej}}$ indistinguishability property of splittable signature scheme Spl, given only $vk_C$ or $vk_{C, \text{rej}}$, the two hybrids are computationally indistinguishable.

\textbf{Claim B.42}. Let PRF be a selectively secure puncturable PRF. Then for any PPT adversary $A$, $|\text{Adv}_A^{0,3,i,d} - \text{Adv}_A^{0,3,i,e}| \leq \text{negl}(\lambda)$.  

112
Proof. Since both $\tilde{F}^{0,3,i,d}$ and $\tilde{F}^{0,3,i,e}$ depend only on $K_B\{i\}$, by the security of indistinguishability obfuscation, the random value can be switched back to $\text{PRF}(K_B,i)$. Therefore $\text{Hyb}_{0,3,i,d}$ and $\text{Hyb}_{0,3,i,e}$ are computationally indistinguishable. \hfill \qed

Claim B.43. Let $i\mathcal{O}$ be a secure indistinguishability obfuscator. Then for any PPT adversary $A$, $|\text{Adv}_A^{0,3,i,e} - \text{Adv}_A^{0,3,i,f}| \leq \text{negl}(\lambda)$.

Proof. Observe that $\tilde{F}^{0,3,i,e}$ and $\tilde{F}^{0,3,i,f}$ have identical functionality. Therefore $\text{Hyb}_{0,3,i,e}$ and $\text{Hyb}_{0,3,i,f}$ are computationally indistinguishable under the assumption that $i\mathcal{O}$ is a secure indistinguishability obfuscation scheme. \hfill \qed

Claim B.44. Let $i\mathcal{O}$ be a secure indistinguishability obfuscator. Then for any PPT adversary $A$, $|\text{ Adv}_A^{0,3,i,f} - \text{ Adv}_A^{0,3,i+1}| \leq \text{negl}(\lambda)$.

Proof. Observe that $\tilde{F}^{0,3,i,f}$ and $\tilde{F}^{0,3,i+1}$ have identical functionality. Therefore $\text{Hyb}_{0,3,i,f}$ and $\text{Hyb}_{0,3,i+1}$ are computationally indistinguishable under the assumption that $i\mathcal{O}$ is a secure indistinguishability obfuscation scheme. \hfill \qed

To conclude, we have for all PPT $A$, $|\text{Adv}_A^{0,3,i} - \text{Adv}_A^{0,3,i+1}| \leq \text{negl}(\lambda)$ as required. \hfill \qed

B.2 Proof of Lemma 7.3 (Security for Topological Iterators)

Proof. To prove this lemma, we define $\text{Hyb}_0, \ldots, \text{Hyb}_3$.

$\text{Hyb}_0$ In this experiment, the Challenger always sends the normal setup, $(\text{pp}_{\text{Itr}}^{*}, v) \leftarrow \text{Tltr.Setup}(1^\lambda, N)$, to $A$.

$\text{Hyb}_1$ In this experiment, the Challenger computes the normal setup $\text{Tltr.Setup}(1^\lambda, N)$ and the enforced setup with the sink point $ct^{*}$ hard-wired $(\text{pp}_{\text{Itr}}^{*}, K\{v_{l,\text{sink}}, v_{r,\text{sink}}, m_{\text{sink}}\}, v) \leftarrow \text{Tltr.SetupEnf}(1^\lambda, N, \text{DAG})$, and it sends one of the two to $A$.

$\text{Hyb}_2$ In this experiment, the Challenger computes the normal setup $\text{Tltr.Setup}(1^\lambda, N)$ and the enforced setup with the sink point $ct^{*}$ (encrypted with a fresh randomness) hard-wired $(\text{pp}_{\text{Itr}}^{*}, K\{v_{l,\text{sink}}, v_{r,\text{sink}}, m_{\text{sink}}\}, v) \leftarrow \text{Tltr.SetupEnf}(1^\lambda, N, \text{DAG})$, and it sends one of the two to $A$.

$\text{Hyb}_3$ In this experiment, the Challenger computes the normal setup $\text{Tltr.Setup}(1^\lambda, N)$ and the enforced setup and it sends one of the two to $A$.

Claim B.45. $\text{Hyb}_3$ has only negligible advantage over $\text{Hyb}_0$.

Proof. Given that $\text{Tltr.SetupEnf}$ requires each node $n$ has a unique message value $m_{n} \in M_\lambda$, $\text{progEnforce}$ only differs from $\text{prog}$ at the input $(v_{l,\text{sink}}, v_{r,\text{sink}}, m_{\text{sink}})$. Thus we focused on the sink point in following hybrid steps. Assuming $i\mathcal{O}$ is a secure indistinguishable obfuscator, $\text{Hyb}_0 \approx \text{Hyb}_1$ because $\text{pp}_{\text{Itr}}$ and $\text{pp}_{\text{Itr}}^{*}$ are functionally equivalent. $\text{Hyb}_1 \approx \text{Hyb}_2$ by the selective security of puncturable PRF (because the only difference is the randomness at the punctured point). $\text{Hyb}_2 \approx \text{Hyb}_3$ by the semantic security of $PKE$.

The adversary $A$ has no advantage in $\text{Hyb}_0$, and $\text{Hyb}_3$ (which is the $\text{Exp-Setup-Itr}$ game) has only negligible advantage over $\text{Hyb}_0$. Therefore, any PPT adversary $A$ has only negligible advantage in the $\text{Exp-Setup-Itr}$ game. \hfill \qed
Algorithm 46: \( F^{0,3,i} \)

**Input**: \( \tilde{s}^{in} = (t, s^{in}, v^{in}, w^{in}, \sigma^{in}) \), \( \tilde{a}^{in} = (a^{in}, \pi^{in}) \) where \( a^{in} = (I^{in}, B^{in}) \)

**Data**: \( T, pp_{\text{Acc}}, pp_{\text{Itr}}, K_A, K_B, t^* \)

1. If \( t^* < t \leq i \), output \text{Reject};
2. If \( \text{Acc.VerifyRead}(pp_{\text{Acc}}, w^{in}, I^{in}, B^{in}, \pi^{in}) = 0 \) output \text{Reject};
3. Compute \( r_A = \text{PRF}(K_A, t - 1), r_B = \text{PRF}(K_B, t - 1); \)
4. Compute \( (sk_A, vk_A, vk_{A,\text{rej}}) = \text{Spl.Setup}(1^\lambda; r_A), (sk_B, vk_B, vk_{B,\text{rej}}) = \text{Spl.Setup}(1^\lambda; r_B); \)
5. Set \( m^{in} = (v^{in}, s^{in}, w^{in}, I^{in}); \)
6. If \( \text{Spl.Verify}(vk_A, m^{in}, \sigma^{in}) = 0 \) output \text{Reject};
7. if \( t \leq t^* \) then
   8. Compute \( (s^{out}, a^*_A) \leftarrow F^1(s^{in}, a^{in}) \)
9. else
   10. Compute \( (s^{out}, a^*_A) \leftarrow F^0(s^{in}, a^{in}) \)
11. If \( s^{out} = \text{Reject} \), output \text{Reject};
12. \( w^{out} = \text{Acc.Update}(pp_{\text{Acc}}, w^{in}, B^{out}, \pi^{in}); \)
13. If \( w^{out} = \text{Reject} \) output \text{Reject};
14. Compute \( v^{out} = \text{Itr.Iterate}(pp_{\text{Itr}}, v^{in}, (s^{in}, w^{in}, I^{in})); \)
15. If \( v^{out} = \text{Reject} \) output \text{Reject};
16. Compute \( r'_A = \text{PRF}(K_A, t), r'_B = \text{PRF}(K_B, t); \)
17. Compute \( (sk'_A, vk'_A, vk'_{A,\text{rej}}) = \text{Spl.Setup}(1^\lambda; r'_A), (sk'_B, vk'_B, vk'_{B,\text{rej}}) = \text{Spl.Setup}(1^\lambda; r'_B); \)
18. Set \( m^{out} = (v^{out}, s^{out}, w^{out}, I^{out}); \)
19. if \( t = t^* \) then
   20. Compute \( \sigma^{out} = \text{Spl.Sign}(sk'_B, m^{out}); \)
21. else
   22. Compute \( \sigma^{out} = \text{Spl.Sign}(sk'_A, m^{out}); \)
23. Output \( \tilde{s}^{out} = (t + 1, s^{out}, v^{out}, w^{out}, \sigma^{out}), \tilde{a}^{out} = a^*_A; \)
Algorithm 47: $F^{0,3,i,b}$

Input: $\tilde{st}^{in} = (t, st^{in}, v^{in}, w^{in}, \sigma^{in})$, $\tilde{st}^{in} = (a^{in}_A, \pi^{in})$ where $a^{in}_A = (I^{in}, B^{in})$

Data: $T, pp_{\text{Acc}}, pp_{\text{itr}}, K_A\{i\}, K_B, t^*, v_k$

1. If $t^* < t \leq i$, output Reject;
2. If Acc.VerifyRead($pp_{\text{Acc}}, w^{in}, I^{in}, B^{in}, \pi^{in}$) = 0 output Reject;
3. If $t \neq i + 1$ then
   4. Compute $r_A = \text{PRF}(K_A\{i\}, t - 1)$, $r_B = \text{PRF}(K_B, t - 1)$;
   5. Compute $(sk_A, vk_A, vk_{A,rej}) = \text{Spl.Setup}(1^\lambda; r_A), (sk_B, vk_B, vk_{B,rej}) = \text{Spl.Setup}(1^\lambda; r_B)$;
4. else
   7. Set $vk_A = vk$;
8. Set $m^{in} = (v^{in}, st^{in}, w^{in}, I^{in})$;
9. If Spl.Verify($vk_A, m^{in}, \sigma^{in}$) = 0 output Reject;
10. if $t \leq t^*$ then
11. Compute $(st^{out}, a^{out}_{M-A}) \leftarrow F^1(st^{in}, a^{in}_{k-M})$
12. else
13. Compute $(st^{out}, a^{out}_{M-A}) \leftarrow F^0(st^{in}, a^{in}_{k-M})$
14. If $st^{out} = \text{Reject}$, output Reject;
15. $w^{out} = \text{Acc.Update}(pp_{\text{Acc}}, w^{in}, B^{out}, \pi^{in})$;
16. If $w^{out} = \text{Reject}$ output Reject;
17. Compute $v^{out} = \text{itr.Iterate}(pp_{\text{itr}}, v^{in}, (st^{in}, w^{in}, I^{in}))$;
18. If $v^{out} = \text{Reject}$ output Reject;
19. Compute $r'_A = \text{PRF}(K_A, t), r'_B = \text{PRF}(K_B, t)$;
20. Compute $(sk'_A, vk'_A, vk'_{A,rej}) = \text{Spl.Setup}(1^\lambda; r'_A), (sk'_B, vk'_B, vk'_{B,rej}) = \text{Spl.Setup}(1^\lambda; r'_B)$;
21. Set $m^{out} = (v^{out}, st^{out}, w^{out}, I^{out})$;
22. if $t = t^*$ then
23. Compute $\sigma^{out} = \text{Spl.Sign}(sk'_B, m^{out})$;
24. else
25. Compute $\sigma^{out} = \text{Spl.Sign}(sk'_A, m^{out})$;
26. Output $\tilde{st}^{out} = (t + 1, st^{out}, v^{out}, w^{out}, \sigma^{out}), \tilde{a}^{out}_{M-A} = a^{out}_{M-A}$.
B.3 Proof of Theorem 7.6 (Security for CiO-PRAM−)

We now prove the security for our CiO in the PRAM− model. The proof idea is essentially similar to that for CiO for RAM. We first allow the program to accept ‘B’ signatures, so to do this we can straightly use the sequence of hybrids backward from time \( i = t^* \) to 0. Then, we slowly switch \( F^0 \) by \( F^1 \) from \( t = 0 \) to \( t = t^* \). Recall that now both \( F^0 \) and \( F^1 \) include the branch and combine stages. The branch stage takes care of using the same techniques in the proof of CiO for RAM. In particular, the main challenge here is the combine stage. We will show how this is tackled by hardwiring \( \log m \) amount of information in the intermediate steps of the combine stage.

Proof. To show the contradiction, we suppose the theorem statement is false, and then there exists a security parameter \( 1^λ \), computation systems \( Π^0, Π^1 \) with the identical computation trace, and a PPT adversary \( A \) such that \( |Pr[\mathcal{A}(1^λ, Π^β) = 1] - \frac{1}{2}| \) is non-negligible.

Before proceeding to the proof, we first define some notations and conventions used in the following proof.

- We use \( \widehat{F}' \) to denote a program which is identical to \( \widehat{F} \) except that \( F^\text{branch} \) in \( \widehat{F} \) is replaced by \( F_1 \) and \( F^\text{combine} \) is replaced by \( F_2 \).

- Unless specified, the challenger in each hybrid replaces \( \widehat{F} \) by some \( \widehat{F}' \), so that the computation system \( \widehat{Π} \) defined by \( \widehat{F} \) is replaced by another computation system \( \widehat{Π}' \) that defined by \( \widehat{F}' \) and outputs the obfuscated computation \( \widehat{Π}' ← \text{Obf}(1^λ, \widehat{Π}; ρ) \)

We first define the first-layer hybrids \( \text{Hyb}_β \) for \( β \in \{0, 1\} \).

\( \text{Hyb}_β \). In this hybrid, the challenger replaces \( \widehat{F} \) by \( \widehat{F}^β = F^β_\text{branch} \oplus F^β_\text{combine} \), where \( F^β_\text{branch} \) is similar to \( F^\text{branch} \) except that \( F \) is replaced by \( F^β \).

Let us assume that the program \( \widehat{F}^β \) terminates at time \( t^* < T \). To argue that \( |\text{Adv}_A^β - \text{Adv}_A^1| ≤ \text{negl}(λ) \), we define the second- and third-layer hybrids \( \text{Hyb}_{0,0}, \text{Hyb}_{0,0,i}, \text{Hyb}_{0,1}, \text{Hyb}_{0,1,i}, \text{Hyb}_{0,2}, \text{Hyb}_{0,3} \) for \( 0 ≤ i ≤ t^* - 1 \).

\( \text{Hyb}_{0,0} \). This hybrid is identical to \( \text{Hyb}_0 \) in the first layer.

\( \text{Hyb}_{0,0,i} \). In this hybrid, the challenger replaces \( \widehat{F} \) by \( \widehat{F}^{0,0,i} = F^{0,0,i}_\text{branch} \oplus F^{0,0,i}_\text{combine} \), defined in Algorithms 48 and 49. \( \widehat{F}^{0,0,i} \) is similar to \( \widehat{F}^{0,0} \) except the following differences.

- \( F^{0,0,i}_\text{branch} \) uses \( F^1 \) to compute the output if the incoming signature is ‘B’ type.
- At \( i + 1 ≤ t ≤ t^* - 1 \), \( F^{0,0,i}_\text{branch} \) and \( F^{0,0,i}_\text{combine} \) accept ‘B’ type signatures.
- At \( i + 1 ≤ t ≤ t^* - 1 \), \( F^{0,0,i}_\text{branch} \) and \( F^{0,0,i}_\text{combine} \) follow the type of the incoming signature to generate the type of the outgoing signature.

\( \text{Hyb}_{0,1} \). In this hybrid, the challenger replaces \( \widehat{F} \) by \( \widehat{F}^{0,1} = F^{0,1}_\text{branch} \oplus F^{0,1}_\text{combine} \), defined in Algorithms 50 and 51. This program is similar to \( \widehat{F}^0 \) except that it has PRF key \( K_B \) hardwired, accepts both ‘A’ and ‘B’ type signatures at time \( t < t^* \). The type of the outgoing signature follows the type of the incoming signature. In addition, if the incoming signature is ‘B’ type and \( t < t^* \), then \( F^{0,1}_\text{branch} \) uses \( F^1 \) to compute the output.

\( \text{Hyb}_{0,1,i} \). In this hybrid, the challenger replaces \( \widehat{F} \) by \( \widehat{F}^{0,1,i} = F^{0,1,i}_\text{branch} \oplus F^{0,1,i}_\text{combine} \), defined in Algorithms 52 and 53. \( \widehat{F}^{0,1,i} \) is similar to \( \widehat{F}^{0,1} \) except the following differences.

- At \( t ≤ i \), \( F^{0,1,i}_\text{branch} \) uses \( F^1 \) to compute the output; otherwise, uses \( F^0 \).
- At \( t = i \), \( F^{0,1,i}_\text{branch} \) has the correct input message \( m \) hardwired.
- At \( t = i \), \( F^{0,1,i}_\text{branch} \) outputs an ‘A’ type signature if \( m_{out} = m; ‘B’ \) type otherwise.
- At \(i + 1 \leq t \leq t^* - 1\), \(F_{\text{branch}}^{0,1,i}\) and \(F_{\text{combine}}^{0,1,i}\) accept ‘B’ type signatures.
- At \(i + 1 \leq t \leq t^* - 1\), \(F_{\text{branch}}^{0,1,i}\) and \(F_{\text{combine}}^{0,1,i}\) follow the type of the incoming signature to generate the type of the outgoing signature.

**Hyb_{0.2}** This hybrid is similar to \(\text{Hyb}_{0.1,t^* - 1}\) except that \(F_{\text{branch}}^{0,2}\) does not hardwire the input message \(m_{t^* - 1}\).

**Hyb_{0.3}** This hybrid is similar to \(\text{Hyb}_{0.2}\) except that \(F_{\text{branch}}^{0,3}\) uses \(F^1\) to compute the output if \(t > t^*\) instead.

**Analysis.** Let \(\text{Adv}^\lambda_A\) denote the advantage of adversary \(A\) in \(\text{Hyb}_z\).

**Lemma B.46.** Assuming \(iO\) is a secure indistinguishability obfuscator, PRF is a selectively secure puncturable PRF, TItr is an topological iterator satisfying Definitions 7.1 and 7.2, Acc is a secure accumulator, Spl is a secure splittable signature scheme. Then for any PPT adversary \(A\), \(|\text{Adv}^{\lambda}_A - \text{Adv}^{\lambda}_A| \leq \text{negl}(\lambda)\).

**Proof.**
- \(\text{Hyb}_0\) is identical to \(\text{Hyb}_{0,0}\)
- \(\text{Hyb}_{0,0,0}\) is identical to \(\text{Hyb}_{0,0,t^* - 1}\)
- \(\text{Hyb}_{0,0,i} \approx \text{Hyb}_{0,0,0,t^* - 1}\) for \(1 \leq i \leq t^*\) will be proven in Section B.3.1
- \(\text{Hyb}_{0,0,0}\) is identical to \(\text{Hyb}_{0,1}\) \(\blacksquare\)

**Lemma B.47.** Assuming \(iO\) is a secure indistinguishability obfuscator, \(|\text{Adv}^{\lambda}_A - \text{Adv}^{\lambda}_A| \leq \text{negl}(\lambda)\).

**Proof.**
- \(\text{Hyb}_{0.1} \approx \text{Hyb}_{0.1,0}\) since the programs \(\hat{F}^{0,1}\) and \(\hat{F}^{0,1,0}\) are functionally identical
- \(\text{Hyb}_{0.1,i} \approx \text{Hyb}_{0.1,i+1}\) for \(0 \leq i \leq t^* - 1\) will be proven in Section B.3.2
- \(\text{Hyb}_{0.1,t^* - 1} \approx \text{Hyb}_{0.2}\) since the programs \(\hat{F}^{0,1,t^* - 1}\) and \(\hat{F}^{0,2}\) are functionally identical \(\blacksquare\)

**Lemma B.48.** Assuming \(iO\) is a secure indistinguishability obfuscator, \(|\text{Adv}^{\lambda}_A - \text{Adv}^{\lambda}_A| \leq \text{negl}(\lambda)\).

**Proof.** The programs \(\hat{F}^{0,2}\) and \(\hat{F}^{0,3}\) are functionally identical, since they run neither \(F^0\) nor \(F^1\) at time \(t > t^*\) \(\blacksquare\)

**Lemma B.49.** Assuming \(iO\) is a secure indistinguishability obfuscator, PRF is a selectively secure puncturable PRF, TItr is an topological iterator satisfying Definitions 7.1 and 7.2, Acc is a secure positional accumulator, Spl is a secure splittable signature scheme. Then for any PPT adversary \(A\), \(|\text{Adv}^{\lambda}_A - \text{Adv}^{\lambda}_A| \leq \text{negl}(\lambda)\).

The proof of this lemma is identical to the previous proof technique of CiO for RAM. \(\blacksquare\)

**B.3.1 From \(\text{Hyb}_{0,0,3}\) to \(\text{Hyb}_{0,0,1,t^* - 1}\):**

**Lemma B.50.** Assuming \(iO\) is a secure indistinguishability obfuscator, PRF is a selectively secure puncturable PRF, TItr is an topological iterator satisfying Definitions 7.1 and 7.2, Acc is a secure accumulator, Spl is a secure splittable signature scheme. Then for any PPT adversary \(A\), \(|\text{Adv}^{\lambda}_A - \text{Adv}^{\lambda}_A| \leq \text{negl}(\lambda)\).

**Proof.** To argue \(|\text{Adv}^{\lambda}_A - \text{Adv}^{\lambda}_A| \leq \text{negl}(\lambda)\), we define a sequence of fourth-layer hybrids \(\text{Hyb}_{0,0,i,j}\) where \(j\) indexed by the node index via pre-order. For example, in Fig. 3, we consider 4 CPUs, the order of hybrids is \((\text{Hyb}_{0,0,i,e}, \text{Hyb}_{0,0,i,o}, \text{Hyb}_{0,0,i,00}, \text{Hyb}_{0,0,i,01}, \text{Hyb}_{0,0,i,1}, \text{Hyb}_{0,0,i,10}, \text{Hyb}_{0,0,i,11})\).
Algorithm 48: $f_{branch}^{0,0,1}$

**Input:** $\bar{s}^{in} = (st^{in}, id_{cpu}, root\_node), \bar{a}^{in} = (com^{in}, \pi_{st}^{in}, \pi_{com}^{in})$

**Data:** $pp_{Acc, st}, pp_{Acc, com}, pp_{lr}, \bar{K}_{A}$

1. Parse $root\_node$ as $(t, root\_index, w_{st}^{in}, w_{com}^{in}, v^{in}, \sigma_{in})$;
2. Compute $(sk_{A}, vk_{A}, vk_{A, rej}) = Spl. Setup(1, \lambda; r_{A})$ and $(sk_{B}, vk_{B}, vk_{B, rej}) = Spl. Setup(1, \lambda; r_{B})$;
3. Let $\alpha = 'A'$ and $m^{in} = (t, root\_index, w_{st}^{in}, w_{com}^{in}, v^{in})$;
4. if $t \leq i$ then
   5. If Spl.Verify$(vk_{A}, m^{in}, \sigma^{in}) = 1$, set $\alpha = 'A'$;
   6. Else, output $Reject$;
    else
   8. If Spl.Verify$(vk_{A}, m^{in}, \sigma^{in}) = 1$, set $\alpha = 'A'$;
   9. If $\alpha \neq 'A'$ and Spl.Verify$(vk_{B}, m^{in}, \sigma^{in}) = 1$, set $\alpha = 'B'$;
   10. If $\alpha = 'B'$, output $Reject$;
11. If Acc.VerifyRead$(pp_{Acc, st}, w_{st}^{in}, (id_{cpu}, st^{in}), \pi_{st}^{in}) = 0$ output $Reject$;
12. If Acc.VerifyRead$(pp_{Acc, com}, w_{com}^{in}, (src(t, id_{cpu}), com^{in}), \pi_{com}^{in}) = 0$ output $Reject$;
13. if $\alpha = 'B'$ then
   14. Compute $(st^{out}, com^{out}) \leftarrow F^{1}(id_{cpu}, st^{in}, com^{in})$;
   else
   15. Compute $(st^{out}, com^{out}) \leftarrow F^{0}(id_{cpu}, st^{in}, com^{in})$;
   16. Compute $v^{out} = lr. Iterate(pp_{lr}, v^{in}, (t + 1, id_{cpu}, st^{in}, com^{in}, w_{st}^{in}, w_{com}^{in}))$;
   17. if $st^{out} = Reject$ then
   18. Output $Reject$;
   else
   19. Let $r_{A}' = PRF(K_{A}, (t + 1, id_{cpu}))$ and $r_{B}' = PRF(K_{B}, (t + 1, A))$;
   20. Compute $(sk_{A}', vk_{A}', vk_{A, rej}) = Spl. Setup(1, \lambda; r_{A}')$ and $(sk_{B}', vk_{B}', vk_{B, rej}) = Spl. Setup(1, \lambda; r_{B}')$;
   21. Let $m^{out} = (t + 1, id_{cpu}, st^{out}, com^{out}, v^{out})$;
   22. Compute $\sigma^{out} = Spl. Sign(sk_{A}', m^{out})$;
   23. Let $node^{out} = (t + 1, id_{cpu}, st^{out}, com^{out}, v^{out}, \sigma^{out})$;
   24. Output $(st^{out}, id_{cpu}, \perp), \bar{a}^{out} = node^{out}$;
Algorithm 49: $F_{combine}^{0,0,1}$

Input: $st^{in} = (st^{in}, id_{cpu}, \bot), \alpha^{in} = (node_1, node_2)$
Data: $T$, $pp_{Acc,st}, pp_{Acc,com}, pp_{itr}, K_A$
1 Parse node_\zeta as $(t_\zeta, index_\zeta, w_{st,\zeta}, w_{com,\zeta}, v_\zeta, \sigma_\zeta)$ for $\zeta = 1, 2$;
2 If $t_1 \neq t_2$, output Reject. Else, let $t = t_1$;
3 If $t < 1$, output Reject;
4 If $index_1$ and $index_2$ are not siblings, output Reject;
5 Set parent_index as the parent of index_1 and index_2;
6 for $\zeta = 1, 2$ do
7    Let $r_{A,\zeta} = PRF(K_A, (t_\zeta, index_\zeta))$ and $r_{B,\zeta} = PRF(K_B, (t_\zeta, index_\zeta))$;
8    Compute $(sk_{A,\zeta}, vk_{A,\zeta}, vk_{A,\zeta}) = Spl.Setup(1^\lambda; r_{A,\zeta})$ and
9        $(sk_{B,\zeta}, vk_{B,\zeta}, vk_{B,\zeta}) = Spl.Setup(1^\lambda; r_{B,\zeta})$;
10       Let $\alpha_\zeta = 'a'$ and $m_\zeta = (t_\zeta, index_\zeta, w_{st,\zeta}, w_{com,\zeta}, v_\zeta)$;
11          if $t \leq i$ then
12              If Spl.Verify($vk_{A}, m_\zeta, \sigma_\zeta$) = 1, set $\alpha_\zeta = 'A'$;
13                  Else, output Reject;
14          else
15              If Spl.Verify($vk_{A}, m_\zeta, \sigma_\zeta$) = 1, set $\alpha_\zeta = 'A'$;
16                  If $\alpha_\zeta \neq 'A$ and Spl.Verify($vk_{B}, m_\zeta, \sigma_\zeta$) = 1, set $\alpha_\zeta = 'B'$;
17                  If $\alpha_\zeta = 'a'$, output Reject;
18   if $\alpha_1 = 'A$ and $\alpha_2 = 'A$, set $\alpha = 'A'$;
19   Else, set $\alpha = 'B'$;
20   Compute $w'_{st} = Acc.Combine(pp_{Acc,st}, w_{st,1}, w_{st,2})$;
21   Compute $w'_{com} = Acc.Combine(pp_{Acc,com}, w_{com,1}, w_{com,2})$;
22   Compute $v' = ltr.iterate2to1(pp_{itr}, (v_1, v_2), (t, parent.index, w_{st,1}, w_{com,1}, w_{st,2}, w_{com,2}))$;
23   Let $r'_A = PRF(K_A, (t, parent.index))$ and $r'_B = PRF(K_B, (t, parent.index))$;
24   Compute $(sk'_A, vk'_A, vk'_{A,\zeta}) = Spl.Setup(1^\lambda; r'_A)$ and $(sk'_B, vk'_B, vk'_{B,\zeta}) = Spl.Setup(1^\lambda; r'_B)$;
25   Let $m' = (t, parent.index, w'_st, w'_com, v')$;
26       if $t \leq i$ then
27           Compute $\sigma' = Spl.Sign(sk'_A, m')$;
28       else
29           Compute $\sigma' = Spl.Sign(sk'_A, m')$;
30   Let parent_node = $(t, parent.index, w'_st, w'_com, v', \sigma')$;
31       if $parent.index = e$ then
32           Output $st^{out} = (st^{in}, id_{cpu}, parent.node), \alpha^{out} = \bot$;
33       else
34           Output $st^{out} = (st^{in}, id_{cpu}, \bot), \alpha^{out} = parent.node$;
**Algorithm 50**: \( F_{\text{branch}}^{0,1} \)

**Input**: \( \tilde{s}^{\text{in}} = (s^{\text{in}}, id, \text{root} \_\text{node}), \tilde{a}^{\text{in}} = (a^{\text{in}}, \pi^{\text{in}}, a^{\text{in}}) \)

**Data**: \( pp_{\text{Acc, st}}, pp_{\text{Acc, com}}, pp_{\text{itr}}, K_A \)

1. Parse root_node as \( (t, \text{root} \_\text{index}, w^{\text{in}}, w^{\text{com}}, v^{\text{in}}, \sigma^{\text{in}}) \);
2. Let \( r_A = \text{PRF}(K_A, (t, \text{root} \_\text{index})) \) and \( r_B = \text{PRF}(K_B, (t, \text{root} \_\text{index})) \);
3. Compute \( (\text{sk}_A, \text{vk}_A, \text{vk}_A, \text{rej}) = \text{Spl. Setup}(1^\lambda; r_A) \) and \( (\text{sk}_B, \text{vk}_B, \text{vk}_B, \text{rej}) = \text{Spl. Setup}(1^\lambda; r_B) \);
4. Let \( \alpha = \text{‘‘-’’} \) and \( m^{\text{in}} = (t, \text{root} \_\text{index}, w^{\text{in}}, w^{\text{com}}, v^{\text{in}}) \);
5. If \( \text{Spl. Verify}(\text{vk}_A, m^{\text{in}}, \sigma^{\text{in}}) = 1 \), set \( \alpha = \text{‘‘A’’} \);
6. If \( \alpha = \text{‘‘-’’} \) and \( t > t^* \), output Reject;
7. If \( \alpha \neq \text{‘‘A’’} \) and \( \text{Spl. Verify}(\text{vk}_B, m^{\text{in}}, \sigma^{\text{in}}) = 1 \), set \( \alpha = \text{‘‘B’’} \);
8. If \( \alpha = \text{‘‘-’’} \), output Reject;
9. If \( \text{Acc. Verify Read}(pp_{\text{Acc, st}}, w^{\text{in}}, (id, s^{\text{in}}, \pi^{\text{in}})) = 0 \) output Reject;
10. If \( \text{Acc. Verify Read}(pp_{\text{Acc, com}}, w^{\text{com}}, (\text{src}(t, id), \text{com}^{\text{in}}, \pi^{\text{com}})) = 0 \) output Reject;
11. If \( \alpha = \text{‘‘B’’} \) then
12. Compute \( (s^{\text{out}}, \text{com}^{\text{out}}) \leftarrow F^1(id, s^{\text{in}}, \text{com}^{\text{in}}) \);
13. else
14. Compute \( (s^{\text{out}}, \text{com}^{\text{out}}) \leftarrow F^0(id, s^{\text{in}}, \text{com}^{\text{in}}) \);
15. Compute \( v^{\text{out}} = \text{itr. Iterate}(pp_{\text{itr}}, v^{\text{in}}, (t + 1, id, s^{\text{in}}, \text{com}^{\text{in}}, w^{\text{in}}, w^{\text{com}})) \);
16. if \( s^{\text{out}} = \text{Reject} \) then
17. Output Reject;
18. else
19. Let \( r_A = \text{PRF}(K_A, (t + 1, id)) \) and \( r_B = \text{PRF}(K_B, (t + 1, A)) \);
20. Compute \( (\text{sk}_A', \text{vk}_A', \text{vk}_A', \text{rej}) = \text{Spl. Setup}(1^\lambda; r_A') \) and \( (\text{sk}_B', \text{vk}_B', \text{vk}_B', \text{rej}) = \text{Spl. Setup}(1^\lambda; r_B') \);
21. Let \( m^{\text{out}} = (t + 1, id, s^{\text{out}}, \text{com}^{\text{out}}, v^{\text{out}}) \);
22. Compute \( \sigma^{\text{out}} = \text{Spl. Sign}(\text{sk}_A', m^{\text{out}}) \);
23. Let \( \text{node}^{\text{out}} = (t + 1, id, s^{\text{out}}, \text{com}^{\text{out}}, v^{\text{out}}, \sigma^{\text{out}}) \);
24. Output \( s^{\text{out}} = (s^{\text{out}}, id, \perp), a^{\text{out}} = \text{node}^{\text{out}} \);
Algorithm 51: $P_{c_{onb}}^{0,1}$

**Input**: $\text{st}^{\text{in}} = (\text{st}^{\text{in}}, id_{cpu}, \perp), \tilde{\alpha}^{\text{in}} = (\text{node}_1, \text{node}_2)$

**Data**: $T, \text{pp}_{\text{Acc, st}}, \text{pp}_{\text{Acc, com}}, \text{pp}_{\text{itr}}, K_A$

1. Parse node$_\zeta$ as $(t_\zeta, \text{index}_\zeta, w_{st,\zeta}, w_{com,\zeta}, v_\zeta, \sigma_\zeta)$ for $\zeta = 1, 2$;
2. If $t_1 \neq t_2$, output $\text{Reject}$. Else, let $t = t_1$;
3. If $t < 1$, output $\text{Reject}$;
4. If index$_1$ and index$_2$ are not siblings, output $\text{Reject}$;
5. Set parent$_\text{index}$ as the parent of index$_1$ and index$_2$;
6. For $\zeta = 1, 2$
   7. Let $r_{A,\zeta} = \text{PRF}(K_A, (t_\zeta, \text{index}_\zeta))$ and $r_{B,\zeta} = \text{PRF}(K_B, (t_\zeta, \text{index}_\zeta))$;
   8. Compute $(sk_{A,\zeta}, vk_{A,\zeta}, vk_{A,\text{rej},\zeta}) = \text{Spl.Setup}(1^\lambda; r_{A,\zeta})$ and $(sk_{B,\zeta}, vk_{B,\zeta}, vk_{B,\text{rej},\zeta}) = \text{Spl.Setup}(1^\lambda; r_{B,\zeta})$;
   9. Let $\alpha_\zeta = \text{‘}$$\perp$$\text{’}$ and $m_\zeta = (t_\zeta, \text{index}_\zeta, w_{st,\zeta}, w_{com,\zeta}, v_\zeta);$
10. If $\text{Spl.Verify}(vk_A, m_\zeta, \sigma_\zeta) = 1$, set $\alpha_\zeta = \text{‘}A$$\text{’}$;
11. If $\alpha_\zeta \neq \text{‘}A$$\text{’}$ and $\text{Spl.Verify}(vk_B, m_\zeta, \sigma_\zeta) = 1$, set $\alpha_\zeta = \text{‘}B$$\text{’}$;
12. If $\alpha_\zeta = \text{‘}$$\perp$$\text{’}$, output $\text{Reject}$;
13. If $\alpha_1 = \text{‘}A$$\text{’}$ and $\alpha_2 = \text{‘}A$$\text{’}$, set $\alpha = \text{‘}A$$\text{’}$;
14. Else, set $\alpha = \text{‘}B$$\text{’}$;
15. Compute $w_{st} = \text{Acc.Combine}(\text{pp}_{\text{Acc, st}}, w_{st,1}, w_{st,2})$;
16. Compute $w_{com} = \text{Acc.Combine}(\text{pp}_{\text{Acc, com}}, w_{com,1}, w_{com,2})$;
17. Compute $v' = \text{itr.\text{Iterate2to1}}(\text{pp}_{\text{itr}}, (v_1, v_2), (t, \text{parent\_index}, w_{st,1}, w_{com,1}, w_{st,2}, w_{com,2}))$;
18. Let $r_A' = \text{PRF}(K_A, (t, \text{parent\_index}))$ and $r_B' = \text{PRF}(K_B, (t, \text{parent\_index}))$;
19. Compute $(sk_A', vk_{A}', vk_{A,\text{rej}}) = \text{Spl.Setup}(1^\lambda; r_A')$ and $(sk_{B}', vk_{B}', vk_{B,\text{rej}}) = \text{Spl.Setup}(1^\lambda; r_B')$;
20. Let $m' = (t, \text{parent\_index}, w_{st}', w_{com}', v')$;
21. Compute $\sigma' = \text{Spl.Sign}(sk_{\alpha}', m')$;
22. Let parent$_\text{node} = (t, \text{parent\_index}, w_{st}', w_{com}', v', \sigma')$;
23. If $\text{parent\_index} = \epsilon$ then
   24. Output $\text{st}^{\text{out}} = (\text{st}^{\text{in}}, id_{cpu}, \text{parent\_node}), \tilde{\alpha}^{\text{out}} = \perp$;
25. Else
   26. Output $\text{st}^{\text{out}} = (\text{st}^{\text{in}}, id_{cpu}, \perp), \tilde{\alpha}^{\text{out}} = \text{parent\_node}$;
Algorithm 52: \( F_{0,1, \text{branch}} \)

**Input**: \( \tilde{v}^{\text{in}} = (v^{\text{in}}_t, id_{cpu}, \text{root\_node}), \tilde{a}^{\text{in}} = (com^{\text{in}}_t, \pi_\text{st}^{\text{in}}, \pi_\text{com}^{\text{in}}) \)

**Data**: \( \text{pp}_{\text{Acc, st}}, \text{pp}_{\text{Acc, com}}, \text{pp}_{\text{tr}}, K_A, K_B, m_i, \text{Root} \)

1. Parse \text{root\_node} as \((t, \text{root\_index}, w^{\text{in}}_\text{st}, w^{\text{in}}_\text{com}, v^{\text{in}}, \sigma^{\text{in}})\);
2. Let \( r_A = \text{PRF}(K_A, (t, \text{root\_index})) \) and \( r_B = \text{PRF}(K_B, (t, \text{root\_index})) \);
3. Compute \((sk_A, vk_A, vk_{A, \text{rej}}) = \text{Spl.Setup}(\lambda; r_A) \) and \((sk_B, vk_B, vk_{B, \text{rej}}) = \text{Spl.Setup}(\lambda; r_B)\);
4. Let \( \alpha = 'A' \) and \( m^{\text{in}} = (t, \text{root\_index}, w^{\text{in}}_\text{st}, w^{\text{in}}_\text{com}, v^{\text{in}}); \)
5. If \( t \leq i \) then
   6. If \( \text{Spl.Verify}(vk_A, m^{\text{in}}, \sigma^{\text{in}}) = 1 \), set \( \alpha = 'A'; \)
   7. Else, output \text{Reject};
8. else
   9. If \( \text{Spl.Verify}(vk_A, m^{\text{in}}, \sigma^{\text{in}}) = 1 \), set \( \alpha = 'A'; \)
10. If \( \alpha \neq 'A' \) and \( \text{Spl.Verify}(vk_B, m^{\text{in}}, \sigma^{\text{in}}) = 1 \), set \( \alpha = 'B'; \)
11. If \( \alpha = 'B' \), output \text{Reject};
12. If \( \text{Acc.VerifyRead}(\text{pp}_{\text{Acc, st}}, w^{\text{in}}_\text{st}, (id_{cpu}, st^{\text{in}}), \pi^{\text{in}}_\text{st}) = 0 \) output \text{Reject};
13. If \( \text{Acc.VerifyRead}(\text{pp}_{\text{Acc, com}}, w^{\text{in}}_\text{com}, (\text{src}(t, id_{cpu}), \text{com}^{\text{in}}), \pi^{\text{in}}_\text{com}) = 0 \) output \text{Reject};
14. if \( t \leq i \) or \( \alpha = 'B' \) then
15. Compute \((st^{\text{out}}, com^{\text{out}}) \leftarrow F^1(id_{cpu}, st^{\text{in}}, com^{\text{in}}); \)
16. else
17. Compute \((st^{\text{out}}, com^{\text{out}}) \leftarrow F^0(id_{cpu}, st^{\text{in}}, com^{\text{in}}); \)
18. Compute \((v^{\text{out}} = \text{itr.Iterate}(\text{pp}_{\text{tr}}, v^{\text{in}}, (t + 1, id_{cpu}, st^{\text{in}}, \text{com}^{\text{in}}, w^{\text{in}}_\text{st}, w^{\text{in}}_\text{com}); \)
19. if \( st^{\text{out}} = \text{Reject} \) then
20. Output \text{Reject};
21. else
22. Let \( r'_A = \text{PRF}(K_A, (t + 1, id_{cpu})) \) and \( r'_B = \text{PRF}(K_B, (t + 1, A)); \)
23. Compute \((sk'_A, vk'_A, vk'_{A, \text{rej}}) = \text{Spl.Setup}(\lambda; r'_A) \) and \((sk'_B, vk'_B, vk'_{B, \text{rej}}) = \text{Spl.Setup}(\lambda; r'_B)\);
24. Let \( m^{\text{out}} = (t + 1, id_{cpu}, st^{\text{out}}, \text{com}^{\text{out}}, v^{\text{out}}) \)
25. If \( t = i \) and \( m^{\text{in}} = m_i, \text{Root} \), compute \( \sigma^{\text{out}} = \text{Spl.Sign}(sk'_A, m^{\text{out}}); \)
26. Else if \( t = i \) and \( m^{\text{in}} \neq m_i, \text{Root} \), compute \( \sigma^{\text{out}} = \text{Spl.Sign}(sk'_B, m^{\text{out}}); \)
27. Else, compute \( \sigma^{\text{out}} = \text{Spl.Sign}(sk'_\alpha, m^{\text{out}}); \)
28. Let \( \text{node}^{\text{out}} = (t + 1, id_{cpu}, st^{\text{out}}, \text{com}^{\text{out}}, v^{\text{out}}, \sigma^{\text{out}}); \)
29. Output \( \tilde{v}^{\text{out}} = (st^{\text{out}}, id_{cpu}, \perp), \tilde{a}^{\text{out}} = \text{node}^{\text{out}}; \)
Algorithm 53: $P_{\text{combine}}^{0,1,1}$

**Input**: $\tilde{\text{st}}^{\text{in}} = (\text{st}^{\text{in}}, \text{id}_{\text{cpu}}, \perp), \tilde{\alpha}^{\text{in}} = (\text{node}_1, \text{node}_2)$

**Data**: $T, p\text{pAcc}_{\text{std}}, p\text{pAcc}_{\text{com}}, p\text{pItr}, K_A, K_B$

1. Parse $\text{node}_\zeta$ as $(t_\zeta, \text{index}_\zeta, w_{\text{st},\zeta}, w_{\text{com},\zeta}, v_\zeta, \sigma_\zeta)$ for $\zeta = 1,2$;
2. If $t_1 \neq t_2$, output Reject. Else, let $t = t_1$;
3. If $t < 1$, output Reject;
4. If $\text{index}_1$ and $\text{index}_2$ are not siblings, output Reject;
5. Set parent index as the parent of $\text{index}_1$ and $\text{index}_2$;
6. for $\zeta = 1,2$ do
   7. Let $r_{A,\zeta} = \text{PRF}(K_A, (t_\zeta, \text{index}_\zeta))$ and $r_{B,\zeta} = \text{PRF}(K_B, (t_\zeta, \text{index}_\zeta));$
   8. Compute $(sk_{A,\zeta}, vk_{A,\zeta}, vk_{A,\text{rej},\zeta}) = \text{Spl.Setup}(1^\lambda; r_{A,\zeta})$ and
      $(sk_{B,\zeta}, vk_{B,\zeta}, vk_{B,\text{rej},\zeta}) = \text{Spl.Setup}(1^\lambda; r_{B,\zeta});$
   9. Let $\alpha_\zeta = 'A'$ and $m_\zeta = (t_\zeta, \text{index}_\zeta, w_{\text{st},\zeta}, w_{\text{com},\zeta}, v_\zeta, \sigma_\zeta);$
10. if $t \leq i$ then
      11. If Spl.Verify$(vk_{A}, m_\zeta, \sigma_\zeta) = 1$, set $\alpha_\zeta = 'A'$;
      12. Else, output Reject;
      13. else
      14. If Spl.Verify$(vk_{A}, m_\zeta, \sigma_\zeta) = 1$, set $\alpha_\zeta = 'A'$;
      15. If $\alpha_\zeta \neq 'A'$ and Spl.Verify$(vk_{B}, m_\zeta, \sigma_\zeta) = 1$, set $\alpha_\zeta = 'B'$;
      16. If $\alpha_\zeta = 'A'$, output Reject;
17. if $\alpha_1 = 'A'$ and $\alpha_2 = 'A'$, set $\alpha = 'A'$;
18. Else, set $\alpha = 'B'$;
19. Compute $w'_{\text{st}} = \text{Acc.Combine}(p\text{pAcc}_{\text{std}}, w_{\text{st},1}, w_{\text{st},2});$
20. Compute $w'_{\text{com}} = \text{Acc.Combine}(p\text{pAcc}_{\text{com}}, w_{\text{com},1}, w_{\text{com},2});$
21. Compute $v' = \text{Itr.IterateTo1}(p\text{pItr}, (v_1, v_2), (t, \text{parent index}, w_{\text{st},1}, w_{\text{com},1}, w_{\text{st},2}, w_{\text{com},2}));$
22. Let $r'_A = \text{PRF}(K_A, (t, \text{parent index}))$ and $r'_B = \text{PRF}(K_B, (t, \text{parent index}));$
23. Compute $(sk'_A, vk'_A, vk'_{A,\text{rej}}) = \text{Spl.Setup}(1^\lambda; r'_A)$ and $(sk'_B, vk'_B, vk'_{B,\text{rej}}) = \text{Spl.Setup}(1^\lambda; r'_B);$
24. Let $m' = (t, \text{parent index}, w'_A, w'_B, v');$
25. if $t \leq i$ then
   26. Compute $\sigma' = \text{Spl.Sign}(sk'_A, m');$
   27. else
   28. Compute $\sigma' = \text{Spl.Sign}(sk'_A, m');$
29. Let parent node = $(t, \text{parent index}, w'_A, w'_B, v', \sigma')$;
30. if parent index = $\epsilon$ then
   31. Output $\tilde{\text{st}}^{\text{out}} = (\text{st}^{\text{in}}, \text{id}_{\text{cpu}}, \text{parent node}), \tilde{\alpha}^{\text{out}} = \perp$;
   32. else
33. Output $\tilde{\text{st}}^{\text{out}} = (\text{st}^{\text{in}}, \text{id}_{\text{cpu}}, \perp), \tilde{\alpha}^{\text{out}} = \text{parent node};$
**Hyb\textsubscript{0,0,i,j}**. This hybrid similar to **Hyb\textsubscript{0,0,i}** except of the following:

- At time \( t = i \), if \( id\text{cpu} \geq \text{min-cpu}(j) \), \( F^{0,0,i,j}_{\text{branch}} \) follows the type of the incoming signature to generate the type of the outgoing signature

- At time \( t = t+1 \), if \( \text{parent\_index} \geq j \), \( F^{0,0,i,j}_{\text{combine}} \) only accepts ‘A’ type signatures

Finally, from **Hyb\textsubscript{0,0,i,j}** to **Hyb\textsubscript{0,0,i,j+1}**, we can directly apply KKLW proof technique as in the proof of Lemma B.2.

\[\sqrt{2}\]  

**Algorithm 54: \( F^{0,0,i,j}_{\text{branch}} \)**  

\[
\text{Input} : \text{in} = (\text{st}^{\text{in}}, id\text{cpu}, \text{root\_node}), \text{in} = (\text{com}^{\text{in}}, \pi^{\text{in}}, \alpha^{\text{in}})  
\text{Data: pp}_{\text{Acc.st}}, pp_{\text{Acc.com}}, pp_{\text{Itr}}, K_A
\]

1. Parse root\_node as \((t, \text{root\_index}, w^{\text{in}}, u^{\text{in}}, v^{\text{in}}, \sigma^{\text{in}})\);
2. Let \( r_A = \text{PRF}(K_A, (t, \text{root\_index})) \) and \( r_B = \text{PRF}(K_B, (t, \text{root\_index}))\);
3. Compute \((\text{sk}_A, \text{vk}_A, \text{vk}\text{\_A}, \text{vk}\text{\_A}) = \text{Spl\_Setup}(1^\lambda, r_A) \) and \((\text{sk}_B, \text{vk}_B, \text{vk}\text{\_B}, \text{vk}\text{\_B}) = \text{Spl\_Setup}(1^\lambda, r_B)\);
4. Let \( \alpha = \text{"-"} \) and \( m^{\text{in}} = (t, \text{root\_index}, w^{\text{in}}, u^{\text{com}}, v^{\text{in}})\);
5. If \( t \leq i \) then
   - If \( \text{Spl\_Verify}(\text{vk}_A, m^{\text{in}}, \sigma^{\text{in}}) = 1 \), set \( \alpha = \text{‘A’}; \)
   - Else, output \text{Reject};
8. Else
   - If \( \text{Spl\_Verify}(\text{vk}_A, m^{\text{in}}, \sigma^{\text{in}}) = 1 \), set \( \alpha = \text{‘A’}; \)
   - If \( \alpha \neq \text{‘A’} \) and \( \text{Spl\_Verify}(\text{vk}_B, m^{\text{in}}, \sigma^{\text{in}}) = 1 \), set \( \alpha = \text{‘B’}; \)
   - If \( \alpha = \text{‘-’} \), output \text{Reject};
12. If \( \text{Acc\_Verify\_Read}(pp_{\text{Acc.st}}, w^{\text{in}}, (id\text{cpu}, \text{st}^{\text{in}}), \pi^{\text{in}}) = 0 \) output \text{Reject};
13. If \( \text{Acc\_Verify\_Read}(pp_{\text{Acc.com}}, w^{\text{in}}, (\text{src}(t, id\text{cpu}), \text{com}^{\text{in}}), \pi^{\text{in}}) = 0 \) output \text{Reject};
14. If \( \alpha = \text{‘B’} \) then
   - Compute \((\text{st}^{\text{out}}, \text{com}^{\text{out}}) \leftarrow F^1(id\text{cpu}, \text{st}^{\text{in}}, \text{com}^{\text{in}}); \)
   - Else
     - Compute \((\text{st}^{\text{out}}, \text{com}^{\text{out}}) \leftarrow F^0(id\text{cpu}, \text{st}^{\text{in}}, \text{com}^{\text{in}}); \)
18. Compute \( u^{\text{out}} = \text{Itr\_Iterate}(pp_{\text{Itr}}, v^{\text{in}}, (t + 1, id\text{cpu}, \text{st}^{\text{in}}, \text{com}^{\text{in}}, w^{\text{in}}, u^{\text{in}})); \)
19. If \( \text{st}^{\text{out}} = \text{Reject} \) then
   - Output \text{Reject};
21. Else
   - Let \( r'_A = \text{PRF}(K_A, (t + 1, id\text{cpu})) \) and \( r'_B = \text{PRF}(K_B, (t + 1, A)); \)
   - Compute \((\text{sk}'_A, \text{vk}'_A, \text{vk}'\text{\_A}, \text{vk}'\text{\_A}) = \text{Spl\_Setup}(1^\lambda, r'_A) \) and \((\text{sk}'_B, \text{vk}'_B, \text{vk}'\text{\_B}, \text{vk}'\text{\_B}) = \text{Spl\_Setup}(1^\lambda, r'_B)\);
   - Let \( m^{\text{out}} = (t + 1, id\text{cpu}, \text{st}^{\text{out}}, \text{com}^{\text{out}}, u^{\text{out}}); \)
   - If \( t = i \) then
     - If \( id\text{cpu} \geq \text{min-cpu}(j) \), compute \( \sigma^{\text{out}} = \text{Spl\_Sign}(\text{sk}'_A, m^{\text{out}}); \)
     - Else, compute \( \sigma^{\text{out}} = \text{Spl\_Sign}(\text{sk}'_A, m^{\text{out}}); \)
   - Else
     - Compute \( \sigma^{\text{out}} = \text{Spl\_Sign}(\text{sk}'_A, m^{\text{out}}); \)
29. Let \( \text{node}^{\text{out}} = (t + 1, id\text{cpu}, \text{st}^{\text{out}}, \text{com}^{\text{out}}, u^{\text{out}}, \sigma^{\text{out}}); \)
31. Output \( \text{st}^{\text{out}} = (\text{st}^{\text{out}}, id\text{cpu}, \bot), \alpha^{\text{out}} = \text{node}^{\text{out}}; \)
Algorithm 55: $F^{0,0,i,j}_{\text{combine}}$

Input: $\bar{st}^{\text{in}} = (st^{\text{in}}, id_{\text{cpu}}, \bot)$, $\bar{a}^{\text{in}} = (\text{node}_1, \text{node}_2)$

Data: $T$, $pp_{\text{Acc.st}}, pp_{\text{Acc.com}}, pp_{\text{itr}}, K_A$

1. Parse $\text{node}_\zeta$ as $(t_\zeta, \text{index}_\zeta, w_{st,\zeta}, w_{com,\zeta}, \upsilon_\zeta, \sigma_\zeta)$ for $\zeta = 1, 2$;
2. If $t_1 \neq t_2$, output $\text{Reject}$. Else, let $t = t_1$;
3. If $t < 1$, output $\text{Reject};$
4. If $\text{index}_1$ and $\text{index}_2$ are not siblings, output $\text{Reject};$
5. Set $\text{parent\_index}$ as the parent of $\text{index}_1$ and $\text{index}_2$;
6. for $\zeta = 1, 2$ do
7.   Let $r_{A,\zeta} = \text{PRF}(K_A, (t_\zeta, \text{index}_\zeta))$ and $r_{B,\zeta} = \text{PRF}(K_B, (t_\zeta, \text{index}_\zeta))$;
8.   Compute $(sk_{A,\zeta}, \text{vk}_{A,\zeta}, \text{vk}_{A,\text{rej},\zeta}) = \text{Spl.Setup}(1^\lambda; r_{A,\zeta})$ and
9.      $(sk_{B,\zeta}, \text{vk}_{B,\zeta}, \text{vk}_{B,\text{rej},\zeta}) = \text{Spl.Setup}(1^\lambda; r_{B,\zeta});$
10. Let $\alpha_\zeta = \text{‘A’}$ and $m_\zeta = (t_\zeta, \text{index}_\zeta, w_{st,\zeta}, w_{com,\zeta}, \upsilon_\zeta);$
11. if $t \leq i$ or $(t = i + 1$ and $\text{parent\_index} \geq j)$ then
12.   If $\text{Spl.Verify}(\text{vk}_{A,\zeta}, m_\zeta, \sigma_\zeta) = 1$, set $\alpha_\zeta = \text{‘A’}$;
13.      Else, output $\text{Reject};$
14.   else
15.      If $\text{Spl.Verify}(\text{vk}_{A,\zeta}, m_\zeta, \sigma_\zeta) = 1$, set $\alpha_\zeta = \text{‘A’}$;
16.         If $\alpha_1 \neq \text{‘A’}$ and $\text{Spl.Verify}(\text{vk}_{B,\zeta}, m_\zeta, \sigma_\zeta) = 1$, set $\alpha_\zeta = \text{‘B’}$;
17.         If $\alpha_\zeta = \text{‘B’}$, output $\text{Reject};$
18.      if $\alpha_1 = \text{‘A’}$ and $\alpha_2 = \text{‘A’}$, set $\alpha = \text{‘A’}$;
19.      else, set $\alpha = \text{‘B’}$;
20. Compute $\ell'_{st} = \text{Acc.Combine}(pp_{\text{Acc.st}}, w_{st,1}, w_{st,2});$
21. Compute $\ell'_{com} = \text{Acc.Combine}(pp_{\text{Acc.com}}, w_{com,1}, w_{com,2});$
22. Compute $\ell' = \text{itr.iterate2to1}(pp_{\text{itr}}, (v_1, v_2), (t, \text{parent\_index}, w_{st,1}, w_{com,1}, w_{st,2}, w_{com,2}));$
23. Let $r'_A = \text{PRF}(K_A, (t, \text{parent\_index}))$ and $r'_B = \text{PRF}(K_B, (t, \text{parent\_index}));$
24. Compute $(sk'_A, \text{vk}'_A, \text{vk}'_{A,\text{rej}}) = \text{Spl.Setup}(1^\lambda; r'_A)$ and $(sk'_B, \text{vk}'_B, \text{vk}'_{B,\text{rej}}) = \text{Spl.Setup}(1^\lambda; r'_B);$
25. Let $m' = (t, \text{parent\_index}, w'_{st}, w'_{com}, v');$
26. if $t \leq i$ then
27.   Compute $\sigma' = \text{Spl.Sign}(sk'_A, m');$
28. else
29.   Compute $\sigma' = \text{Spl.Sign}(sk'_\alpha, m');$
30. Let $\text{parent\_node} = (t, \text{parent\_index}, w'_st, w'_com, v', \sigma');$
31. if $\text{parent\_index} = \epsilon$ then
32.   Output $\bar{st}^{\text{out}} = (st^{\text{in}}, id_{\text{cpu}}, \text{parent\_node}), \bar{a}^{\text{out}} = \bot;$
33. else
34.   Output $\bar{st}^{\text{out}} = (st^{\text{in}}, id_{\text{cpu}}, \bot), \bar{a}^{\text{out}} = \text{parent\_node};$
B.3.2 From $\text{Hyb}_{0,1,i}$ to $\text{Hyb}_{0,1,i+1}$:

Lemma B.51. Assuming $i\mathcal{O}$ is a secure indistinguishability obfuscator, PRF is a selectively secure puncturable PRF, $\mathcal{Tl}tr$ is an indistinguishability obfuscator satisfying Definitions 7.1 and 7.2, $\text{Acc}$ is an accumulator, $\text{Spl}$ is a secure splittable signature scheme. Then for any PPT adversary $A$, $|\operatorname{Adv}_{A}^{0,1,i} - \operatorname{Adv}_{A}^{0,1,i+1}| \leq \operatorname{negl}(\lambda)$.

Proof. To argue $|\operatorname{Adv}_{A}^{0,1,i} - \operatorname{Adv}_{A}^{0,1,i+1}| \leq \operatorname{negl}(\lambda)$, we define a sequence of fourth-layer hybrids $\text{Hyb}_{0,1,i,j}$ where $j$ indexed by the node index via post-order, and (type) specifies the type of node $j$.

Concretely, we define the fourth-layer hybrids $\text{Hyb}_{0,1,i,j}^{0,1,i,j}$, $\text{Hyb}_{0,1,i,j}^{0,1,i,j}$, $\text{Hyb}_{0,1,i,j}^{0,1,i,j}$, and $\text{Hyb}_{0,1,i,j}^{0,1,i,j}$. See Figure 3 as an example.

Figure 3: The sequence of hybrids with 4 CPUs. Each node is a computation step, which also has a corresponding hybrid on it. Each arrow is the input/output to be hardwired by some hybrids. Hybrids are proceeded by: $\text{Hyb}_{0,1,i,j}^{0,1,i,j}$, $\text{Hyb}_{0,1,i,j}^{0,1,i,j}$, $\text{Hyb}_{0,1,i,j}^{0,1,i,j}$, $\text{Hyb}_{0,1,i,j}^{0,1,i,j}$. As an example, $\text{Hyb}_{0,1,i,j}^{0,1,i,j}$ is circled in thick blue line ($0, 1, i, 10$), and its hardwired information are shown in thick blue arrows.

$\text{Hyb}_{0,1,i,j}^{0,1,i,j}$: $j$ is a left leaf node. In this hybrid, the challenger outputs an obfuscation of $\hat{F}^{0,1,i,j} = F_{\text{branch}}^{0,1,i,j} + F_{\text{combine}}^{0,1,i,j}$ defined in Algorithms 56 and 57. $\hat{F}^{0,1,i,j}$ is similar to $\hat{F}^{0,1,i,j}$ except the following differences.

- At $t = i$, $F_{\text{branch}}^{0,1,i,j}$ has the correct input message $m_{i,\text{root.index}}$ and an agent $j$'s output message $m_{i,j}$ hardwired.
- At $t = i$, if $m_{i} = m_{i,j}$ and $A > j$, $F_{\text{branch}}^{0,1,i,j}$ outputs an ‘A’ type signature.
- If $m_{i} \neq m_{i,j}$ and $A > j$, outputs a ‘B’ type signature.
- If $m_{i} = m_{i,j}$ and $A = j$, outputs an ‘A’ type signature.
- If $m_{i} = m_{i,j}$ and $A = j$, outputs a ‘B’ type signature.
- $F_{\text{combine}}^{0,1,i,j}$ hardwires a set of indices $C_{i,j}$ and the corresponding set of output message $M_{i,j}$.
- $F_{\text{combine}}^{0,1,i,j}$ accepts ‘B’ type signatures only for inputs if $i + 2 \leq t \leq t^* - 1$ or (parent_index $> j$ and $t = i + 1$).
- For parent_index $\in C_{i,j}$ at time $t = i + 1$, $F_{\text{combine}}^{0,1,i,j}$ checks whether $m' = m_{\text{parent.index}} = M_{i,j}$ or not. If $m' = m_{\text{parent.index}}$, outputs an ‘A’ type signature; otherwise, outputs ‘B’ type.
\( \textbf{Hyb}_{0,1,i,j}^{\text{right-leaf}}: \) \( j \) is a right leaf node. In this hybrid, the challenger outputs an obfuscation of \( \hat{F}_{0,1,i,j}^{\text{right-leaf}} = F_{\text{branch}}^{0,1,i,j} \oplus F_{\text{combine}}^{0,1,i,j} \) where \( F_{\text{branch}}^{0,1,i,j} \) is defined in Algorithm 58. In particular, \( F_{\text{combine}}^{0,1,i,j} \) is functionally identical to \( F_{\text{combine}}^{0,1,i,j-1} \) since hardwired \((C_{i,j}, M_{i,j})\) in \( F_{\text{combine}}^{0,1,i,j} \) is identical to the hardwired \((C_{i,j-1}, M_{i,j-1})\) in \( F_{\text{combine}}^{0,1,i,j-1} \). \( \hat{F}_{0,1,i,j}^{\text{right-leaf}} \) is similar to \( F_{0,1,i,j}^{\text{right-leaf}} \) except the following differences.

- At \( t = i \), \( F_{\text{branch}}^{0,1,i,j} \) has the correct input message \( m_{i,\text{root}} \) and agents \( j-1 \) and \( j \)'s output message \( m_{i,j-1} \) and \( m_{i,j} \) hardwired.
- At \( t = i \), if \( m_{\text{in}}^{i} = m_{i,\text{root}} \) and \( A > j \), \( F_{\text{branch}}^{0,1,i,j} \) outputs an ‘A’ type signature.
  
  If \( m_{\text{in}}^{i} \neq m_{i,\text{root}} \) and \( A > j \), outputs a ‘B’ type signature.
  
  If \( m_{\text{out}} = m_{i,j} \) and \( A = j \), outputs an ‘A’ type signature.
  
  If \( m_{\text{out}} \neq m_{i,j} \) and \( A = j \), outputs a ‘B’ type signature.
  
  If \( m_{\text{out}} = m_{i,j-1} \) and \( A = j-1 \), outputs an ‘A’ type signature.
  
  If \( m_{\text{out}} \neq m_{i,j-1} \) and \( A = j-1 \), outputs a ‘B’ type signature.

\( \textbf{Hyb}_{0,1,i,j}^{\text{internal}}: \) \( j \) is an internal node. In this hybrid, the challenger outputs an obfuscation of \( \hat{F}_{0,1,i,j}^{\text{internal}} = F_{\text{branch}}^{0,1,i,j} \oplus F_{\text{combine}}^{0,1,i,j} \) defined in Algorithms 59 and 60. \( \hat{F}_{0,1,i,j}^{\text{internal}} \) is similar to \( \hat{F}_{0,1,i,j} \) except the following differences.

- At \( t = i \), if \( m_{\text{in}}^{i} = m_{i,\text{root}} \) and \( A > \max\text{-cpu}(j) \), \( F_{\text{branch}}^{0,1,i,j} \) outputs an ‘A’ type signature.
  
  If \( m_{\text{in}}^{i} \neq m_{i,\text{root}} \) and \( A > \max\text{-cpu}(j) \), outputs a ‘B’ type signature.
  
  \( F_{\text{combine}}^{0,1,i,j} \) hardwires an output message \( m_{i,j} \), a set of indices \( C_{i,j} \) and the corresponding set of output message \( M_{i,j} \).
  
  \( F_{\text{combine}}^{0,1,i,j} \) accepts ‘B’ type signatures only for inputs if \( i + 2 \leq t \leq t^{*} - 1 \) or \( \text{parent}_{\text{index}} > j \) and \( t = i + 1 \).
  
  For \( \text{parent}_{\text{index}} \in C_{i,j} \) at time \( t = i + 1 \), \( F_{\text{combine}}^{0,1,i,j} \) checks whether \( m' = m_{\text{parent}_{\text{index}}} \in M_{i,j} \) or not. If \( m' \neq m_{\text{parent}_{\text{index}}} \), outputs an ‘A’ type signature; otherwise, outputs ‘B’ type.
  
  For \( \text{parent}_{\text{index}} = j \) at time \( t = i + 1 \), \( F_{\text{combine}}^{0,1,i,j} \) checks whether \( m' = m_{i,j} \) or not. If \( m' = m_{i,j} \), outputs an ‘A’ type signature; otherwise, outputs ‘B’ type.

\( \textbf{Hyb}_{0,1,i,j}^{\text{intermediate}}: \) \( j \) is an internal node. In this hybrid, the challenger outputs an obfuscation of \( \hat{F}_{0,1,i,j}^{\text{intermediate}} = F_{\text{branch}}^{0,1,i,j} \oplus F_{\text{combine}}^{0,1,i,j} \). \( F_{\text{branch}}^{0,1,i,j} \) is functionally identical to \( F_{\text{branch}}^{0,1,i,j} \), and \( F_{\text{combine}}^{2,i,j} \) is defined in Algorithm 61. This hybrid is similar to \( \textbf{Hyb}_{0,1,i,j}^{\text{internal}} \) except that

- \( F_{\text{combine}}^{0,1,i,j} \) hardwires two input messages \( (m_{i,j-1}, m_{i,j}) \).
- For \( \text{parent}_{\text{index}} = j \) at time \( t = i + 1 \), \( F_{\text{combine}}^{0,1,i,j} \) outputs ‘A’ type signature if \( m_{1} = m_{i,j-1} \) and \( m_{2} = m_{i,j} \), or outputs ‘B’ type if not.

Conclusively, we define \( \textbf{Hyb}_{0,1,i,\text{root}}^{\text{index}}: \) in \( \hat{F}_{0,1,i,\text{root}}^{\text{index}} \), \( F_{\text{branch}}^{0,1,i,\text{root}} \) is similar to \( F_{\text{branch}}^{0,1,i+1} \) except for no hardwired information, and \( F_{\text{combine}}^{0,1,i,\text{root}} \) is identical to \( F_{\text{combine}}^{0,1,i,\text{root}} \). Note that \( \hat{F}_{0,1,i,\text{root}}^{\text{index}} \) and \( \hat{F}_{0,1,i,\text{root}}^{\text{index}} \) are functionally equivalent, which implies \( \textbf{Hyb}_{0,1,i,\text{root}}^{\text{index}} \approx \textbf{Hyb}_{0,1,i,\text{root}}^{\text{index}} \). Then, we conclude \( \textbf{Hyb}_{0,1,i,\text{root}}^{\text{index}} \approx \textbf{Hyb}_{0,1,i+1} \) by KLW proof technique. In general, we can directly apply it as in the proof of Lemma B.9 to prove the argument from any case \( \textbf{Hyb}_{0,1,i,j} \) to \( \textbf{Hyb}_{0,1,i,j+1} \) (with/without \( \textbf{Hyb}_{0,1,i,j+1} \)).
Instantiation. Consider the following sequence of hybrids which corresponds to $\text{Hyb}_{0,1,i,i,10}$, $\text{Hyb}_{0,1,i,11}$, $\text{Hyb}_{0,1,i,i,1}$, and $\text{Hyb}_{0,1,i,i,\epsilon}$ in Figure 3.

$$\text{Hyb}_{0,1,i,j}\text{(left-leaf)} \approx \text{Hyb}_{0,1,i,j+1}\text{(right-leaf)} \approx \text{Hyb}_{0,1,i,j+2}\text{(internal)} \approx \text{Hyb}_{0,1,i,j+3}\text{(internal)}$$

To prove the indistinguishability of the hybrids in the above sequence, we further claim the sequences below:

- $\text{Hyb}_{0,1,i,j}\text{(left-leaf)} \approx \text{Hyb}_{0,1,i,j+1}\text{(right-leaf)}$
- $\text{Hyb}_{0,1,i,j+1}\text{(right-leaf)} \approx \text{Hyb}_{0,1,i,j+2}\text{(intermediate)} \approx \text{Hyb}_{0,1,i,j+3}\text{(internal)}$
- $\text{Hyb}_{0,1,i,j+2}\text{(internal)} \approx \text{Hyb}_{0,1,i,j+3}\text{(internal)} \approx \text{Hyb}_{0,1,i,j+3}\text{(internal)}$

The indistinguishability of the hybrids in each of the above sequence can be proven by the K LW proof techniques as in the proof of Lemma B.9. Note that we only need to hardware $O(\log m)$ messages in $\text{Hyb}_{0,1,i,j}$ according to the above argument.

B.4 Proof Sketch of Theorem 7.8 (Security for CiO-PRAM)

Compared to the CiO construction in the memory-less PRAM model, there are two major differences in the construction in the standard PRAM model. Firstly, we need to verify memory inputs, which can be a value that read from memory, or a proof of the path to the writing location, against the memory accumulator. Secondly, we need to compute the memory accumulator (digest) by running oblivious algorithm $\text{OUpdate}$ several rounds. Both differences have a similar hybridizing strategy described in previous sections, and we introduce a series of hybrids by the computation time, which is the same with that of RAM.

Hybrids to replace $F^0$ with $F^1$ are applied iteratively as follows.

Verification of Memory Input. To illustrate these hybrids, let time $i$ be a read round for both $F^0$ and $F^1$, where both program takes no input from memory and outputs a read command. Let $\widehat{F}^i$ be a hybrid program that runs $F^1$ if $t < i$ with the memory digest value $w_{\text{mem}}^{i-1}$ hardwired. Because there is no memory input, those hybrids from program $\widehat{F}^i$ to $\widehat{F}^{i+1}$ is identical to the combine tree described in Section B.3.2, which replaces from $F^0$ to $F^1$ at $t = i$.

Because time $i$ is a read step and does not change memory digest value, $\widehat{F}^{i+1}$ also hardwires $w_{\text{mem}}^{i-1}$. The next round $i + 1$ must be a write round which has an input read from memory and outputs a write command. At time $i + 1$, $\widehat{F}^{i+1}$ verifies memory inputs just as that of RAM programs, so that security proof is directly identical to that of the RAM program (Section B.1) except we need series of hybrids for each CPU agent $\pi \in [m]$. Given the fact that the digest value is correct at time $i + 1$, the hybrids are to setup read enforcement for the memory input at time $i + 1$ and to argue that read value is information-theoretically correct if it is verified by accumulator. At this step, we can safely replace the PRAM program from $F^0$ to $F^1$ by security of iO, and then we have the next hybrid program $\widehat{F}^{i+1}\text{OUpdate}$ by the combine tree described in Section B.3.2.

We continue with those hybrids of OUpdate.

Hardwiring the Next Accumulator Digest. Let us consider the second difference after time $i + 1$. It is necessary to show the digest computed by OUpdate are correct, and we need to show the result of OUpdate can be replaced by a hardwired correct memory digest $w_{\text{mem}}^{i+1}$ at the next hybrid program $\widehat{F}^{i+2}$.

Firstly, an observation is that OUpdate is exactly carried through an oblivious and memory-less PRAM computation, where each CPU agent has old digest $w_{\text{mem}}^{i-1}$, write location loc$_A$, old proof $\pi_A$ to the location, and a bit $b_A$ to write. Therefore, we can apply those hybrids in Section 7.5 and replace OUpdate with OUpdate$^{i+1}$ that always output the correct new memory digest $w_{\text{mem}}^{i+1}$ at time $i + 1$. In particular, we design
Algorithm 56: $I_{F_{0,1,1,j}}$(left-leaf)

**Input**: $st^{in} = (st^{in}, id_{cpu}, root\_node), \tilde{a}^{in} = (com^{in}, n_{st}^{in}, n_{com}^{in})$

**Data**: $pp_{Acc, st}, pp_{Acc, com}, pp_{Itr}, K_{A}, K_{B}, m_i, Root, m_{i, j}$

1. Parse root\_node as $(t, root\_index, w_{st}^{in}, w_{com}^{in}, v^{in}, \sigma^{in})$;
2. Let $r_A = PRF(K_A, (t, root\_index))$ and $r_B = PRF(K_B, (t, root\_index))$;
3. Compute $(sk_A, vk_A, vk_{A, rej}) = Spl.Setup(1^\lambda; r_A)$ and $(sk_B, vk_B, vk_{B, rej}) = Spl.Setup(1^\lambda; r_B)$;
4. Let $\alpha = \cdot$ and $m^{in} = (t, root\_index, w_{st}^{in}, w_{com}^{in}, v^{in})$;
5. if $t \leq i$ then
6. \hspace{1em} If $Spl.\text{Verify}(vk_A, m^{in}, \sigma^{in}) = 1$, set $\alpha = \cdot A$;
7. \hspace{1em} Else, output Reject;
8. else
9. \hspace{1em} if $Spl.\text{Verify}(vk_A, m^{in}, \sigma^{in}) = 1$, set $\alpha = \cdot A$;
10. \hspace{1em} if $\alpha \neq \cdot A$ and $Spl.\text{Verify}(vk_B, m^{in}, \sigma^{in}) = 1$, set $\alpha = \cdot B$;
11. \hspace{1em} if $\alpha = \cdot$, output Reject;
12. if $Acc.\text{VerifyRead}(pp_{Acc, st}, w_{st}^{in}, (id_{cpu}, st^{in}), \pi_{st}^{in}) = 0$ output Reject;
13. if $Acc.\text{VerifyRead}(pp_{Acc, com}, w_{com}^{in}, (src(t, id_{cpu}), com^{in}), \pi_{com}^{in}) = 0$ output Reject;
14. if $t \leq i$ or $\alpha = \cdot B$ then
15. \hspace{1em} Compute $(st^{out}, com^{out}) \leftarrow F^1(id_{cpu}, st^{in}, com^{in})$;
16. else
17. \hspace{1em} Compute $(st^{out}, com^{out}) \leftarrow F^0(id_{cpu}, st^{in}, com^{in})$;
18. Compute $v^{out} = \text{itr.\text{Iterate}}(pp_{Itr}, v^{in}, (t + 1, id_{cpu}, st^{in}, com^{in}, w_{st}^{in}, w_{com}^{in}))$;
19. if $st^{out} = \text{Reject}$ then
20. \hspace{1em} Output Reject;
21. else
22. \hspace{1em} Let $r'_{A} = PRF(K_{A}, (t + 1, id_{cpu}))$ and $r'_{B} = PRF(K_{B}, (t + 1, A))$;
23. Compute $(sk'_{A}, vk'_{A}, vk'_{A, rej}) = Spl.Setup(1^\lambda; r'_{A})$ and $(sk'_{B}, vk'_{B}, vk'_{B, rej}) = Spl.Setup(1^\lambda; r'_{B})$;
24. Let $m^{out} = (t + 1, id_{cpu}, st^{out}, com^{out}, v^{out})$;
25. if $t = i$ then
26. \hspace{1em} if $id_{cpu} > j$ and $m^{in} = m_{i, Root} - \sigma^{out} = Spl.\text{Sign}(sk'_{A}, m^{out})$;
27. \hspace{1em} else if $id_{cpu} > j$ and $m^{in} \neq m_{i, Root} - \sigma^{out} = Spl.\text{Sign}(sk'_{B}, m^{out})$;
28. \hspace{1em} else if $id_{cpu} = j$ and $m^{out} = m_{i, j} - \sigma^{out} = Spl.\text{Sign}(sk'_{A}, m^{out})$;
29. \hspace{1em} else if $id_{cpu} = j$ and $m^{out} \neq m_{i, j} - \sigma^{out} = Spl.\text{Sign}(sk'_{B}, m^{out})$;
30. \hspace{1em} else, $\sigma^{out} = Spl.\text{Sign}(sk'_{A}, m^{out})$;
31. else
32. \hspace{1em} Compute $\sigma^{out} = Spl.\text{Sign}(sk'_{A}, m^{out})$
33. Let $node^{out} = (t + 1, id_{cpu}, st^{out}, com^{out}, v^{out}, \sigma^{out})$;
34. Output $st^{out} = (st^{out}, id_{cpu}, \bot), \tilde{a}^{out} = node^{out}$.
Algorithm 57: $I_{0,1,i,j}$(left-leaf)

\begin{align*}
\textbf{Input} & : s_t^{in} = (s_t^{in}, id_{cpu}, \bot), \tilde{s}_t^{in} = (node_1, node_2) \\
\textbf{Data} & : T, pp_{Acc, st}, pp_{Acc, com}, pp_{itr}, K_A, K_B, (C_{i,j}, M_{i,j}) \\
1 & \text{Parse node}_\zeta \text{ as } (t_\zeta, \text{index}_\zeta, w_{st, \zeta}, w_{com, \zeta}, v_\zeta, \sigma_\zeta) \text{ for } \zeta = 1, 2; \\
2 & \text{If } t_1 \neq t_2, \text{ output } \text{Reject}. \text{ Else, let } t = t_1; \\
3 & \text{If } t < 1, \text{ output } \text{Reject}; \\
4 & \text{If index}_1 \text{ and index}_2 \text{ are not siblings, output } \text{Reject}; \\
5 & \text{Set parent_index as the parent of index}_1 \text{ and index}_2; \\
6 & \text{for } \zeta = 1, 2 \text{ do} \\
7 & \text{ Let } r_{A, \zeta} = \text{PRF}(K_A, (t_\zeta, \text{index}_\zeta)) \text{ and } r_{B, \zeta} = \text{PRF}(K_B, (t_\zeta, \text{index}_\zeta)); \\
8 & \text{ Compute } (sk_{A, \zeta}, v_{A, \zeta}, v_{B, \zeta}) = \text{Spl.Setup}(1^\lambda; r_{A, \zeta}) \text{ and } \text{compute } (sk_{B, \zeta}, v_{B, \zeta}, v_{B, \zeta}) = \text{Spl.Setup}(1^\lambda; r_{B, \zeta}); \\
9 & \text{ Let } \alpha_\zeta = ‘\cdot’ \text{ and } m_\zeta = (t_\zeta, \text{index}_\zeta, w_{st, \zeta}, w_{com, \zeta}, v_\zeta); \\
10 & \text{ if } t \leq i \text{ or } (t = i + 1 \text{ and parent_index} \leq j) \text{ then} \\
11 & \text{ If Spl.Verify}(v_{A, \zeta}, m_\zeta, \sigma_\zeta) = 1, \text{ set } \alpha_\zeta = ‘A’; \\
12 & \text{ Else, output } \text{Reject}; \\
13 & \text{ else} \\
14 & \text{ If Spl.Verify}(v_{A, \zeta}, m_\zeta, \sigma_\zeta) = 1, \text{ set } \alpha_\zeta = ‘A’; \\
15 & \text{ If } \alpha_\zeta \neq ‘A’ \text{ and Spl.Verify}(v_{B, \zeta}, m_\zeta, \sigma_\zeta) = 1, \text{ set } \alpha_\zeta = ‘B’; \\
16 & \text{ If } \alpha_\zeta = ‘\cdot’, \text{ output } \text{Reject}; \\
17 & \text{ If } \alpha_1 = ‘A’ \text{ and } \alpha_2 = ‘A’, \text{ set } \alpha = ‘A’; \\
18 & \text{ Else, set } \alpha = ‘B’; \\
19 & \text{ Compute } u_{st}’ = \text{Acc.Combine}(pp_{Acc, st}, w_{st, 1}, w_{st, 2}); \\
20 & \text{ Compute } u_{com}’ = \text{Acc.Combine}(pp_{Acc, com}, w_{com, 1}, w_{com, 2}); \\
21 & \text{ Compute } v’ = \text{itr.iterate2to1}(pp_{itr}, (v_1, v_2), (t, \text{parent_index}, w_{st, 1}, w_{com, 1}, w_{st, 2}, w_{com, 2})); \\
22 & \text{ Let } r_A’ = \text{PRF}(K_A, (t, \text{parent_index})) \text{ and } r_B’ = \text{PRF}(K_B, (t, \text{parent_index})); \\
23 & \text{ Compute } (sk_A’, v_A’, v_{A, \zeta}) = \text{Spl.Setup}(1^\lambda; r_A’) \text{ and } (sk_B’, v_B’, v_{B, \zeta}) = \text{Spl.Setup}(1^\lambda; r_B’); \\
24 & \text{ Let } m’ = (t, \text{parent_index}, u_{st}, u_{com}, v’); \\
25 & \text{ if } t \leq i \text{ then} \\
26 & \text{ Compute } \sigma’ = \text{Spl.Sign}(sk_A’, m’); \\
27 & \text{ if } t = i + 1 \text{ then} \\
28 & \text{ If parent_index} = \text{index’} \text{ and } m’ = m_{\text{index’}} \text{ for index’} \in C_{i,j} \\
29 & \text{ and } m_{\text{index’}} \in M_{i,j}, \text{ compute } \sigma’ = \text{Spl.Sign}(sk_A’, m’); \\
30 & \text{ Else if parent_index} = \text{index’} \text{ and } m’ \neq m_{\text{index’}} \text{ for index’} \in C_{i,j} \\
31 & \text{ and } m_{\text{index’}} \in M_{i,j}, \text{ compute } \sigma’ = \text{Spl.Sign}(sk_B’, m’); \\
32 & \text{ Else, compute } \sigma’ = \text{Spl.Sign}(sk_A’, m’); \\
33 & \text{ else} \\
34 & \text{ Compute } \sigma’ = \text{Spl.Sign}(sk_A’, m’); \\
35 & \text{ Let parent_node} = (t, \text{parent_index}, u_{st}’, u_{com}’, v’, \sigma’); \\
36 & \text{ if parent_index} = \epsilon \text{ then} \\
37 & \text{ Output } s’ = (s_t^{in}, id_{cpu}, \text{parent_node}); \\
38 & \text{ else} \\
39 & \text{ Output } s’ = (s_t^{in}, id_{cpu}, \bot), \tilde{s}_t^{out} = \text{parent_node}; \\
\end{align*}
Algorithm 58: $F^{0,1,i,j}$ (right-leaf)

Input: $\tilde{w}^{in} = (st^{in}, id_{cpu}, root_{node}), \tilde{a}^{in} = (com^{in}, \pi^{in}, \tau^{in})$

Data: $pp_{Acc, st}, pp_{Acc, com}, pp_{ltt}, K_A, K_B, m_i, \text{Root}, m_i, j - 1, m_i, j$

1. Parse root_{node} as $(t, \text{root}_{index}, w^{st}_{in}, w^{com}_{in}, v^{in}, \sigma^{in})$;
2. Let $r_A = \text{PRF}(K_A, (t, \text{root}_{index}))$ and $r_B = \text{PRF}(K_B, (t, \text{root}_{index}))$;
3. Compute $(sk_A, vk_A, vk_{A, rej}) = \text{Spl.Setup}(1^\lambda; r_A)$ and $(sk_B, vk_B, vk_{B, rej}) = \text{Spl.Setup}(1^\lambda; r_B)$;
4. Let $\alpha = 'I'$ and $m^{in} = (t, \text{root}_{index}, w^{st}_{in}, w^{com}_{in}, v^{in})$;
5. if $t \leq i$ then
   6. if $\text{Spl.Verify}(vk_A, m^{in}, \sigma^{in}) = 1$, set $\alpha = 'A'$;
      7. Else, output Reject;
   8. else
      9. if $\text{Spl.Verify}(vk_A, m^{in}, \sigma^{in}) = 1$, set $\alpha = 'A'$;
         10. if $\alpha \neq 'A'$ and $\text{Spl.Verify}(vk_B, m^{in}, \sigma^{in}) = 1$, set $\alpha = 'B'$;
         11. if $\alpha = 'I'$, output Reject;
12. if Acc.VerifyRead$(pp_{Acc, st}, w^{st}_{in}, (id_{cpu}, st^{in}), \pi^{st}_{in}) = 0$, output Reject;
13. if Acc.VerifyRead$(pp_{Acc, com}, w^{com}_{in}, (src(t, id_{cpu}), com^{in}), \pi^{com}_{in}) = 0$, output Reject;
14. if $t < i$ or $\alpha = 'B'$ then
   15. Compute $(st^{out}, com^{out}) \leftarrow F^1(id_{cpu}, st^{in}, com^{in})$;
16. else
   17. Compute $(st^{out}, com^{out}) \leftarrow F^0(id_{cpu}, st^{in}, com^{in})$;
18. Compute $v^{out} = \text{ltt}.\text{Iterate}(pp_{ltt}, v^{in}, (t + 1, id_{cpu}, st^{in}, com^{in}, w^{st}_{in}, w^{com}_{in}))$;
19. if $st^{out} = \text{Reject}$ then
   20. Output Reject;
21. else
   22. Let $r'_A = \text{PRF}(K_A, (t + 1, id_{cpu}))$ and $r'_B = \text{PRF}(K_B, (t + 1, A))$;
   23. Compute $(sk'_A, vk'_A, vk'_{A, rej}) = \text{Spl.Setup}(1^\lambda; r'_A)$ and $(sk'_B, vk'_B, vk'_{B, rej}) = \text{Spl.Setup}(1^\lambda; r'_B)$;
   24. Let $m^{out} = (t + 1, id_{cpu}, st^{out}, com^{out}, v^{out})$;
25. if $t \leq i$ then
   26. if $id_{cpu} > j$ and $m^{in} = m_i, \text{Root}$, $\sigma^{out} = \text{Spl.Sign}(sk'_A, m^{out})$;
         27. else if $id_{cpu} > j$ and $m^{in} \neq m_i, \text{Root}$, $\sigma^{out} = \text{Spl.Sign}(sk'_B, m^{out})$;
         28. else if $id_{cpu} = j - 1$ and $m^{out} = m_i, j - 1$, $\sigma^{out} = \text{Spl.Sign}(sk'_A, m^{out})$;
         29. else if $id_{cpu} = j - 1$ and $m^{out} \neq m_i, j - 1$, $\sigma^{out} = \text{Spl.Sign}(sk'_B, m^{out})$;
         30. else if $id_{cpu} = j$ and $m^{out} = m_i, j$, $\sigma^{out} = \text{Spl.Sign}(sk'_A, m^{out})$;
         31. else if $id_{cpu} = j$ and $m^{out} \neq m_i, j$, $\sigma^{out} = \text{Spl.Sign}(sk'_B, m^{out})$;
         32. else, $\sigma^{out} = \text{Spl.Sign}(sk'_A, m^{out})$;
   33. else
         34. Compute $\sigma^{out} = \text{Spl.Sign}(sk'_A, m^{out})$
   35. Let $node^{out} = (t + 1, id_{cpu}, st^{out}, com^{out}, v^{out}, \sigma^{out})$;
   36. Output $\tilde{w}^{out} = (st^{out}, id_{cpu}, \bot), \tilde{a}^{out} = node^{out}$.
Algorithm 59: $I_{\text{branch}}^{0,1,i,j}$ (internal)

**Input**: st$_{\text{in}}$ = (st$_{\text{in}}$, id$_{\text{cpu}}$, root$_{\text{node}}$), a$_{\text{in}}$ = (com$_{\text{in}}$, in$_{\text{st}}$, com$_{\text{in}}$)

**Data**: pp$_{\text{Acc.st}}$, pp$_{\text{Acc.com}}$, pp$_{\text{itr}}$, $K_A$, $K_B$, $m_i$, Root

1. Parse root$_{\text{node}}$ as (t, root$_{\text{index}}$, w$_{\text{st}}$, w$_{\text{com}}$, v$_{\text{in}}$, $\sigma_{\text{in}}$);
2. Let $r_A$ = PRF($K_A$, (t, root$_{\text{index}}$)) and $r_B$ = PRF($K_B$, (t, root$_{\text{index}}$));
3. Compute (sk$_A$, vk$_A$, vk$_{A,\text{rej}}$) = Spl.Setup($1^\lambda$; $r_A$) and (sk$_B$, vk$_B$, vk$_{B,\text{rej}}$) = Spl.Setup($1^\lambda$; $r_B$);
4. Let $\alpha = \text{?}$ and $m_{\text{in}}$ = (t, root$_{\text{index}}$, w$_{\text{st}}$, w$_{\text{com}}$, v$_{\text{in}}$);
5. if $t \leq i$ then
   6. if Spl.Verify(vk$_A$, m$_{\text{in}}$, $\sigma_{\text{in}}$) = 1, set $\alpha = \text{A}$;
   7. else, output Reject;
8. else
   9. if Spl.Verify(vk$_A$, m$_{\text{in}}$, $\sigma_{\text{in}}$) = 1, set $\alpha = \text{A}$;
10. if $\alpha \neq \text{A}$ and Spl.Verify(vk$_B$, m$_{\text{in}}$, $\sigma_{\text{in}}$) = 1, set $\alpha = \text{B}$;
11. if $\alpha = \text{?}$, output Reject;
12. if Acc.VerifyRead(pp$_{\text{Acc.st}}$, w$_{\text{st}}$, (id$_{\text{cpu}}$, st$_{\text{in}}$), in$_{\text{st}}$) = 0 output Reject;
13. if Acc.VerifyRead(pp$_{\text{Acc.com}}$, w$_{\text{com}}$, (src(t, id$_{\text{cpu}}$), com$_{\text{in}}$), in$_{\text{com}}$) = 0 output Reject;
14. if $t \leq i$ or $\alpha = \text{B}$ then
   15. Compute $(\text{st}_{\text{out}}, \text{com}_{\text{out}})$ ← $F^1$(id$_{\text{cpu}}$, st$_{\text{in}}$, com$_{\text{in}}$);
16. else
   17. Compute $(\text{st}_{\text{out}}, \text{com}_{\text{out}})$ ← $F^0$(id$_{\text{cpu}}$, st$_{\text{in}}$, com$_{\text{in}}$);
18. Compute $v_{\text{out}}$ = ltr.iterate(pp$_{\text{itr}}$, v$_{\text{in}}$, (t + 1, id$_{\text{cpu}}$, st$_{\text{in}}$, com$_{\text{in}}$, w$_{\text{st}}$, w$_{\text{com}}$));
19. if st$_{\text{out}}$ = Reject then
20. Output Reject;
21. else
22. Let $r_A'$ = PRF($K_A$, (t + 1, id$_{\text{cpu}}$)) and $r_B'$ = PRF($K_B$, (t + 1, A));
23. Compute (sk$_A'$, vk$_A'$, vk$_{A,\text{rej}}'$) = Spl.Setup($1^\lambda$; $r_A'$) and (sk$_B'$, vk$_B'$, vk$_{B,\text{rej}}'$) = Spl.Setup($1^\lambda$; $r_B'$);
24. Let $m_{\text{out}}$ = (t + 1, id$_{\text{cpu}}$, st$_{\text{out}}$, com$_{\text{out}}$, v$_{\text{out}}$);
25. if $t = i$ then
   26. if id$_{\text{cpu}}$ > max-cpu(j) and $m_{\text{in}}$ = $m_i$, Root, $\sigma_{\text{out}}$ = Spl.Sign(sk$_A'$, m$_{\text{out}}$);
   27. else if id$_{\text{cpu}}$ > max-cpu(j) and $m_{\text{in}}$ = $m_i$, Root, $\sigma_{\text{out}}$ = Spl.Sign(sk$_B'$, m$_{\text{out}}$);
   28. else, $\sigma_{\text{out}}$ = Spl.Sign(sk$_A'$, m$_{\text{out}}$);
29. else
   30. Compute $\sigma_{\text{out}}$ = Spl.Sign(sk$_A'$, m$_{\text{out}}$);
31. Let node$_{\text{out}}$ = (t + 1, id$_{\text{cpu}}$, st$_{\text{out}}$, com$_{\text{out}}$, v$_{\text{out}}$, $\sigma_{\text{out}}$);
32. Output $\text{st}_{\text{out}}$ = $(\text{st}_{\text{out}}$, id$_{\text{cpu}}$, ⊥), $\alpha_{\text{out}}$ = node$_{\text{out}}$.  

132
Algorithm 60: $E_{\text{combine}}^{0,1,i,j(\text{internal})}$

Input: $\mathbf{st}^{\text{in}} = (\mathbf{st}^{\text{in}}, id_{\text{cpu}}, \bot), \mathbf{an}^{\text{in}} = (\text{node}_1, \text{node}_2)$

Data: $T, pp_{\text{Acc.st}}, pp_{\text{Acc.com}}, pp_{\text{itr}}, K_A, K_B, m_{i,j}$

1. Parse node as $(t_\zeta, \text{index}_\zeta, w_{\text{st},\zeta}, w_{\text{com},\zeta}, v_\zeta, \sigma_\zeta)$ for $\zeta = 1, 2$;
2. If $t_1 \neq t_2$, output Reject. Else, let $t = t_1$;
3. If $t < 1$, output Reject;
4. If index$_1$ and index$_2$ are not siblings, output Reject;
5. Set parent index as the parent of index$_1$ and index$_2$;
6. For $\zeta = 1, 2$ do
7.   Let $r_{A,\zeta} = \text{PRF}(K_A, (t_\zeta, \text{index}_\zeta))$ and $r_{B,\zeta} = \text{PRF}(K_B, (t_\zeta, \text{index}_\zeta))$;
8.   Compute $(sk_{A,\zeta}, vk_{A,\zeta}, vk_{A,\text{rej},\zeta}) = \text{Spl.Setup}(1^\lambda; r_{A,\zeta})$ and $(sk_{B,\zeta}, vk_{B,\zeta}, vk_{B,\text{rej},\zeta}) = \text{Spl.Setup}(1^\lambda; r_{B,\zeta})$;
9.   Let $\alpha_\zeta = \{^\cdot\}$ and $m_\zeta = (t_\zeta, \text{index}_\zeta, w_{\text{st},\zeta}, w_{\text{com},\zeta}, v_\zeta)$;
10. If $t < i$ or $(t = i + 1 and \text{parent.index} \leq j)$ then
11.       If $\text{Spl.Verify}(vk_A, m_\zeta, \sigma_\zeta) = 1$, set $\alpha_\zeta = 'A';$
12.       Else, output Reject;
13.   else
14.       If $\text{Spl.Verify}(vk_A, m_\zeta, \sigma_\zeta) = 1$, set $\alpha_\zeta = 'A';$
15.       If $\alpha_1 \neq 'A'$ and $\text{Spl.Verify}(vk_B, m_\zeta, \sigma_\zeta) = 1$, set $\alpha_\zeta = 'B';$
16.       If $\alpha_\zeta = \{^\cdot\}$, output Reject;
17.   If $\alpha_1 = 'A'$ and $\alpha_2 = 'A'$, set $\alpha = 'A';$
18.   Else, set $\alpha = 'B';$
19. Compute $w'_{\text{st}} = \text{Acc.Combine}(pp_{\text{Acc.st}}, w_{\text{st},1}, w_{\text{st},2});$
20. Compute $w'_{\text{com}} = \text{Acc.Combine}(pp_{\text{Acc.com}}, w_{\text{com},1}, w_{\text{com},2});$
21. Compute $v' = \text{Itr.Iterate2to1}(pp_{\text{itr}}, (v_1, v_2), (t, \text{parent.index}, w_{\text{st},1}, w_{\text{com},1}, w_{\text{st},2}, w_{\text{com},2}));$
22. Let $r'_{A} = \text{PRF}(K_A, (t, \text{parent.index}))$ and $r'_{B} = \text{PRF}(K_B, (t, \text{parent.index}))$;
23. Compute $(sk'_{A}, vk'_{A}, vk'_{A,\text{rej}}) = \text{Spl.Setup}(1^\lambda; r'_{A})$ and $(sk'_{B}, vk'_{B}, vk'_{B,\text{rej}}) = \text{Spl.Setup}(1^\lambda; r'_{B})$;
24. Let $m' = (t, \text{parent.index}, w'_{\text{st}}, w'_{\text{com}}, v');$
25. If $t \leq i$ then
26.       Compute $\sigma' = \text{Spl.Sign}(sk'_{A}, m');$
27.   if $t = i + 1$ then
28.       if parent.index = index for index $\in C_{i,j}$ then
29.           If $m' = m_{\text{index}}$ for $m_{\text{index}} \in M_{i,j}$, compute $\sigma' = \text{Spl.Sign}(sk'_{A'}, m');$
30.           Else, $m' \neq m_{\text{index}}$ for $m_{\text{index}} \in M_{i,j}$, compute $\sigma' = \text{Spl.Sign}(sk'_{B'}, m');$
31.       else if parent.index = $j$ then
32.           If $m' = m_{i,j}$, compute $\sigma' = \text{Spl.Sign}(sk'_{A}, m');$
33.           Else, compute $\sigma' = \text{Spl.Sign}(sk'_{B}, m');$
34.           else
35.               Compute $\sigma' = \text{Spl.Sign}(sk'_{A'}, m')$;
36.               Compute $\sigma' = \text{Spl.Sign}(sk'_{B'}, m')$;
37.           else
38.               Compute $\sigma' = \text{Spl.Sign}(sk'_{A'}, m')$;
39.       Let parent_node = $(t, \text{parent.index}, w'_{\text{st}}, w'_{\text{com}}, v', \sigma')$;
40.       if parent.index = $\epsilon$ then
41.           Output $\mathbf{st}^{\text{out}} = (\mathbf{st}^{\text{in}}, id_{\text{cpu}}, \text{parent.node}), \mathbf{an}^{\text{out}} = \bot$;
42.       else
43.           Output $\mathbf{st}^{\text{out}} = (\mathbf{st}^{\text{in}}, id_{\text{cpu}}, \bot), \mathbf{an}^{\text{out}} = \text{parent.node}$;
Algorithm 61: $E_{\text{combine}}^{0,1,i,j}(\text{intermediate})$

**Input**: $s_t^\text{in} = (s_t^\text{in}, id_{cpu}, \bot), \overline{a}_t^\text{in} = (\text{node}_1, \text{node}_2)$

**Data**: $T, pp_{\text{Acc, st}}, pp_{\text{Acc, com}}, pp_{\text{itr}}, K_A, K_B, (m_{i,j,1}, m_{i,j,2})$

1. Parse node$_\zeta$ as $(t_\zeta, \text{index}_\zeta, w_{\text{st, } \zeta}, w_{\text{com, } \zeta}, v_\zeta, \sigma_\zeta)$ for $\zeta = 1, 2$;
2. If $t_1 \neq t_2$, output Reject. Else, let $t = t_1$;
3. If $t < 1$, output Reject;
4. If index$_1$ and index$_2$ are not siblings, output Reject;
5. Set parent index as the parent of index$_1$ and index$_2$;
6. for $\zeta = 1, 2$ do
   7. Let $r_{A, \zeta} = \text{PRF}(K_A, (t_\zeta, \text{index}_\zeta))$ and $r_{B, \zeta} = \text{PRF}(K_B, (t_\zeta, \text{index}_\zeta))$;
   8. Compute $(sk_{A, \zeta}, vk_{A, \zeta}) = \text{Spl.Setup}(1^\lambda; r_{A, \zeta})$ and $(sk_{B, \zeta}, vk_{B, \zeta}) = \text{Spl.Setup}(1^\lambda; r_{B, \zeta})$;
   9. Let $\alpha_\zeta = \cdot\cdot\cdot$ and $m_\zeta = (t_\zeta, \text{index}_\zeta, w_{\text{st, } \zeta}, w_{\text{com, } \zeta}, v_\zeta)$;
   10. if $t \leq i$ or $(t = i + 1 \text{ and parent index } \leq j)$ then
       11. if Spl.$\text{Verify}(vk_{A, m_\zeta}, \sigma_\zeta) = 1$, set $\alpha_\zeta = \cdot\cdot\cdot$;
       12. else, output Reject;
   13. else
       14. if Spl.$\text{Verify}(vk_{A, m_\zeta}, \sigma_\zeta) = 1$, set $\alpha_\zeta = \cdot\cdot\cdot$;
       15. if $\alpha_\zeta \neq \cdot\cdot\cdot$ and Spl.$\text{Verify}(vk_{B, m_\zeta}, \sigma_\zeta) = 1$, set $\alpha_\zeta = \cdot\cdot\cdot$;
       16. if $\alpha_\zeta \neq \cdot\cdot\cdot$, output Reject;
7. If $\alpha_1 = \cdot\cdot\cdot$ and $\alpha_2 = \cdot\cdot\cdot$, set $\alpha = \cdot\cdot\cdot$;
8. Else, set $\alpha = \cdot\cdot\cdot$;
9. Compute $w'_s = \text{Acc.Combine}(pp_{\text{Acc, st}}, w_{\text{st, } 1}, w_{\text{st, } 2})$;
10. Compute $w'_{\text{com}} = \text{Acc.Combine}(pp_{\text{Acc, com}}, w_{\text{com, } 1}, w_{\text{com, } 2})$;
11. Compute $v' = \text{itr.\text{Iterate2to1}}(pp_{\text{itr}}, (v_1, v_2), (t, \text{parent index}, w_{\text{st, } 1}, w_{\text{com, } 1}, w_{\text{st, } 2}, w_{\text{com, } 2}))$;
12. Let $r'_A = \text{PRF}(K_A, (t, \text{parent index}))$ and $r'_B = \text{PRF}(K_B, (t, \text{parent index}))$;
13. Compute $(sk_A', vk_A', vk_{A, \text{rej}}) = \text{Spl.Setup}(1^\lambda; r'_A)$ and $(sk_B', vk_B', vk_{B, \text{rej}}) = \text{Spl.Setup}(1^\lambda; r'_B)$;
14. Let $m' = (t, \text{parent index}, w'_s, w'_{\text{com}}, v')$;
15. if $t = i$ then
16. Compute $\sigma' = \text{Spl.Sign}(sk_A', m')$;
17. if $t = i + 1$ then
18. if parent index = index$1$ for index$\in C_{i,j}$ then
19. if $m' = m_{\text{index}}$ for $m_{\text{index}} \in M_{i,j}$, compute $\sigma' = \text{Spl.Sign}(sk_A', m')$;
20. else, $m' \neq m_{\text{index}}$ for $m_{\text{index}} \in M_{i,j}$, compute $\sigma' = \text{Spl.Sign}(sk_B', m')$;
21. else if parent index$= j$ then
22. if $m_1 = m_{i,j,1}$ and $m_2 = m_{i,j,2}$, compute $\sigma' = \text{Spl.Sign}(sk_A', m')$;
23. else, compute $\sigma' = \text{Spl.Sign}(sk_B', m')$;
24. else
25. Compute $\sigma' = \text{Spl.Sign}(sk_A', m')$;
26. else
27. Compute $\sigma' = \text{Spl.Sign}(sk_A', m')$;
28. Let parent node$= (t, \text{parent index}, w'_s, w'_{\text{com}}, v', \sigma')$;
29. if parent index$= \epsilon$ then
30. Output $\overline{s}_t^{\text{out}} = (s_t^{\text{in}}, id_{cpu}, \text{parent node}), \overline{a}_t^{\text{out}} = \bot$;
31. else
32. Output $\overline{s}_t^{\text{out}} = (s_t^{\text{in}}, id_{cpu}, \bot), \overline{a}_t^{\text{out}} = \text{parent node}$;
hybrids through $F_{\text{branch}}$ and $F_{\text{combine}}$, use the hybrid steps in memory-less PRAM, and then we can use (indistinguishably) $\hat{F}^{t+1, \text{OUpdate}^1}$ that hardwires the correct digest value as the result. Finally, we design hybrids from $\hat{F}^{t+1, \text{OUpdate}^1}$ to $\hat{F}^{t+2}$, where the difference is only at the last round of OUpdate$^1$. The proof is similar to Lemma B.9, which is to move hardwired digest from the output of OUpdate$^{i+1}$ to input of $\hat{F}^{t+2}$.

Now we have a hybridized program $\hat{F}^{t+2}$ that always has a correct digest value at a read round, and the hybrid can be carried iteratively to replace all $F^0$ with $F^1$.

### B.5 Proof of Theorem 8.1 (Security for $\mathcal{RE}$-RAM)

In this subsection, we provide the security proof for our $\mathcal{RE}$ scheme. Following the security definition of randomized encoding scheme, in order to prove that our construction achieve the hiding property, in Section B.5.1 we first present a simulator which generates a simulated encoding. Then in Section B.5.2, we outline the main hybrids to prove that the simulated encoding is indistinguishable from the encoding generated in our $\mathcal{RE}$ scheme. As highlighted in technical overview in Section 4, our proof here is highly non-trivial, and we use “backward in time” hybrid argument by [KLW15] in Section B.5.3, and introduce “puncturing ORAM” technique in Section B.5.4, and more fine-grained “partial puncturing” technique in Section B.5.5. In order to present our proof in a better way, we formulate several technical lemmas. In the proof of each technical lemma, we first give high-level intuitions, and then present the proof details.

#### B.5.1 Real and Ideal Experiments

Recall that in our construction, the generated encoding is of the form $\text{CiO}(P_{\text{hide}}, x_{\text{hide}})$, where $P_{\text{hide}}$ is a compiled version of $P$, and $x_{\text{hide}}$ is an encrypted version of $x$. To prove the security, i.e., hiding, of our $\mathcal{RE}$, we need, via a sequence of hybrids, obtain a simulated encoding $\text{CiO}(P_{\text{Sim}}, x_{\text{Sim}})$ where all encryptions generated by $P_{\text{Sim}}$ as well as in $x_{\text{Sim}}$ are replaced by encryption of a special dummy symbol. More precisely, $P_{\text{Sim}}$ simulates the access pattern by applying the known public strategy and at each time step $t < t^*$, simply ignores the input and outputs encryptions of dummy (for both CPU state and memory content), and output $y$ at time step $t = t^*$. More concretely, we consider two security experiments, **Real** and **Ideal**:

- in **Real**, the adversary $A$ is given the encoding $\text{ENC}$ which is generated as in the $\mathcal{RE}$ scheme, i.e., $\text{ENC} \leftarrow \mathcal{RE} \cdot \text{Encode}(P, x, 1^\lambda)$.
- in **Ideal**, the adversary $A$ is given the emulated encoding $\text{ENC}_{\text{sim}}$ which is generated by a simulator $S$, i.e., $\text{ENC}_{\text{sim}} \leftarrow S(1^{|P|}, 1^{|x|}, t^*, y, 1^\lambda, T, S)$.

To complete the proof, we now construct such simulator $S$ to generate a simulated encoding, and then in the next subsection, we show that a computationally bounded $A$ cannot distinguish ENC from $\text{ENC}_{\text{sim}}$.

**Encoding-Simulation algorithm** $\text{ENC}_{\text{sim}} \leftarrow S(1^{|P|}, 1^{|x|}, t^*, y, 1^\lambda, T, S)$: The simulator, i.e., the encoding-simulation algorithm takes the following steps to generate the encoding $\text{ENC}_{\text{sim}}$.

- The encoding-simulation algorithm first stores dummy information with $|x|$-bits in $\text{mem}^0_{\text{sim}}$, and sets $\text{st}^0 := \text{Init}$, and then transforms $(\text{mem}^0_{\text{sim}}, \text{st}^0)$ into $(\text{mem}^0_{o,\text{sim}}, \text{st}^0_o)$ using $\text{OAccess}\{K_N\}$ as in the construction. Then it chooses puncturable PRF key $K_{\text{Sim}} \leftarrow \text{PPRF}.\text{Setup}(1^\lambda)$, and constructs an access pattern simulation program $\text{SIMOAccess}\{K_{\text{Sim}}\}$ (see Algorithm 62), and further defines $F_{o,\text{sim}}$ based on $\text{SIMOAccess}$. Now the encoding-simulation algorithm defines $\Pi_{o,\text{sim}} = ((\text{mem}^0_{o,\text{sim}}, \text{st}^0_o), F_{o,\text{sim}})$

- The encoding-simulation algorithm transforms $\Pi_{o,\text{sim}}$ into $\Pi_{e,\text{sim}} = ((\text{mem}^0_{e,\text{sim}}, \text{st}^0_e), F_{e,\text{sim}})$
Here the encoding-simulation algorithm chooses puncturable PRF key $K_E \leftarrow \text{PPRF.Setup}(1^\lambda)$, and then compute $t^* = \lceil t^*/q_o \rceil$. Then based on $F_{o,sim}$, $t^*$ as well as the corresponding output value $y$, it generates the next-step program $F_{e,sim}$ as in Algorithm 63.

The simulation algorithm encrypts $\text{mem}_{o,sim}^0$ into $\text{mem}_{e,sim}^0$ as in the construction. In addition, the encoding of $s_t^0$ is identical to that in construction.

Finally, the encoding-simulation algorithm computes $\text{ENC}_{sim} \leftarrow \text{CiO.Obf}(1^\lambda, \Pi_{e,sim})$ and outputs $\text{ENC}_{sim}$.

---

**Algorithm 62: SimOACCESS\{$K_{Sim}$\}:** the recursive program simulates the access pattern of $\text{OACCESS}\{K_N\}$.

| Input | $t, d$ |
| Output | No return value |
| Data: | $K_{Sim}$, $\alpha, \text{MaxDepth}$ (Memory size $S = \alpha^{\text{MaxDepth}}$) |
1. If $d \geq \text{MaxDepth}$ then
2. \[ \text{return}; \] // Fetch
3. SimOACCESS($t, d + 1$);
4. Pick leaf $\text{pos}$ at recursion level $d$ based on PRF($K_{Sim}, (t, d, \text{FetchR})$);
5. $I_{\text{fetch}} \leftarrow \text{PATH}(d, \text{pos})$;
6. $B_{\text{fetch}} \leftarrow \text{READ}(I_{\text{fetch}})$;
7. $\text{WRITE}(I_{\text{fetch}}, \text{dummy})$;
8. Pick leaf $\text{pos''}$ at recursion level $d$ based on PRF($K_{Sim}, (t, d, \text{FlushR})$);
9. $I_{\text{flush}} \leftarrow \text{PATH}(d, \text{pos''})$;
10. $B_{\text{flush}} \leftarrow \text{READ}(I_{\text{flush}})$;
11. $\text{WRITE}(I_{\text{flush}}, \text{dummy})$;
12. \[ \text{return}; \]

---

**B.5.2 Proof Outline: From Hyb$_0$ to Hyb$_3$**

We here provide a roadmap for proving the security of our construction, and we outline the main hybrids.

**Proof.** We let Hyb$_0$ be the real security game Real, and Hyb$_3$ be the ideal security game Ideal. We will show via multiple layers of hybrids that Hyb$_0$ is computationally indistinguishable from Hyb$_3$. In each hybrid, the simulator generates the encoding ENC as in the construction, except that different next-step programs are used. The overview of the intermediate hybrids is shown as follows:

- **Real** = Hyb$_0 \approx$ Hyb$_1 \approx$ Hyb$_{2,t^*} \approx \ldots \approx$ Hyb$_{2,0} =$ Hyb$_3 =$ Ideal
- Hyb$_{2,i} =$ Hyb$_{2,i,0,0} \approx \ldots \approx$ Hyb$_{2,i,0,d_{max}} \approx \ldots \approx$ Hyb$_{2,i,0',0} =$ Hyb$_{2,i-1}$
- Hyb$_{2,i,0,j,1} \approx$ Hyb$_{2,i,0,j,1,0} \approx$ Hyb$_{2,i,0,j,1,j+1} \approx \ldots \approx$ Hyb$_{2,i,0,j,1,i-1} \approx \ldots \approx$ Hyb$_{2,i,0,j,1,z} \approx$ Hyb$_{2,i,0,j,1,z-1}$
- Hyb$_{2,i,0,j,1,z} \approx$ Hyb$_{2,i,0,j,1,z-1}$

In the first and outermost layer, we define the hybrids Hyb$_1$ and Hyb$_{2,i}$ for $0 \leq i \leq t^*$.

**Hyb$_0$.** This hybrid is the real security game Real.

**Hyb$_1$.** In this hybrid, next-step program $P_{e1}$ as defined in Algorithm 64, is used. This program is similar to the next-step program $P_e$ in Real, except that, at time $t = t^*$, it outputs the signed correct computation result $y := P(x)$, which is hardwired into the program. At $t > t^*$, the program outputs Reject.
Algorithm 63: $F_{e,sim}$

```
Input : $st^\text{in} = (st^\text{in}, t)$, $\tilde{a}^\text{in}_{K-H} = (I^\text{in}, (B^\text{in}, lw^\text{in}))$
Data: $T, K_E, t^*, y, K_N, K_{Sim}$
1 Compute $t = \lceil t/q_0 \rceil$;
2 If $t > t^*$, output Reject;
3 if $t = t^*$ then
  4 Set $st^\text{out} = (\text{halt}, y), \tilde{a}^\text{out}_{K-H} = \perp$;
  5 Output $(st^\text{out}, \tilde{a}^\text{out}_{K-H})$;
6 Compute $(I^*, B^*) \leftarrow F_{e,sim}(t)$
7 Set $lw^\text{out} = (t, \ldots, t)$;
8 Compute $(r_1^\text{out}, r_1^*) = \text{PRF}(K_E, (lw^\text{out}, h(I^*)))$;
9 Compute $(r_2^\text{out}, r_2^*) = \text{PRF}(K_E, t)$;
10 Compute $(pk', sk') = \mathcal{P}K\mathcal{E}.Gen(1^\lambda; r_1^\text{out})$;
11 Compute $B^\text{out} = \mathcal{P}K\mathcal{E}.Encrypt(pk', B^*; r_2^\text{out})$;
12 Compute $(pk', sk') = \mathcal{P}K\mathcal{E}.Gen(1^\lambda; r_3^*)$;
13 Compute $st^\text{out} = \mathcal{P}K\mathcal{E}.Encrypt(pk', \text{dummy}; r_4^\text{out})$;
14 Set $I^\text{out} = I^*$;
15 Output $\tilde{st}^\text{out} = (st^\text{out}, t + 1), \tilde{a}^\text{out}_{K-H} = (I^\text{out}, (B^\text{out}, lw^\text{out}))$;
```

$\text{Hyb}_{2,t^*}$. In this hybrid, $F^1_e$ is replaced by $F^{2,t^*}_e$ defined in Algorithm 65. This program is similar to $F^1_e$, except that its access pattern at time $t$, where $i \leq t \leq t^*$ is replaced by a simulated access pattern provided by the SIMOACCESS defined in Algorithm 62, and the output state is replaced by an encryption of a special symbol dummy.

$\text{Hyb}_3$. This hybrid is the ideal security game Ideal. In this hybrid, $F_{e,sim}$, defined in Algorithm 63, is used. This program is identical to $F^{2,0}_e$, in which the access pattern in all time steps $t$ where $t \leq t^*$ are simulated. The initial memory mem$^0$ is written with dummy (rather than $x$) during the encoding process, and mem$^0$ is the only difference between $\text{Hyb}_{2,0}$ and $\text{Hyb}_3$.

Analysis. In the remaining of this subsection, we complete the proof of the theorem via several lemmas.

From $\text{Hyb}_0$ to $\text{Hyb}_1$: The only difference between $F_e$ and $F^1_e$ is that, in $F^1_e$, the output in time $t = t^*$ is hardwired and all computation are rejected after halting time $t^*$. Therefore, by Theorem 6.2, since $\Pi_e$ and $\Pi^1_e$ have the same computation trace, their encodings are computationally indistinguishable. We remark that rejecting all computation after $t^*$ is very useful when arguing $\mathcal{P}K\mathcal{E}$ security in following hybrids because it guarantees the private key is never used after time $t^*$.

From $\text{Hyb}_1$ to $\text{Hyb}_{2,t^*}$: The only difference between $F^1_e$ and $F^{2,t^*}_e$ is that, in $F^{2,t^*}_e$, the access pattern in time $t = t^*$ is simulated. However, since the program terminates at $t = t^*$ (that means, $t = t^*$) by outputting the hardwired computation result, the modified part will never be executed. Therefore, by Theorem 6.2, since $\Pi_e$ and $\Pi^{2,t^*}_e$ have the same computation trace, their encodings are computationally indistinguishable.
From Hyb$_{2,i}$ to Hyb$_{2,i-1}$: This is the most complicated part, which we will defer the discussion to Lemma B.52.

From Hyb$_{2,0}$ to Hyb$_3$: The only difference between the two hybrids is that the initial memory mem$^0$ in Hyb$_3$ is encryption of dummy. Note that the initial memory is never decrypted in $F_{e,sim}$, and we argue its indistinguishability by standard puncturing and $\mathcal{PK}\mathcal{E}$ properties. For each non-empty bit $b_i$ in mem$^0$, replace its corresponding bit $b'_i$ in mem$^0$ with dummy by following hybrids:

- Puncture PRF key $K_E$ at $(0, h_i)$ in $F_{e,sim}$, where $h_i$ is the “height” given by function $h(\cdot)$ to encrypt the bucket $B$ storing $b'_i$. This does not change the computation trace and is computationally indistinguishable.
- Encrypt $B$ that contains bit $b'_i$ in mem$^0$ with a truly random $\mathcal{PK}\mathcal{E}$ public key, which is computationally indistinguishable by selective security of PPRF.
- Encrypt $B$ that contains dummy instead of bit $b'_i$. The indistinguishability is guaranteed by the IND-CPA security of $\mathcal{PK}\mathcal{E}$.

Therefore, Hyb$_{2,0}$ and Hyb$_3$ are computationally indistinguishable.

From above, Hyb$_0$ and Hyb$_3$ are computationally indistinguishable as required.

Algorithm 64: $F_{e,1}^1$

| Input | $\tilde{\text{st}}^{in} = (\tilde{\text{st}}^{in}, t)$, $\tilde{\alpha}_{\text{ICS}}^{in} = (\tilde{\text{I}}^{in}, (\tilde{\text{B}}^{in}, \tilde{\text{lw}}^{in}))$ |
| Data: | $T, K_E, t^*, y, K_N$ |
| 1 | Compute $t = \lceil t/g_0 \rceil$; |
| 2 | \textbf{if} $t > t^*$, output \textbf{Reject}; |
| 3 | \textbf{if} $t = t^*$ then |
| 4 | Set $\tilde{\text{st}}^{out} = (\text{halt}, y), \tilde{\alpha}_{\text{ICS}}^{out} = \bot$; |
| 5 | Output $(\tilde{\text{st}}^{out}, \tilde{\alpha}_{\text{ICS}}^{out})$; |
| 6 | Compute $(r_1^{in}, r_2^{in}) = \text{PRF}(K_E, (\tilde{\text{lw}}^{in}, h(T^{in})))$; |
| 7 | Compute $(\text{pk}^{in}, \text{sk}^{in}) = \mathcal{PK}\mathcal{E}.\text{Gen}(1^\lambda; r_1^{in})$; |
| 8 | Compute $\text{B}^{in} = \mathcal{PK}\mathcal{E}.\text{Decrypt}(\text{sk}^{in}, \tilde{\text{B}}^{in})$; |
| 9 | Compute $(r_3^{t-1}, r_4^{t-1}) = \text{PRF}(K_E, t-1)$; |
| 10 | Compute $(\text{pk}_{st}, \text{sk}_{st}) = \mathcal{PK}\mathcal{E}.\text{Gen}(1^\lambda; r_3^{t-1})$; |
| 11 | Compute $\text{st}^{in} = \mathcal{PK}\mathcal{E}.\text{Decrypt}(\text{sk}_{st}, \tilde{\text{st}}^{in})$; |
| 12 | Compute $(\tilde{\text{st}}^{out}, \tilde{\text{I}}^{out}, \tilde{\text{B}}^{out}) = F_0(t, \tilde{\text{st}}^{in}, \tilde{\text{I}}^{in}, \tilde{\text{B}}^{in})$; |
| 13 | Set $\tilde{\text{lw}}^{out} = (t, \ldots, t)$; |
| 14 | Compute $(r_1^{out}, r_2^{out}) = \text{PRF}(K_E, (\tilde{\text{lw}}^{out}, h(\tilde{\text{I}}^{out})))$; |
| 15 | Compute $(\text{pk}', \text{sk}') = \mathcal{PK}\mathcal{E}.\text{Gen}(1^\lambda; r_1^{out})$; |
| 16 | Compute $\text{B}^{out} = \mathcal{PK}\mathcal{E}.\text{Encrypt}(\text{pk}', \tilde{\text{B}}^{out}, r_2^{out})$; |
| 17 | Compute $(r_3^{t}, r_4^{t}) = \text{PRF}(K_E, t)$; |
| 18 | Compute $(\text{pk}', \text{sk}') = \mathcal{PK}\mathcal{E}.\text{Gen}(1^\lambda; r_3^{t})$; |
| 19 | Compute $\tilde{\text{st}}^{out} = \mathcal{PK}\mathcal{E}.\text{Encrypt}(\text{pk}', \tilde{\text{st}}^{out}, r_4^{t})$; |
| 20 | Output $\tilde{\text{st}}^{out} = (\tilde{\text{st}}^{out}, t+1), \tilde{\alpha}_{\text{ICS}}^{out} = (\tilde{\text{I}}^{out}, (\tilde{\text{B}}^{out}, \tilde{\text{lw}}^{out}))$; |
Algorithm 65: $F^{2,i}_c$

Input: $\tilde{s}_t^{in} = (s_t^{in}, t)$, $\tilde{d}_t^{in} = (I^{in}, (B^{in}, lw^{in}))$

Data: $T, K_E, t^*, y, K_N, K_{Sim}, i$

1. Compute $t = \lceil t/q_0 \rceil$;
2. If $t > t^*$, output Reject;
3. if $t = t^*$ then
   4. \[\ldots\]
5. if $i \leq t < t^*$ then
   6. Compute $(I^*, B^*) \leftarrow F_{o,sim}(t)$
   7. Set $lw^{out} = (t, \ldots, t)$;
   8. Compute $(r_1^{out}, r_2^{out}) = \text{PRF}(K_E, (lw^{out}, h(I^*)))$;
   9. Compute $(r_3, r_4) = \text{PRF}(K_E, t)$;
10. Compute $(pk', sk') = \mathcal{PKE}.Gen(1^\lambda, r_1^{out})$;
11. Compute $B^{out} = \mathcal{PKE}.Encrypt(pk', B^*; r_2^{out})$;
12. Compute $st^{out} = \mathcal{PKE}.Encrypt(pk', \text{dummy}; r_4^{out})$;
13. Set $I^{out} = I^*$;
else
16. Compute $(r_1^{in}, r_2^{in}) = \text{PRF}(K_E, (lw^{in}, h(I^{in})))$;
17. Compute $(pk^{in}, sk^{in}) = \mathcal{PKE}.Gen(1^\lambda, r_1^{in})$;
18. Compute $B^{in} = \mathcal{PKE}.Decrypt(sk^{in}, B^{in})$;
19. Compute $(r_3^{t-1}, r_4^{t-1}) = \text{PRF}(K_E, t - 1)$;
20. Compute $(pk_{st}, sk_{st}) = \mathcal{PKE}.Gen(1^\lambda, r_3^{t-1})$;
21. Compute $st^{in} = \mathcal{PKE}.Decrypt(sk_{st}, st^{in})$;
22. Compute $(st^{out}, I^{out}, B^{out}) = F_o(t, st^{in}, I^{in}, B^{in})$;
23. Set $lw^{out} = (t, \ldots, t)$;
24. Compute $(r_1^{out}, r_2^{out}) = \text{PRF}(K_E, (lw^{out}, h(I^{out})))$;
25. Compute $(pk', sk') = \mathcal{PKE}.Gen(1^\lambda, r_1^{out})$;
26. Compute $B^{out} = \mathcal{PKE}.Encrypt(pk', B^{out}; r_2^{out})$;
27. Compute $(r_3, r_4) = \text{PRF}(K_E, t)$;
28. Compute $(pk', sk') = \mathcal{PKE}.Gen(1^\lambda, r_3^{t-1})$;
29. Compute $st^{out} = \mathcal{PKE}.Encrypt(pk', st^{out}; r_4^{out})$;
30. Output $st^{out} = (st^{out}, t + 1)$, $\tilde{d}_t^{out} = (I^{out}, (B^{out}, lw^{out}))$;
B.5.3 Backward Erasing: From Hyb$_{2,i}$ to Hyb$_{2,i-1}$

We start to elaborate the outline provided in the previous subsection. We prove the security by a sequence of hybrids that “erase” the computation backward in time, which leads to a simulated encoding $\text{ENC}_{\text{sim}} = \text{CiO}(P_{\text{Sim}}, x_{\text{Sim}})$ where all encryptions generated by $P_{\text{Sim}}$ as well as in $x_{\text{Sim}}$ are replaced by encryption of a special dummy symbol. More precisely, $P_{\text{Sim}}$ simulates the access pattern using the public access function $\text{ap}$, and at each time step $t < t^*$, simply ignores the input and outputs encryptions of dummy (for both CPU state and memory content), and output $y$ at time step $t = t^*$.

By erasing the computation backward in time, we consider intermediate hybrids Hyb$_{2,i}$ where the first $i$ time step of computation are real, and that of the remaining time step are simulated. Namely, Hyb$_{2,i}$ is a hybrid encoding $\text{CiO}(P_{\text{Hyb}_{2,i}}, x_{\text{hide}})$, where $P_{\text{Hyb}_{2,i}}$ acts as $P_{\text{hide}}$ for the first $i$ time step, and acts as $P_{\text{Sim}}$ in the remaining time steps. (Note here that $P_{\text{Hyb}_{2,i}}, P_{\text{hide}}, P_{\text{Sim}}$ correspond to next-step programs $F_{e,i}^2$, $F_e$, $F_{e,\text{sim}}$, respectively.)

The main step is to show indistinguishability of Hyb$_{2,i}$ and Hyb$_{2,i-1}$, which corresponds to erasing the computation at the $i$-th time step. Roughly, to argue this, the key observation is that the $i$-th decryption key is not used in the honest evaluation, which allows us to replace the output of the $i$-th time step by encryption of dummy by a puncturing argument. We can then further remove the computation at the $i$-th time step readily by $\text{CiO}$ security.

In fact, the argument is more involved given the fact that the CP ORAM is used in our construction. Suppose that at time $i$ the program wishes to access a memory block $\ell$ which is well-defined by the computation. The program must read the position map value $p = \text{pos}([\ell])$ at first, and then fetches the block $\ell$ along the path $p$ in the ORAM tree. However, our $\mathcal{RE}$ construction relies on CP ORAM tree-based structure where the position map is recursively outsourced to $d_{\text{max}}$ ORAM trees. Here we divide the sequence of hybrids into two phases. The first one is to simulate the memory accesses from level 0 to $d_{\text{max}}$. The second one is also simulate to the memory accesses as well as in $\text{Sim}$.

The two important hybrids corresponding to these two phases are respectively defined as follows.

Hyb$_{2,i,0,j}$ (the first phase):
- At time $t = i - 1$, $F_{e,i}^{2,i,0,j}$ returns real $\text{st}^{\text{out}}$, and outputs real accesses identical to $\text{OACCESS}$ if $d \geq j$.
- At time $t = i - 1$, $F_{e,i}^{2,i,0,j}$ returns real $\text{st}^{\text{out}}$, but outputs the simulated accesses if $d < j$.

Hyb$_{2,i,0',j}$ (the second phase):
- At time $t = i - 1$, $F_{e,i}^{2,i,0',j}$ outputs the simulated accesses, and returns real $\text{st}^{\text{out}}$ if $d \leq j$.
- At time $t = i - 1$, $F_{e,i}^{2,i,0',j}$ outputs the simulated accesses, but returns $\text{st}^{\text{out}} = \text{dummy}$ if $d > j$.

Note that Hyb$_{2,i}$ is identical to Hyb$_{2,i,0,0'}$, and Hyb$_{2,i,0,0'}$ is also identical to Hyb$_{2,i-1}$. Clearly, we need to argue the remaining hybrids are indistinguishable, Hyb$_{2,i,0,0} \approx \ldots \approx$ Hyb$_{2,i,d_{\text{max}}}$ $\approx$ Hyb$_{2,i,0',d_{\text{max}}} \approx \ldots \approx$ Hyb$_{2,i,0',0}$.

Lemma B.52. Let $\mathcal{PKE}$ be an IND-CPA secure public key encryption scheme, $\text{CiO}$ be a computation-trace indistinguishability obfuscation scheme in RAM model, PRF be a secure puncturable PRF scheme. Then the hybrids Hyb$_{2,i}$ and Hyb$_{2,i-1}$ are computationally indistinguishable for $1 \leq i \leq t^*$.

Proof. For each $i$, we define two second-layer hybrids Hyb$_{2,i,0,j}$ and Hyb$_{2,i,0',j}$ for $0 \leq j \leq d_{\text{max}}$, where $d_{\text{max}}$ denotes the maximum depth of the ORAM tree.
Hyb\(_{2,i,0,j}\). In this hybrid, the program \(F_{e,0,j}^{2,i,0,j}\) is defined in Algorithm 66. At time \(t = i - 1\), \(F_{e,0,j}^{2,i,0,j}\) uses HYBOACCESS\(_j\) which outputs the simulated accesses if \(d < j\), and it outputs those accesses identical to OACCESS if \(d \geq j\) (Algorithm 67). Like previous programs, \(F_{e,0,j}^{2,i,0,j}\) uses the HYBOACCESS\(_j\) compiled program named \(F_{o,hyb}^{j} = \text{Compile}(F, \text{HYBOACCESS}\(_j\}\{K_N, K_{Sim}\})\). Note that the values \((\text{loc}, \text{val})\) from the input, \(\text{newpos}\) and \(\text{pos}\) returned by PRF\((K_N, \cdot)\) and HYBOACCESS\(_j\)(\(d + 1, \cdot\)) are never used if \(d < j\).

Hyb\(_{2,i,0',j}\). In this hybrid, the program \(F_{e,0',j}^{2,i,0',j}\) is defined in Algorithm 68. At time \(t = i - 1\), \(F_{e,0',j}^{2,i,0',j}\) replace \(\text{st}_{\text{out}}\) by \(\text{dummy}\) for all \(d > j\).

**Analysis.** In the remaining of this subsection, we will complete the proof of the lemma.

From Hyb\(_{2,i}\) to Hyb\(_{2,i,0,0}\): These two hybrids are identical.

From Hyb\(_{2,i,0,j}\) to Hyb\(_{2,i,0,j+1}\): We defer the discussion to Lemma B.53.

From Hyb\(_{2,i,0,d_{\text{max}}}\) to Hyb\(_{2,i,0',d_{\text{max}}}\): These two hybrids are identical.

From Hyb\(_{2,i,0',j}\) to Hyb\(_{2,i,0',j-1}\): This step can be proved via multiple hybrids. For readability, we describe the hybrids without defining them in separate algorithms. The only difference between \(F_{e,0',j-1}^{2,i,0',j}\) and \(F_{e,0',j-1}^{2,i,0',j-1}\) is that, in \(F_{e,0',j-1}^{2,i,0',j-1}\), \(\text{st}_{\text{out}}\) is replaced by \(\text{dummy}\) at time \(t = i - 1\) and depth \(d = j\). In the first hybrid, we puncture the input \((i - 1, j, \text{Init})\) for PRF key \(K_E\) and hardwire the pseudorandomness computed from \(K_E\). Since the computation defined by this program has identical computation trace as that in the previous hybrid, indistinguishability is guaranteed by Theorem 6.2. In the next hybrid, we replace the pseudorandomness by a truly random number. Indistinguishability is guaranteed by the security of the puncturable PRF. Then, we hardwire \(\text{st}_{\text{out}}\), which is generated by the true randomness in the previous hybrid, into the program and take away the hardwired true randomness. Since the computation defined by this program has identical computation trace as that in the previous hybrid, indistinguishability is guaranteed by Theorem 6.2. Next, we replace hardwired \(\text{st}_{\text{out}}\) by an encryption of \(\text{dummy}\). Indistinguishability is guaranteed by the IND-CPA security of \(\mathcal{PKE}\). Finally, we un-puncture the PRF key \(K_E\) to obtain the required hybrid. Indistinguishability is again guaranteed by the security of the puncturable PRF.

From Hyb\(_{2,i,0',0}\) to Hyb\(_{2,i-1}\): These two hybrids are identical. 

\(\square\)
Algorithm 66: $F_{e, i, 0, j}$

Input: $\tilde{\text{st}}^{\text{in}} = (\text{st}^{\text{in}}, t)$, $\tilde{\text{a}}^{\text{in}}_{h+1} = (\text{I}^{\text{in}}, (\text{B}^{\text{in}}, \text{lw}^{\text{in}}))$

Data: $T$, $K_E$, $t^*$, $y$, $K_N$, $K_{\text{Sim}}$, $i, j$

1 Compute $t = \lceil t / q_0 \rceil$:
2 If $t > t^*$, output $\text{Reject}$;
3 if $t = t^*$ then
4 ... 
5 if $i \leq t < t^*$ then
6 ... 
7 else
8 Compute $(t_1^{\text{in}}, r_2^{\text{in}}) = \text{PRF}(K_E, (\text{lw}^{\text{in}}, h(\text{I}^{\text{in}})))$;
9 Compute $(\text{pk}^{\text{in}}, \text{sk}^{\text{in}}) = \text{PKE}.\text{Gen}(1^{\lambda}; r_1^{\text{in}})$;
10 Compute $\text{B}^{\text{in}} = \text{PKE}.\text{Decrypt}(\text{sk}^{\text{in}}, \text{B}^{\text{in}})$;
11 Compute $(r_3^{t-1}, r_4^{t-1}) = \text{PRF}(K_E, t - 1)$;
12 Compute $(\text{pk}_{\text{st}}, \text{sk}_{\text{st}}) = \text{PKE}.\text{Gen}(1^{\lambda}; r_3^{t-1})$;
13 Compute $\text{st}^{\text{in}} = \text{PKE}.\text{Decrypt}(\text{sk}_{\text{st}}, \text{st}^{\text{in}})$;
14 if $t = i - 1$ then
15 $\text{Compute } (\text{st}^{\text{out}}, \text{I}^{\text{out}}, \text{B}^{\text{out}}) \leftarrow F_{\text{o}, \text{hyb}}^{j}(t, \text{st}^{\text{in}}, \text{I}^{\text{in}}, \text{B}^{\text{in}})$;
$\text{// } F_{\text{o}, \text{hyb}}^{j} = \text{CP-ORAM}.\text{Compile}(F, \text{HYBOACCESS}^j)$
16 else
17 Compute $(\text{st}^{\text{out}}, \text{I}^{\text{out}}, \text{B}^{\text{out}}) = F_0(t, \text{st}^{\text{in}}, \text{I}^{\text{in}}, \text{B}^{\text{in}})$;
18 Set $\text{lw}^{\text{out}} = (t, \ldots, t)$;
19 Compute $(F_1^{\text{out}}, F_2^{\text{out}}) = \text{PRF}(K_E, (\text{lw}^{\text{out}}, h(\text{I}^{\text{out}})))$;
20 Compute $(\text{pk}', \text{sk}') = \text{PKE}.\text{Gen}(1^{\lambda}; r_1^{\text{out}})$;
21 Compute $\text{B}^{\text{out}} = \text{PKE}.\text{Encrypt}(\text{pk}', \text{B}^{\text{out}}, r_2^{\text{out}})$;
22 Compute $(r_3^t, r_4^t) = \text{PRF}(K_E, t)$;
23 Compute $(\text{pk}', \text{sk}') = \text{PKE}.\text{Gen}(1^{\lambda}; r_3^t)$;
24 Compute $\text{st}^{\text{out}} = \text{PKE}.\text{Encrypt}(\text{pk}', \text{st}^{\text{out}}; r_4^t)$;
25 Output $\text{st}^{\text{out}} = (\text{st}^{\text{out}}, t + 1)$, $\tilde{\text{a}}^{\text{out}}_{h+1} = (\text{I}^{\text{out}}, (\text{B}^{\text{out}}, \text{lw}^{\text{out}}))$;
Algorithm 67: HYBOACCESS\(^j\)\(\{K_N, K_{Sim}\}\)

**Input**: \(t, d, \text{loc}, \text{val}\)

**Output**: \(old\text{val}\)

**Data**: \(K_N, K_{Sim}, \alpha, \text{MaxDepth}\) (Memory size \(S = \alpha^{\text{MaxDepth}}\))

1. if \(d \geq \text{MaxDepth}\) then
2.  \[\text{return 0;}\]
3.  \(\text{pos} \leftarrow \text{HYBOACCESS}\(^j\)(t, d + 1, \lfloor \text{loc}/\alpha \rfloor, \text{newpos});\)
4. if \((d < j)\) then
5.  \(\text{pos} \leftarrow \text{HYBOACCESS}\(^j\)(t, d + 1, \lfloor \text{loc}/\alpha \rfloor, \text{newpos});\)
6.  \(\text{I}_{\text{fetch}} \leftarrow \text{PATH}(d, \text{pos});\)
7.  \(\text{B}_{\text{fetch}} \leftarrow \text{READ}(\text{I}_{\text{fetch}});\)
8.  \(\text{WRITE}(\text{I}_{\text{fetch}}, \text{dummy});\)
9.  \(\text{pos}'' \leftarrow \text{HYBOACCESS}\(^j\)(t, d, \text{FlushR});\)
10.  \(\text{I}_{\text{flush}} \leftarrow \text{PATH}(d, \text{pos}'');\)
11.  \(\text{B}_{\text{flush}} \leftarrow \text{READ}(\text{I}_{\text{flush}});\)
12.  \(\text{WRITE}(\text{I}_{\text{flush}}, \text{dummy});\)
13.  \(\text{return};\)
14. else // identical to OACCESS
15.  \(\text{I}_{\text{fetch}} \leftarrow \text{PATH}(d, \text{pos});\) // Fetch
16.  \(\text{B}_{\text{fetch}} \leftarrow \text{READ}(\text{I}_{\text{fetch}});\)
17.  \((\text{B}_{\text{fetch}}, old\text{val}) \leftarrow \text{FETCH}\text{AND}\text{UPDATE}(\text{B}_{\text{fetch}}, \text{loc}, \text{val}, \alpha, \text{pos}, \text{newpos});\)
18.  \(\text{WRITE}(\text{I}_{\text{fetch}}, \text{B}_{\text{fetch}});\)
19.  \(\text{pos}'' \leftarrow \text{HYBOACCESS}\(^j\)(t, d, \text{FlushR});\) // Flush
20.  \(\text{I}_{\text{flush}} \leftarrow \text{PATH}(d, \text{pos}'');\)
21.  \(\text{B}_{\text{flush}} \leftarrow \text{READ}(\text{I}_{\text{flush}});\)
22.  \(\text{B}_{\text{flush}}'' \leftarrow \text{FLUSH}(\text{B}_{\text{flush}}, \text{pos}'');\)
23.  \(\text{WRITE}(\text{I}_{\text{flush}}, \text{B}_{\text{flush}}'');\)
24.  \(\text{return old\text{val}};\)
Algorithm 68: $F_e^{2,i,0',j}$

**Input**: $\tilde{\text{st}}^{\text{in}} = (\text{st}^{\text{in}}, t)$, $\tilde{a}_{k-M}^{\text{in}} = (\text{I}^{\text{in}}, (\text{B}^{\text{in}}, \text{lw}^{\text{in}}))$

**Data**: $T, K_E, t^*, y, \ K_N, K_{\text{Sim}}, i, j$

1. Compute $t = \lceil t/q_0 \rceil$;
2. If $t > t^*$, output $\text{Reject}$;
3. if $t = t^*$ then
   4. …
5. if $i \leq t < t^*$ then
   6. …
else
   8. Compute $(r_1^{\text{in}}, r_2^{\text{in}}) = \text{PRF}(K_E, (\text{lw}^{\text{in}}, h(\text{I}^{\text{in}})))$;
   9. Compute $(\text{pk}^{\text{in}}, \text{sk}^{\text{in}}) = \mathcal{PKE}.\text{Gen}(1^\lambda; r_1^{\text{in}})$;
   10. Compute $\text{B}^{\text{in}} = \mathcal{PKE}.\text{Decrypt}(\text{sk}^{\text{in}}, \text{B}^{\text{in}})$;
   11. Compute $(r_3^{t-1}, r_4^{t-1}) = \text{PRF}(K_E, t-1)$;
   12. Compute $(pk_{\text{st}}, sk_{\text{st}}) = \mathcal{PKE}.\text{Gen}(1^\lambda; r_3^{t-1})$;
   13. Compute $\text{st}^{\text{in}} = \mathcal{PKE}.\text{Decrypt}(sk_{\text{st}}, \text{st}^{\text{in}})$;
   14. if $t = i - 1$ then
      15. Compute $(\text{st}^{\text{out}}, \text{I}^{\text{out}}, \text{B}^{\text{out}}) \leftarrow F_{o,\text{hyb}}^d(t, \text{st}^{\text{in}}, \text{I}^{\text{in}}, \text{B}^{\text{in}})$;
      16. If $(d > j$ and $a = \text{Init})$, set $\text{st}^{\text{out}} = \text{dummy}$;
   17. else
      18. Compute $(\text{st}^{\text{out}}, \text{I}^{\text{out}}, \text{B}^{\text{out}}) = F_o(t, \text{st}^{\text{in}}, \text{I}^{\text{in}}, \text{B}^{\text{in}})$;
   19. Set $\text{lw}^{\text{out}} = (t, \ldots, t)$;
   20. Compute $(r_1^{\text{out}}, r_2^{\text{out}}) = \text{PRF}(K_E, (\text{lw}^{\text{out}}, h(\text{I}^{\text{out}})))$;
   21. Compute $(\text{pk}', \text{sk}') = \mathcal{PKE}.\text{Gen}(1^\lambda; r_1^{\text{out}})$;
   22. Compute $\text{B}^{\text{out}} = \mathcal{PKE}.\text{Encrypt}(\text{pk}', \text{B}^{\text{out}}; r_2^{\text{out}})$;
   23. Compute $(r_3, r_4) = \text{PRF}(K_E, t)$;
   24. Compute $(pk', sk') = \mathcal{PKE}.\text{Gen}(1^\lambda; r_3)$;
   25. Compute $\text{st}^{\text{out}} = \mathcal{PKE}.\text{Encrypt}(pk', \text{st}^{\text{out}}; r_4)$;
   26. Output $\text{st}^{\text{out}} = (\text{st}^{\text{out}}, t + 1)$, $\tilde{a}_{k-M}^{\text{out}} = (\text{I}^{\text{out}}, (\text{B}^{\text{out}}, \text{lw}^{\text{out}}))$.
B.5.4 Punctured ORAM: From $\text{Hyb}_{2,i,0,j}^{*}$ to $\text{Hyb}_{2,i,0,j+1}^{*}$

Our goal now is to show that $\text{Hyb}_{2,i,0,j}^{*}$ and $\text{Hyb}_{2,i,0,j+1}^{*}$ are indistinguishable, which amounts to switch time step $(t,d) = (i-1,j)$ from real computation to a simulated one. Suppose that at time $(t,d) = (i-1,j)$ the ORAM compiled program $F_o$ wishes to access some memory location $\text{loc}$, which points to a cell in $\text{block}^*$ (recall that the program is deterministic, so $\text{loc}$ is well-defined by the computation), it reads the position map value $\text{pos}^*$ and fetches the $\text{block}^*$ along the path $\text{pos}^*$ in the ORAM tree. We need to simulate the memory access pattern (induced by $\text{pos}^*$) and output data (including memory data and CPU state), where output data are encrypted in ciphertext and the indistinguishable simulation can be constructed by semantic security of PKE. The main challenge here is to switch $\text{pos}^*$ to a simulated path, since $\text{pos}^*$ is information theoretically determined by the previous computation and $\text{pos}^*$ must be revealed directly through memory access.

**Punctured ORAM** To simulate $\text{pos}^*$, our approach is to move to a hybrid with punctured ORAM program, where $\text{pos}^*$ is information-theoretically erased so that we can switch $\text{pos}^*$ to a simulated path. Towards this goal, let us trace closely the value $\text{pos}^*$ in the program execution. First, we observe that $\text{pos}^*$ is stored in two places in the ORAM data structure:

1. The block $\text{block}^*$ itself, which is stored somewhere in the ORAM tree.
2. The position map stored in another layer of ORAM tree recursively.

Let $t_{\text{pos}}$ be that time $\text{pos}^*$ being created by PPRF, which is also the last access time of $\text{block}^*$ before time step $i-1$. At time $t_{\text{pos}}$, the value $\text{pos}^*$ is stored in both $\text{block}^*$ in the root node and the recursive position map. Note that $t_{\text{pos}}$ can be much smaller than $i-1$.

To “information-theoretically erase” $\text{pos}^*$, we move to a hybrid program where the value $\text{pos}^*$ is not generated at time $t_{\text{pos}}$. Specifically, we define an intermediate hybrid $\text{Hyb}_{2,i,0,j,2}^{*}$ in which the program is replaced by a punctured ORAM program such that:

$$\text{Hyb}_{2,i,0,j,2}^{*}: \text{At time } t = t_{\text{pos}}, \text{do not generate the value } \text{pos}^*, \text{and instead of putting back the encryption of the fetched } \text{block}^* \text{ to the root of the ORAM tree, an encryption of empty values is put back instead }^{33}. \text{Moreover, the position map value } \text{pos}^* \text{ is not updated.}$$

In $\text{Hyb}_{2,i,0,j,2}^{*}$, the value $\text{pos}^*$ is information-theoretically hidden before time step $i-1$. Since the $\text{block}^*$ is not be accessed from time $t_{\text{pos}}$ to time $i-1$, the modification does not change the computation from time $t_{\text{pos}}$ to time $i-1$. Now, we can simulate the computation at time step $i-1$ as before, and switch $\text{pos}^*$ to a simulated value by the standard PPRF argument. After the path is switched to simulated one, we obtain $\text{Hyb}_{2,i,0,j+1}^{*}$ by un-puncturing ORAM program $F_o$ at the point $\text{pos}^*$.

We prove $\text{Hyb}_{2,i,0,j}^{*}$ and $\text{Hyb}_{2,i,0,j+1}^{*}$ are indistinguishable in Lemma B.53 with the help of puncturable ORAM, and we will later prove that punctured ORAM is computationally indistinguishable from its non-punctured ORAM counterpart in the next sub-section (Lemma B.54).

**Lemma B.53.** Let $\text{PKE}$ be an IND-CPA secure public key encryption scheme, $\text{CIO}$ be a computation-trace indistinguishability obfuscation scheme in RAM model, PRF be a secure puncturable PRF scheme. Then the hybrids $\text{Hyb}_{2,i,0,j}^{*}$ and $\text{Hyb}_{2,i,0,j+1}^{*}$ are computationally indistinguishable for all $0 \leq i \leq t^*$ and all $0 \leq j \leq d_{\text{max}}$.

**Proof.** We define three third-layer hybrids $\text{Hyb}_{2,i,0,j,1}^{*}$, $\text{Hyb}_{2,i,0,j,2}^{*}$ and $\text{Hyb}_{2,i,0,j,3}^{*}$.

---

$^{33}$ Recall in ORAM construction, a bucket is a vector with $K$ elements, where each element is either a valid block or an unique empty-slot symbol $\text{Empty} = (\bot, \bot, \bot)$. The value being put pack is in fact $\text{Empty}$ (rather than $\text{block}^*$), which also yields a consistent ORAM tree.
Table 6: Intuitions of the hybrid series from $\text{Hyb}_{2,i,0,j}$ to $\text{Hyb}_{2,i,0,j+1}$, where we focus on the simulated memory access locations as a path in the ORAM tree. Sim. stands for simulated.

<table>
<thead>
<tr>
<th></th>
<th>t = $t_{pos}$ and $d = j$</th>
<th>t = $(i - 1)$ and $d = j$</th>
<th>t = $(i - 1)$ and $d &lt; j$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{Hyb}_{2,i,0,j}$</td>
<td>Honest</td>
<td>Honest path and values</td>
<td>Sim. path, erased values</td>
</tr>
<tr>
<td>$\text{Hyb}_{2,i,0,j+1}$</td>
<td>Honest</td>
<td>Honest path, erased values</td>
<td>Sim. path, erased values</td>
</tr>
<tr>
<td>$\text{Hyb}_{2,i,0,j,2}$</td>
<td>Puncture $pos^*$</td>
<td>Hard-wired honest path, erased values</td>
<td>Sim. path, erased values</td>
</tr>
<tr>
<td>$\text{Hyb}_{2,i,0,j,3}$</td>
<td>Puncture $pos^*$</td>
<td>Sim. path, erased values</td>
<td>Sim. path, erased values</td>
</tr>
<tr>
<td>$\text{Hyb}_{2,i,0,j+1}$</td>
<td>Honest</td>
<td>Sim. path, erased values</td>
<td>Sim. path, erased values</td>
</tr>
</tbody>
</table>

$\text{Hyb}_{2,i,0,j,1}$. In this hybrid, $F$ is replaced by $F_e^{2,i,0,j,1}$ defined in Algorithm 69. $F_e^{2,i,0,j,1}$ uses $\text{HYBOACCESS}^j,1$ that is similar to $\text{HYBOACCESS}^j,1$, except that at $d = j$ all values written are replaced by dummy data. All other computation are carried out honestly and access locations $I_{\text{fetch}}$ (induced by $pos^*$) in $\text{HYBOACCESS}^j,1$ are identical to those in $\text{HYBOACCESS}^j,1$.

$\text{Hyb}_{2,i,0,j,2}$. In this hybrid, $F$ is replaced by $F_e^{2,i,0,j,2}$ defined in Algorithm 71. $F_e^{2,i,0,j,2}$ invokes different variants of $F_o$ at different $t$: $F_{o,\text{sim}}$ for $t \geq i$, $F_{o,\text{hyb}}^{2,i,0,j,2}$ for $t = i - 1$, $F_{o,\text{punct}}^{2,i,0,j,2}$ for $t = t_{pos}$, and normal $F_o$ otherwise, where
- $F_{o,\text{hyb}}^{2,i,0,j,2}$ is the ORAM compiled program using $\text{HYBOACCESS}^j,2$ that is similar to $\text{HYBOACCESS}^j,1$ except that it hard wires and uses $pos^*$ (rather than $pos$ that returned from recursive call), where $pos^*$ is the pre-computed value of $pos$ at $(t = i - 1 \land d = j)$ in an honest evaluation of $OACCESS$ (Algorithm 72).
- $F_{o,\text{punct}}^{2,i,0,j,2}$ is the punctured ORAM program using $\text{HYBOACCESS}^j,2$ that is similar to normal $OACCESS$, except that it is punctured at $t_{pos}$, which writes dummy symbol to the position map and removes block at the $j$-th recursion (Algorithm 73)
- $t_{pos}$ is the time $t$ so that $pos^*$ is generated by $\text{PRF}(K_N, (t, d, \text{flag}))$.

$\text{Hyb}_{2,i,0,j,3}$. In this hybrid, $F$ is replaced by $F_e^{2,i,0,j,3}$ defined in Algorithm 74 $F_e^{2,i,0,j,3}$ is similar to $F_e^{2,i,0,j,2}$, except that it uses $\text{HYBOACCESS}^j+1$ at $t = i - 1$.

Analysis. In the remaining of this subsection, we will complete the proof of the lemma.

From $\text{Hyb}_{2,i,0,j}$ to $\text{Hyb}_{2,i,0,j,1}$: Note that in $F_e^{2,i,0,j}$, the entire computation for $i \leq t \leq t^*$ is simulated, and when $t > t^*$, $F_e^{2,i,0,j}$ always output Reject. It will thus never be the case that, at time $t > i - 1$, the program decrypts the ciphertext written at $(i - 1, j, \text{flag})$ where flag = $\text{FetchW}$ or $\text{FlushW}$. We can therefore replace the ciphertexts output in the fetch and flush phase by the encryption of dummy, and replace the flush positions by a simulated version.

Formally, indistinguishability is established via the following hybrids:

1. In the first hybrid, we puncture the input $(i - 1, j, \text{FlushR})$ for PRF keys $K_N$ and $K_\text{Sim}$, and the input $(i - 1, j, \text{flag})$ where flag = $\text{FetchW}$ and $\text{FlushW}$ for PRF keys $K_E$. We hardwire the pseudorandomness computed from $K_N$, $K_\text{Sim}$ and $K_E$. Since the computation defined by the program has identical computation trace as that in the previous hybrid, indistinguishability is guaranteed by Theorem 6.2.

\[34\text{REMOVE BLOCK}(B, \text{loc}, \alpha, pos)\] searches for the tuple of block = $(|loc/\alpha|, pos, data)$ in each bucket $\in B$. It outputs $B^-$ with block being removed.
2. In the next hybrid, we replace the pseudorandomness by truly random numbers. Indistinguishability is guaranteed by the security of the puncturable PRF.

3. Then, we hardwire \( B_{\text{out}} \) and \( I_{\text{flush}} \), which are generated by the true randomness in the previous hybrid, into the program and take away the hardwired true randomness. Since the computation defined by the program has identical computation trace as that in the previous hybrid, indistinguishability is guaranteed by Theorem 6.2.

4. Next, we replace the values to be written by dummy. Indistinguishability is guaranteed by the IND-CPA security of \( \mathcal{PKE} \) because these values are encrypted and \( F_e^{2,i,0,j,1} \) would never decrypt the ciphertext with the private key.

5. We replace \( I_{\text{flush}} \) by a simulated version, which is generated from the hardwired true randomness that corresponds to \( K_{\text{Sim}} \). Indistinguishability is guaranteed by the selective security of the puncturable PRF.

6. Finally, we un-puncture the PRF keys \( K_N, K_{\text{Sim}} \) and \( K_E \) to obtain the required hybrid. Indistinguishability is again guaranteed by the security of the puncturable PRF.

From Hyb\(_{2,i,0,j,1} \) to Hyb\(_{2,i,0,j,2} \): We defer the discussion to Lemma B.54.

From Hyb\(_{2,i,0,j,2} \) to Hyb\(_{2,i,0,j,3} \): In \( F_e^{2,i,0,j,2} \), since our ORAM program has punctured \( pos^* \) that generated at time \( (t_{\text{pos}}, j) \) and \( pos^* \) is only used at time \( (i - 1, j) \), we can use \( \text{HYBOACCESS}^{j+1} \) instead of \( \text{HYBOACCESS}^{j,2} \) by selective security of PPRF and Theorem 6.2.

Formally, indistinguishability is established via the following hybrids:

1. In the first hybrid, we use punctured PRF keys \( K_N\{(t_{\text{pos}}, j, \text{FetchR})\} \) and \( K_{\text{Sim}}\{i - 1, j, \text{FetchR}\} \). We do not use \( K_{\text{Sim}} \) at \( (i - 1, j, \text{FetchR}) \) in this step, and the only value relies on the \( K_N \) at \( (t_{\text{pos}}, j, \text{FetchR}) \) is \( pos^* \), which is already hardwired. Since the program has identical computation trace as that in the previous hybrid, indistinguishability is guaranteed by Theorem 6.2.

2. In the next hybrid, we replace hardwired value \( pos^* \) (generated from \( K_N\{(t_{\text{pos}}, j, \text{FetchR})\} \)) with \( pos^{**} \), which is the random ORAM position computed from a true randomness. Indistinguishability is guaranteed by the selective security of PPRF.

3. Then, we replace hardwired value \( pos^{**} \) with \( pos_{\text{Sim}}^* \), which is generated by randomness computed by \( \text{PRF}(K_{\text{Sim}}, (i - 1, j, \text{FetchR})) \). Indistinguishability is guaranteed by the selective security of PPRF.

4. Finally, we un-puncture the PRF keys \( K_N, K_{\text{Sim}} \) to obtain the required hybrid. Since the program has identical computation trace as that in the previous hybrid, indistinguishability is guaranteed by Theorem 6.2.

From Hyb\(_{2,i,0,j,3} \) to Hyb\(_{2,i,0,j+1} \): The proof is similar to that of Lemma B.54.
Algorithm 69: $F_e^{2,i,0,j,1}$

**Input**: $\tilde{\text{st}}^{\text{in}} = (\text{st}^{\text{in}}, t)$, $\tilde{a}_{\text{Hyb}}^{\text{in}} = (\text{I}^{\text{in}}, (\text{B}^{\text{in}}, \text{lw}^{\text{in}}))$

**Data**: $T, K_E, t^*, y$, $K_N, K_{\text{Sim}}, i, j$

1. Compute $t = \lceil t/q_0 \rceil$;
2. If $t > t^*$, output Reject;
3. If $t = t^*$ then
   4. $\ldots$
5. If $i \leq t < t^*$ then
   6. $\ldots$
else
   8. Compute $(t_1^{\text{in}}, r_2^{\text{in}}) = \text{PRF}(K_E, (\text{lw}^{\text{in}}, h(\text{I}^{\text{in}})))$;
   9. Compute $(\text{pk}^{\text{in}}, \text{sk}^{\text{in}}) = \mathcal{PK}E.\text{Gen}(1^\lambda; r_1^{\text{in}})$;
10. Compute $\text{B}^{\text{in}} = \mathcal{PK}E.\text{Decrypt}(\text{sk}^{\text{in}}, \text{B}^{\text{in}})$;
11. Compute $(r_3^{t-1}, r_4^{t-1}) = \text{PRF}(K_E, t - 1)$;
12. Compute $(\text{pk}_{\text{st}}, \text{sk}_{\text{st}}) = \mathcal{PK}E.\text{Gen}(1^\lambda; r_3^{t-1})$;
13. Compute $\text{st}^{\text{in}} = \mathcal{PK}E.\text{Decrypt}(\text{sk}_{\text{st}}, \text{st}^{\text{in}})$;
14. If $t = i - 1$ then
   15. Compute $(\text{st}^{\text{out}}, \text{I}^{\text{out}}, \text{B}^{\text{out}}) \leftarrow F_{o,\text{Hyb}}^{j,1}(t, \text{st}^{\text{in}}, \text{I}^{\text{in}}, \text{B}^{\text{in}})$;
      // $F_{o,\text{Hyb}}^{j,1} = \text{CP-ORAM.\text{Compile}}(F, \text{HYBOACCESS}^{j,1})$
   16. else
      17. Compute $(\text{st}^{\text{out}}, \text{I}^{\text{out}}, \text{B}^{\text{out}}) = F_o(t, \text{st}^{\text{in}}, \text{I}^{\text{in}}, \text{B}^{\text{in}})$;
   18. Set $\text{lw}^{\text{out}} = (t, \ldots, t)$;
   19. Compute $(r_1^{\text{out}}, r_2^{\text{out}}) = \text{PRF}(K_E, (\text{lw}^{\text{out}}, h(\text{I}^{\text{out}})))$;
   20. Compute $(\text{pk}', \text{sk}') = \mathcal{PK}E.\text{Gen}(1^\lambda; r_1^{\text{out}})$;
   21. Compute $\text{B}^{\text{out}} = \mathcal{PK}E.\text{Encrypt}(\text{pk}', \text{B}^{\text{out}}; r_2^{\text{out}})$;
   22. Compute $(r_3^t, r_4^t) = \text{PRF}(K_E, t)$;
   23. Compute $(pk', sk') = \mathcal{PK}E.\text{Gen}(1^\lambda; r_3^t)$;
   24. Compute $\text{st}^{\text{out}} = \mathcal{PK}E.\text{Encrypt}(pk', \text{st}^{\text{out}}; r_4^t)$;
25. Output $\text{st}^{\text{out}} = (\text{st}^{\text{out}}, t + 1)$, $\tilde{a}_{\text{Hyb}}^{\text{out}} = (\text{I}^{\text{out}}, (\text{B}^{\text{out}}, \text{lw}^{\text{out}}))$.
Algorithm 70: HYBOACCESS$^2$\{\(K_N, K_{Sim}\)\}

Input: \(t, d, \text{loc}, \text{val}\)
Output: \(oldval\)
Data: \(K_N, K_{Sim}, \alpha, \text{MaxDepth}\) (Memory size \(S = \alpha^\text{MaxDepth}\))

1 if \(d \geq \text{MaxDepth}\) then
   2 return 0;
3 Pick leaf \(\text{newpos}\) at recursion level \(d\) based on \(\text{PRF}(K_N, (t, d, \text{FetchR}))\); \hfill // Update position map
4 \(\text{pos} \leftarrow \text{HYBOACCESS}^2\{t, d + 1, \lfloor \text{loc}/\alpha \rfloor, \text{newpos}\}\);
5 if \((d < j)\) then
   6 Pick leaf \(\text{pos}\) at recursion level \(d\) based on \(\text{PRF}(K_{Sim}, (t, d, \text{FetchR}))\);
   7 \(\text{I}_{\text{fetch}} \leftarrow \text{PATH}(d, \text{pos})\);
   8 \(\text{B}_{\text{fetch}} \leftarrow \text{READ}(\text{I}_{\text{fetch}})\);
   9 WRITE(\(\text{I}_{\text{fetch}}, \text{dummy}\));
   10 Pick leaf \(\text{pos}'\) at recursion level \(d\) based on \(\text{PRF}(K_{Sim}, (t, d, \text{FlushR}))\);
   11 \(\text{I}_{\text{flush}} \leftarrow \text{PATH}(d, \text{pos}')\);
   12 \(\text{B}_{\text{flush}} \leftarrow \text{READ}(\text{I}_{\text{flush}})\);
   13 WRITE(\(\text{I}_{\text{flush}}, \text{dummy}\));
   14 return;
15 else
   16 \(\text{I}_{\text{fetch}} \leftarrow \text{PATH}(d, \text{pos})\); \hfill // Fetch
   17 \(\text{B}_{\text{fetch}} \leftarrow \text{READ}(\text{I}_{\text{fetch}})\);
   18 if \((d = j)\) then
      19 WRITE(\(\text{I}_{\text{fetch}}, \text{dummy}\));
      20 Pick leaf \(\text{pos}'\) at recursion level \(d\) based on \(\text{PRF}(K_{Sim}, (t, d, \text{FlushR}))\);
      21 \(\text{I}_{\text{flush}} \leftarrow \text{PATH}(d, \text{pos}')\);
      22 \(\text{B}_{\text{flush}} \leftarrow \text{READ}(\text{I}_{\text{flush}})\);
      23 WRITE(\(\text{I}_{\text{flush}}, \text{dummy}\));
      24 return;
   25 else
      26 \((\text{B}_{\text{out}}, \text{oldval}) \leftarrow \text{FETCHANDUPDATE}(\text{B}_{\text{fetch}}, \text{loc}, \text{val}, \alpha, \text{pos}, \text{newpos})\);
      27 WRITE(\(\text{I}_{\text{fetch}}, \text{B}_{\text{out}}\));
      28 Pick leaf \(\text{pos}'\) at recursion level \(d\) based on \(\text{PRF}(K_N, (t, d, \text{FlushR}))\); \hfill //Flush
      29 \(\text{I}_{\text{flush}} \leftarrow \text{PATH}(d, \text{pos}')\);
      30 \(\text{B}_{\text{flush}} \leftarrow \text{READ}(\text{I}_{\text{flush}})\);
      31 \(\text{B}_{\text{out}} \leftarrow \text{FLUSH}(\text{B}_{\text{flush}}, \text{pos}')\);
      32 WRITE(\(\text{I}_{\text{flush}}, \text{B}_{\text{out}}\));
      33 return \(\text{oldval}\);
Algorithm 71: $F_e^{2,i,0,j,2}$

Input: $\mathbf{s}_t^{\text{in}} = ((\mathbf{s}_t^{\text{in}}), t)$, $\tilde{\mathbf{a}}_{k+n}^{\text{in}} = (\mathbf{I}_t^{\text{in}}, (\mathbf{B}_t^{\text{in}}, \mathbf{l}w^{\text{in}}))$

Data: $T, K_E, t^*, y, K_N, K_{\text{Sim}}, i, j$

1. Compute $t = \lfloor t/g_0 \rfloor$;
2. If $t > t^*$, output Reject;
3. If $t = t^*$ then
   4. $\ldots$
5. If $i \leq t < t^*$ then
   6. $\ldots$
7. else
   8. Compute $(r_1^{\text{in}}, r_2^{\text{in}}) = \text{PRF}(K_E, (\mathbf{l}w^{\text{in}}, h(\mathbf{I}_t^{\text{in}})))$;
   9. Compute $(\mathbf{pk}_t^{\text{in}}, \mathbf{sk}_t^{\text{in}}) = \mathcal{PKE}.\text{Gen}(1^\lambda; r_1^{\text{in}})$;
10. Compute $\mathbf{B} = \mathcal{PKE}.\text{Decrypt}(\mathbf{sk}_t^{\text{in}}, \mathbf{B}_t^{\text{in}})$;
11. Compute $(r_3^{t-1}, r_4^{t-1}) = \text{PRF}(K_E, t - 1)$;
12. Compute $(\mathbf{pk}_{st}^{\text{in}}, \mathbf{sk}_{st}^{\text{in}}) = \mathcal{PKE}.\text{Gen}(1^\lambda; r_1^{t-1})$;
13. Compute $\mathbf{s}_t^{\text{in}} = \mathcal{PKE}.\text{Decrypt}(\mathbf{sk}_{st}^{\text{in}}, \mathbf{st}^{\text{in}})$;
14. if $t = i - 1$ then
   15. Compute $(\mathbf{st}_t^{\text{out}}, \mathbf{I}_t^{\text{out}}, \mathbf{B}_t^{\text{out}}) \leftarrow F_{o,hyb}^{2,i,2}(t, \mathbf{s}_t^{\text{in}}, \mathbf{I}_t^{\text{in}}, \mathbf{B}_t^{\text{in}})$;
   16. else if $t = t_{\text{pos}}$ then
17. Compute $(\mathbf{st}_t^{\text{out}}, \mathbf{I}_t^{\text{out}}, \mathbf{B}_t^{\text{out}}) = F_{o,punct}^{2,i,2}(t, \mathbf{st}^{\text{in}}, \mathbf{I}_t^{\text{in}}, \mathbf{B}_t^{\text{in}})$;
18. else
19. Compute $(\mathbf{st}_t^{\text{out}}, \mathbf{I}_t^{\text{out}}, \mathbf{B}_t^{\text{out}}) = F_{o}(t, \mathbf{st}^{\text{in}}, \mathbf{I}_t^{\text{in}}, \mathbf{B}_t^{\text{in}})$;
20. Set $\mathbf{l}w_{\text{out}} = (t, \ldots, t)$;
21. Compute $(r_{1t}^{\text{out}}, r_{2t}^{\text{out}}) = \text{PRF}(K_E, (\mathbf{l}w_{\text{out}}, h(\mathbf{I}_t^{\text{out}})))$;
22. Compute $(\mathbf{pk}_t^{\prime}, \mathbf{sk}_t^{\prime}) = \mathcal{PKE}.\text{Gen}(1^\lambda; r_1^{t+1})$;
23. Compute $\mathbf{B}_t^{\text{out}} = \mathcal{PKE}.\text{Encrypt}(\mathbf{pk}_t^{\prime}, \mathbf{B}_t^{\text{out}}, r_{2t}^{\text{out}})$;
24. Compute $(r_3^{t}, r_4^{t}) = \text{PRF}(K_E, t)$;
25. Compute $(\mathbf{pk}_t^{\prime}, \mathbf{sk}_t^{\prime}) = \mathcal{PKE}.\text{Gen}(1^\lambda; r_3^{t})$;
26. Compute $\mathbf{st}_t^{\text{out}} = \mathcal{PKE}.\text{Encrypt}(\mathbf{pk}_t^{\prime}, \mathbf{st}_t^{\text{out}}, r_4^{t})$;
27. Output $\mathbf{st}_t^{\text{out}} = ((\mathbf{st}_t^{\text{out}}, t +1), \mathbf{a}_{B_{t+1}}^{\text{out}} = ((\mathbf{B}_t^{\text{out}}, \mathbf{l}w_{\text{out}})))$;
Algorithm 72: HYBOACCESS^j,2\{K_N, K\_Sim\}

**Input**: t, d, loc, val

**Output**: oldval

**Data**: K_N, K\_Sim, α, MaxDepth (Memory size S = α^{MaxDepth}, pos*)

1. if d ≥ MaxDepth then
   - return 0;

2. Pick leaf newpos at recursion level d based on PRF(K_N, (t, d, FetchR)); // Update position map
3. pos ← HYBOACCESS^j,2(t, d + 1, [loc/α], newpos, K\_Sim);

4. if (d < j) then
   - Pick leaf pos at recursion level d based on PRF(K\_Sim, (t, d, FetchR));
   - I\_fetch ← PATH(d, pos);
   - B\_fetch ← READ(I\_fetch);
   - WRITE(I\_fetch, dummy);
   - Pick leaf pos'' at recursion level d based on PRF(K\_Sim, (t, d, FlushR));
   - I\_flush ← PATH(d, pos'');
   - B\_flush ← READ(I\_flush);
   - WRITE(I\_flush, dummy);
   - return;

5. if (d = j) then
   - I\_fetch ← PATH(d, pos*);
   - B\_fetch ← READ(I\_fetch);
   - WRITE(I\_fetch, dummy);
   - Pick leaf pos'' at recursion level d based on PRF(K\_Sim, (t, d, FlushR));
   - I\_flush ← PATH(d, pos'');
   - B\_flush ← READ(I\_flush);
   - WRITE(I\_flush, dummy);
   - return;

6. else
   - I\_fetch ← PATH(d, pos);
   - B\_fetch ← READ(I\_fetch);
   - (B\_\_out, oldval) ← FETCH\_AND\_UPDATE(B\_fetch, loc, val, α, pos, newpos);
   - WRITE(I\_fetch, B\_\_out);
   - Pick leaf pos'' at recursion level d based on PRF(K_N, (t, d, FlushR)); // Flush
   - I\_flush ← PATH(d, pos'');
   - B\_flush ← READ(I\_flush);
   - B\_\_out ← FLUSH(B\_\_flush, pos'');
   - WRITE(I\_flush, B\_\_out);
   - return oldval;
Algorithm 73: \textsc{HybOAccess}^{\text{punct}}\{K_N\}

\begin{verbatim}
Input : t, d, loc, val
Output: oldval
Data: K_N, \alpha, \text{MaxDepth} (Memory size S = \alpha^{\text{MaxDepth}}, \text{loc}_{i,j})
1 if d \geq \text{MaxDepth} then
   2 return 0
3 if (d = j) then
   4 pos ← \textsc{HybOAccess}^{\text{punct}}(d + 1, \lfloor \text{loc}/\alpha \rfloor, \text{dummy});
else
   6 Pick leaf newpos at recursion level d based on PRF(K_N, (t, d, \text{FetchR}));
   7 pos ← \textsc{HybOAccess}^{\text{punct}}(d + 1, \lfloor \text{loc}/\alpha \rfloor, newpos);
   8 I_{\text{fetch}} ← \textsc{Path}(d, \text{pos});
   9 B_{\text{fetch}} ← \textsc{Read}(I_{\text{fetch}});
10 if (d = j) then
   11 (B_{\text{fetch},-}, oldval) ← \text{REMOVEBLOCK}(B_{\text{fetch}}, \text{loc}, \alpha, \text{pos});
   12 WRITE(I_{\text{fetch}}, B_{\text{fetch},-});
else
   14 (B_{\text{out},-}, oldval) ← \textsc{FETCHANDUPDATE}(B_{\text{fetch}}, \text{loc}, \text{val}, \alpha, \text{pos}, newpos);
   15 WRITE(I_{\text{fetch}}, B_{\text{out},-});
16 Pick leaf pos'' at recursion level d based on PRF(K_N, (t, d, \text{FlushR}));
17 I_{\text{flush}} ← \textsc{Path}(d, pos'');
18 B_{\text{flush}} ← \textsc{Read}(I_{\text{flush}});
19 B_{\text{out}} ← \textsc{FLUSH}(B_{\text{flush}, pos''});
20 WRITE(I_{\text{flush}}, B_{\text{out}});
return \text{oldval};
\end{verbatim}
Algorithm 74: $F^{2,i,0,j,3}_{e}$

**Input**: $\tilde{st}^\text{in} = (\tilde{st}^\text{in}, t)$, $\tilde{a}_{K}\rightarrow st^\text{in} = (I^\text{in}, (B^\text{in}, lw^\text{in}))$

**Data**: $T, K_E, t^*, y, K_N, K_{Sim}, i, j$

1. Compute $t = \lceil t/qo \rceil$;
2. If $t > t^*$, output $\text{Reject}$;
3. If $t = t^*$ then
   4. ...
5. If $i \leq t < t^*$ then
   6. ...
7. else
   8. Compute $(r^{in}_1, r^{in}_2) = \text{PRF}(K_E, (lw^\text{in}, h(I^\text{in})))$;
   9. Compute $(pk^{in}, sk^{in}) = \mathcal{PKE}.Gen(1^\lambda; r^{in}_1)$;
   10. Compute $B^{in} = \mathcal{PKE}. Decrypt(sk^{in}, B^{in})$;
   11. Compute $(r^{t-1}_3, r^{t-1}_4) = \text{PRF}(K_E, t - 1)$;
   12. Compute $(pk_{st}, sk_{st}) = \mathcal{PKE}.Gen(1^\lambda; r^{t-1}_3)$;
   13. Compute $st^{in} = \mathcal{PKE}. Decrypt(sk_{st}, st^{in})$;
   14. if $t = i - 1$ then
      15. Compute $(st^{out}, I^{out}, B^{out}) \leftarrow F^{j+1}_{o,hyb}(t, st^{in}, I^{in}, B^{in})$;
   else if $t = t^\text{pos}$ then
      17. Compute $(st^{out}, I^{out}, B^{out}) = F^{j^\text{punct}}(t, st^{in}, I^{in}, B^{in})$;
   else
      19. Compute $(st^{out}, I^{out}, B^{out}) = F_{o}(t, st^{in}, I^{in}, B^{in})$;
   20. Set $lw^{\text{out}} = (t, \ldots, t)$;
   21. Compute $(r^{out}_1, r^{out}_2) = \text{PRF}(K_E, (lw^{\text{out}}, h(I^{\text{out}})))$;
   22. Compute $(pk', sk') = \mathcal{PKE}.Gen(1^\lambda; r^{out}_1)$;
   23. Compute $B^{out} = \mathcal{PKE}. Encrypt(pk', B^{out}; r^{out}_2)$;
   24. Compute $(r^3, r^4) = \text{PRF}(K_E, t)$;
   25. Compute $(pk', sk') = \mathcal{PKE}.Gen(1^\lambda; r^3)$;
   26. Compute $st^{out} = \mathcal{PKE}. Encrypt(pk', st^{out}; r^4)$;
27. Output $\tilde{st}^{out} = (st^{out}, t + 1), \tilde{a}_{K}\rightarrow st^{out} = (I^{out}, (B^{out}, lw^{out}))$. 

153
B.5.5 Partially Punctured ORAM: From Hyb\textsubscript{2,i,0,j,1} to Hyb\textsubscript{2,i,0,j,2}

Before giving the proof details that the hybrids \textbf{Hyb}\textsubscript{2,i,0,j,1} and \textbf{Hyb}\textsubscript{2,i,0,j,2} are indistinguishable, we provide first the main proof ideas. Recall that in an ORAM tree, a node (as a bucket) consists of multiple blocks of bit string. In the following, let \textit{block}\textsuperscript{*} be the block to be fetched at time \((t, d) = (i - 1, j)\), and \textit{pos}\textsuperscript{*} be the corresponding position of \textit{block}\textsuperscript{*}. We let \(t\text{\textsubscript{pos}}\) denote the time when \textit{pos}\textsuperscript{*} is generated by PPRF; note that \(t\text{\textsubscript{pos}}\) is also the last modification time of \textit{block}\textsuperscript{*}.

Now, how do we move from \textbf{Hyb}\textsubscript{2,i,0,j,1} to \textbf{Hyb}\textsubscript{2,i,0,j,2}, or how do we puncture ORAM compiled next-step program \(F_k^2\)? Our main idea is to erase \textit{block}\textsuperscript{*} and \textit{pos}\textsuperscript{*} value in memory and CPU state from time \(t = t\text{\textsubscript{pos}}\) to time \(t = i - 1\). To simplify the exposition, let us focus on erasing \textit{block}\textsuperscript{*}, and we note that the \textit{pos}\textsuperscript{*} (which is written to ORAM recursively) can be handled analogously. In other words, consider the following simplified goal:

\textbf{Hyb}\textsubscript{2,i,0,j,1′,\textsubscript{tpos}}: (A) At time \(t\text{\textsubscript{pos}}\), instead of putting back the encryption of the fetched \textit{block}\textsuperscript{*} to the root of the ORAM tree, an encryption of dummy value is put back instead.

From \textbf{Hyb}\textsubscript{2,i,0,j,1} to \textbf{Hyb}\textsubscript{2,i,0,j,1′,\textsubscript{tpos}}, we wish to change the step computation at time \(t = t\text{\textsubscript{pos}}\) to \(F_k^2\text{\textsubscript{punct}}\). This step is non-trivial for the following reason: although \textit{block}\textsuperscript{*} to be fetched at \((t, d) = (i - 1, j)\) is encrypted, we cannot leverage its semantic security since the PRF key \(K_E\) used to generate the ciphertext is hardwired in the program, and the security of CiO does not hide these hardwired values. In particular, \textit{block}\textsuperscript{*} might not be in Fetch step or be moved to another node in Flush step from time \(t = t\text{\textsubscript{pos}}\) to time \(t = i - 1\), where both steps must first decrypt all memory input with the private key, which is generated from \(K_E\). Specifically, following cases need to decrypt (and re-encrypt) \textit{block}\textsuperscript{*}:

- Fetch step searches for another block, and \textit{block}\textsuperscript{*} is on the searching path. Because \textit{block}\textsuperscript{*} is not matched, it is decrypted and re-encrypted in the same bucket.
- Flush step flushes the path \textit{pos}\textsuperscript{0}, and \textit{block}\textsuperscript{*} is not moved. Similar to Fetch, \textit{block}\textsuperscript{*} is decrypted and re-encrypted in the same bucket.
- Flush step flushes the path \textit{pos}\textsuperscript{0′}, and \textit{block}\textsuperscript{*} is moved from one bucket to another bucket. \textit{block}\textsuperscript{*} is decrypted and then re-encrypted in two different buckets.

Therefore, in the worst case, the adversary actually has knowledge of the position \textit{pos}\textsuperscript{*} to be fetched, the access pattern at this point is actually deterministic and hence cannot be simulated.

In order to argue that we can indeed switch to \textbf{Hyb}\textsubscript{2,i,0,j,1′,\textsubscript{tpos}}, the trivial approach is to hardwire input of the next time \(t\text{\textsubscript{pos}}\) that decrypts \textit{block}\textsuperscript{*}, but there might exist another next time of \(t\text{\textsubscript{pos}}\) that decrypts \textit{block}\textsuperscript{*}, and so on. This would mean that we need to hardwire \(\Omega(T)\) information inside the program, making the construction not time-succinct. Instead, we will show, via the series of hybrids presented below, that we can erase the corresponding part of the ciphertexts after another, while having only constant amount of information hardwired in every hybrid.

**Partially Punctured Hybrids** Our key idea to do so is to add one \textit{partially puncturing} procedure (B) code to the ORAM program as a helper, which hardwires the \textit{block}\textsuperscript{*} in plaintext and “erase” it whenever this block is decrypted in the memory accesses from time \(t = t\text{\textsubscript{pos}}\) to time \(t = i - 1\).

\textbf{Hyb}\textsubscript{2,i,0,j,1′,\textsubscript{tpos}+1}; (A) At time \(t\text{\textsubscript{pos}}\), instead of putting back the encryption of the fetched \textit{block}\textsuperscript{*} to the root of the ORAM tree, an encryption of dummy value is put back instead.

(B) At time \(t \geq t\text{\textsubscript{pos}} + 1\), if the input state or memory contains \textit{block}\textsuperscript{*}, then replace it by dummy value before performing the computation.

Since we do not put back \textit{block}\textsuperscript{*} at time \(t\text{\textsubscript{pos}}\), \textit{block}\textsuperscript{*} does not exist after time \(t\text{\textsubscript{pos}}\), and thus the (B) code is never executed. Therefore, the programs in \textbf{Hyb}\textsubscript{2,i,0,j,1′,\textsubscript{tpos}} and \textbf{Hyb}\textsubscript{2,i,0,j,1′,\textsubscript{tpos}+1} have identical computation trace,
and the two hybrids are indistinguishable by the security of CiO. So, our goal reduces to move from $\text{Hyb}_{2,i,0,j,1}$ to $\text{Hyb}_{2,i,0,j,1',t_{pos}+1}$.

Towards this, we will first remove the (A) code and add the (B) code only, and we will argue they are indistinguishable by IND-CPA security later. Next, we add the (B) code gradually and parametrize the (B) code by its time step condition, and consider hybrids $\text{Hyb}_{2,i,0,j,1,z}$ with only the (B) code added:

$$\text{Hyb}_{2,i,0,j,1,z}: (B) \text{ At time } t \geq z, \text{ if the input state or memory contains } \text{block}^*, \text{ then replace it by dummy value before performing the computation.}$$

Note that when $z = i - 1$, the (B) code is ineffective, since computation at time step $i - 1$ is already simulated. Thus, $\text{Hyb}_{2,i,0,j,1}$ and $\text{Hyb}_{2,i,0,j,1,i-1}$ are indistinguishable by CiO security.

We next argue indistinguishability of $\text{Hyb}_{2,i,0,j,1,z}$ and $\text{Hyb}_{2,i,0,j,1,z-1}$, where the difference is at time step $z - 1$. If the input at time step $z - 1$ does not contain $\text{block}^*$, then the computation trace is identical and the hybrids are indistinguishable by CiO security. Now, if the input at time step $z - 1$ contains $\text{block}^*$, the key observation here is that since we have the (B) code added for time step $t \geq z$, when we modify the $[\text{block}^*]^{out}$ at time $z - 1$ to dummy value, it does not affect the computation after any time $z$. Therefore, to show that $\text{Hyb}_{2,i,0,j,1,z}$ and $\text{Hyb}_{2,i,0,j,1,z-1}$ are indistinguishable, we need to replace the (encrypted) $[\text{block}^*]^{out}$ in $\text{Hyb}_{2,i,0,j,1,z-1}$ by (encryption of) dummy value. We hardwire the plaintext and ciphertext at time $z - 1$, and this allows us to replace the (encrypted) $[\text{block}^*]^{out}$ by (encryption of) dummy value with PPRF and PKE security.

Now, we have erased $\text{block}^*$ from the output at time $t = z - 1$, but $\text{Hyb}_{2,i,0,j,1,z-1}$ is to erase $\text{block}^*$ from the input. Intuitively, any computation step from time $t = t_{pos}$ to time $t = i - 1$ does not “compute” on $\text{block}^*$, and $\text{block}^*$ is transferred literally from input to output through $F_o$. We claim the overall output at time $t = z - 1$ are always identical by analyzing following cases in CP ORAM:

- In Fetch step, $\text{block}^*$ is always in the same bucket, and it implies that erasing $\text{block}^*$ from input and erasing $\text{block}^*$ from output are identical.
- In Flush step, if $\text{block}^*$ is not moved, then erasing $\text{block}^*$ from input and erasing $\text{block}^*$ from output are identical.
- In Flush step, if $\text{block}^*$ is on the flushing path and is moved from one bucket to another bucket, then erasing input buckets and erasing output buckets yield the identical result, where both buckets have no $\text{block}^*$.

Note this “commute property of erasure” is implied by CP ORAM construction and definition of $\text{block}^*$ and $t_{pos}$.

What we have done allow us to move from $\text{Hyb}_{2,i,0,j,1}$ to $\text{Hyb}_{2,i,0,j,1,t_{pos}+1}$, which has the partially puncturing procedure injected. The difference between $\text{Hyb}_{2,i,0,j,1,t_{pos}+1}$ and $\text{Hyb}_{2,i,0,j,1',t_{pos}+1}$ is the (A) code, which is to replace the (encrypted) $[\text{block}^*]^{out}$ at time step $t_{pos}$ by (encryption of) dummy value (with the helper (B) code added). This is the same task as above, and can be handled by the same hybrids.

Lemma B.54. Let $\text{PKE}$ be an IND-CPA secure public key encryption scheme, CiO be a computation-trace indistinguishability obfuscation scheme in RAM model, PRF be a secure puncturable PRF scheme. Then the hybrids $\text{Hyb}_{2,i,0,j,1}$ and $\text{Hyb}_{2,i,0,j,2}$ are computationally indistinguishable.

Proof. Formally, we define fourth-layer hybrids $\text{Hyb}_{2,i,0,j,1,z}$ for $t_{pos} < z \leq i - 1$, $\text{Hyb}_{2,i,0,j,1',z}$ for $t_{pos} < z \leq i - 1$, $\text{Hyb}_{2,i,0,j,1,t_{pos}+1}$ for $t_{pos} < z \leq i - 1$ and hybrids are proceeded as follows.

- $\text{Hyb}_{2,i,0,j,1} \approx \text{Hyb}_{2,i,0,j,1,i-1} \approx \ldots \approx \text{Hyb}_{2,i,0,j,1,z} \approx \text{Hyb}_{2,i,0,j,1,t_{pos}+1} \approx \text{Hyb}_{2,i,0,j,1',t_{pos}+1} \approx \text{Hyb}_{2,i,0,j,1',t_{pos}} \approx \ldots \approx \text{Hyb}_{2,i,0,j,2}$
- $\text{Hyb}_{2,i,0,j,1,z} \approx \text{Hyb}_{2,i,0,j,1',z} \approx \text{Hyb}_{2,i,0,j,1,z-1}$

Some additional notations used in $\text{Hyb}_{2,i,0,j,1',z}$ is listed in Table 8.
Table 7: The hybrid series from $\text{Hyb}_{2,i,0,j,1}$ to $\text{Hyb}_{2,i,0,j,1',t_{pos}'}$, then to $\text{Hyb}_{2,i,0,j,2}$, with the important instructions in the next-step program that are related to the erasure of $block^*$ in the ORAM tree.

<table>
<thead>
<tr>
<th>Hybrid</th>
<th>$t_{pos}$</th>
<th>$z - 1$</th>
<th>$z$</th>
<th>If decrypts $z - 1$</th>
<th>$i - 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{Hyb}_{2,i,0,j,1}$</td>
<td>honest</td>
<td>honest</td>
<td>honest</td>
<td>honest</td>
<td>honest, pos*,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>simulated data</td>
</tr>
<tr>
<td>$\text{Hyb}_{2,i,0,j,1,1}$</td>
<td>honest</td>
<td>honest</td>
<td>honest</td>
<td>honest</td>
<td>hardwire pos*,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>simulated data</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\text{Hyb}_{2,i,0,j,1,z}$</td>
<td>honest</td>
<td>honest</td>
<td></td>
<td>erase $[block^*]_{in}$</td>
<td>hardwire pos*,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>erase $[block^*]_{in}$</td>
<td>simulated data</td>
</tr>
<tr>
<td>$\text{Hyb}_{2,i,0,j,1',z}$</td>
<td>honest</td>
<td></td>
<td></td>
<td>hardwire $[block^*]_{out}$</td>
<td>hardwire pos*,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$[block^*]_{in}$</td>
<td>simulated data</td>
</tr>
<tr>
<td>$\text{Hyb}_{2,i,0,j,1'',z}$</td>
<td>honest</td>
<td></td>
<td></td>
<td>hardwire $[block^*]_{out}$</td>
<td>hardwire pos*,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>erase $[block^*]_{in}$</td>
<td>simulated data</td>
</tr>
<tr>
<td>$\text{Hyb}_{2,i,0,j,1,z-1}$</td>
<td>honest</td>
<td></td>
<td></td>
<td>erase $[block^*]_{in}$</td>
<td>hardwire pos*,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>erase $[block^*]_{in}$</td>
<td>simulated data</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\text{Hyb}<em>{2,i,0,j,1'',t</em>{pos}+1}$</td>
<td>hardwire $[block^*]_{out}$</td>
<td>erase $[block^*]_{in}$</td>
<td>erase $[block^*]_{in}$</td>
<td>hardwire pos*,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$[block^*]_{in}$</td>
<td>simulated data</td>
</tr>
<tr>
<td>$\text{Hyb}<em>{2,i,0,j,1',t</em>{pos}}$</td>
<td>$[block^*]_{out}$</td>
<td>honest</td>
<td></td>
<td>honest</td>
<td>hardwire pos*,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>simulated data</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\text{Hyb}<em>{2,i,0,j,1',t</em>{pos},z}$</td>
<td>$[block^*]_{out}$</td>
<td>honest</td>
<td></td>
<td>erase $[pos^*]_{in}$</td>
<td>hardwire pos*,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$[pos^*]_{in}$</td>
<td>simulated data</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\text{Hyb}_{2,i,0,j,2}$</td>
<td>$[block^*]_{out}$</td>
<td>honest</td>
<td></td>
<td>honest</td>
<td>hardwire pos*,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>simulated data</td>
</tr>
</tbody>
</table>
Table 8: Additional notations for the $\text{Hyb}_{2,i,0,j,1',z}$

<table>
<thead>
<tr>
<th>Notation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>$h^*_z$</td>
<td>The index of the node which contains $\text{block}^<em>$ at time $t = z$. (If $t = z$ has no $\text{block}^</em>$ in the memory input, then let $h^*_z$ be root index $\epsilon$.)</td>
</tr>
<tr>
<td>$b^*_z$</td>
<td>The plaintext of the node with index $h^*_z$ at time $t = z$.</td>
</tr>
<tr>
<td>$b^*_z$</td>
<td>The ciphertext of the node $b^*_z$ at time $t = z$.</td>
</tr>
<tr>
<td>$b^*_z$</td>
<td>The ciphertext the same node $b^<em>_z$ except that $\text{block}^</em>$ is erased.</td>
</tr>
</tbody>
</table>

$\text{Hyb}_{2,i,0,j,1',z}$. In this hybrid, the program is replaced by $F_{e}^{2,i,0,j,1,z}$ defined in Algorithm 75. $F_{e}^{2,i,0,j,1,z}$ erases the part in the plaintext of the input bits corresponding to $\text{block}^*$ by partially puncturing procedure that searches and erases $\text{block}^*$ at time $t$ such that $z \leq t \leq i - 1$, and it also calls $F_{o,hyb}^{j/2}$ at time $i - 1$. Recall vector $\mathbf{B}^{\text{in}}$ is a vector of nodes on an ORAM tree path, where each node is a bucket that stores several blocks of memory, and the partially puncturing procedure is to search and erase only $\text{block}^*$ from $\mathbf{B}^{\text{in}}$. To denote an empty slot in a bucket, this procedure uses the standard representation in ORAM data structure, which is the empty symbol. Note that at time $t$ where $z < t \leq i - 1$, any memory content which corresponds to $\text{block}^*$ has already been erased, thus the program just execute the “normal” $F_{o}$ function in the sense that it is indeed generating the “real” access pattern with respect to a particular memory which has $\text{block}^*$ erased.

$\text{Hyb}_{2,i,0,j,1',z}$. In this hybrid, the program is replaced by $F_{e}^{2,i,0,j,1',z}$ defined in Algorithm 76. $F_{e}^{2,i,0,j,1',z}$ is similar to $F_{e}^{2,i,0,j,1',z}$, except for the following changes.
- At $t = z - 1$, the bucket of the output ciphertext corresponding to $\text{block}^*$, namely $\mathbf{B}^{\text{out}}[h^*_z-1]$, is replaced by a hardwired ciphertext $b^*_z$.
- At $t \leq z$, an explicit check is imposed so that the private decryption key corresponding to time $t = z - 1$ and $h = h^*_z-1$ will never be used. To keep the program working, we hard-wire the plaintext $b^*_z$ corresponding to $b^*_z-1$ so that $F_{o}$ is running with the correct input.

We expand vector notation of PRF and $\mathcal{PKE}$ decryption to an equivalent loop form, which is easier to denote this special hard-wired condition along with other honest computations.

$\text{Hyb}_{2,i,0,j,1',\text{punct}}$. In this hybrid, the program is replaced by $F_{e}^{2,i,0,j,1',\text{punct}}$ defined in Algorithm 78, which removes the plaintext corresponding to $\text{block}^*$ inside the ORAM access function $\text{OACCESS}^{j/\text{punct}}$ (Algorithm 79).

$\text{Hyb}_{2,i,0,j,1',\text{pos}}$. In this hybrid, the program is replaced by $F_{e}^{2,i,0,j,1',\text{pos}}$ defined in Algorithm 80. $F_{e}^{2,i,0,j,1',\text{pos}}$ is similar to $F_{e}^{2,i,0,j,1',\text{punct}}$ except the erasure of the part in the plaintext of the input bits corresponding to $\text{pos}^*$.

Recall that value $\text{pos}^*$ is generated in $j$-th recursion level and is stored in the position map, which is outsourced to $j + 1$-th level of ORAM recursively. Let $\text{loc}^*$ be the location of the memory cell stores $\text{pos}^*$ in the $j + 1$-th level ORAM, then $\text{pos}^*$ can be found deterministically in the ORAM tree as follows: with $\text{loc}^*$, search the block with the format $[(\lfloor \text{loc}^*/\alpha \rfloor, \cdot, v)]$ in the $j + 1$-th ORAM tree, and then $\text{pos}^*$ must be stored in the $(\text{loc}^* \mod \alpha)$-th cell in $v$. In this hybrid, our additional procedure just hardwires $\text{loc}^*$, searches and erases $\text{pos}^*$ with the unique symbol $\text{dummy}$ for all time $t$ such that $z \leq t \leq i - 1$ and for recursion level $d = j + 1$.

Analysis. In the remaining of this subsection, we will complete the proof of the lemma. We applied Theorem 6.2 several times, and it allows arbitrary modification in the hybrid program as long as the computation trace remains identical.
Algorithm 75: \( F^{2, i, 0, j, 1, z}_c \)

<table>
<thead>
<tr>
<th>Input</th>
<th>( \tilde{\text{st}}^\text{in} = (\text{st}^\text{in}, t), \quad \tilde{a}^\text{in}_{\text{M}-\text{H}} = (\mathbf{I}^\text{in}, (\mathbf{B}^\text{in}, \text{lw}^\text{in})) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data:</td>
<td>( T, K_E, t^<em>, y, z, \text{block}^</em>, K_N, K_{\text{Sim}}, i, j )</td>
</tr>
</tbody>
</table>

1. Compute \( t = \lceil t / q_0 \rceil \);
2. If \( t > t^* \), output \textbf{Re}ject;
3. If \( t = t^* \) then
   - \( \ldots \)
4. If \( i \leq t < t^* \) then
   - \( \ldots \)
5. If \( i = t^* \) then
   - \( \ldots \)
6. Else
   - Compute \((r^1, r^2) = \text{PRF}(K_E, (\text{lw}^\text{in}, h(\mathbf{I}^\text{in})))\);
   - Compute \((\text{pk}^\text{in}, \text{sk}^\text{in}) = \mathcal{PK}\mathcal{E}.\text{Gen}(1^\lambda; r^1)\);
   - Compute \(\mathbf{B}^\text{in} = \mathcal{PK}\mathcal{E}.\text{Decrypt}(\text{sk}^\text{in}, \mathbf{B}^\text{in})\);
   - Compute \((r^3, r^4) = \text{PRF}(K_E, t - 1)\);
   - Compute \((\text{pk}^\text{out}, \text{sk}^\text{out}) = \mathcal{PK}\mathcal{E}.\text{Gen}(1^\lambda; r^3)\);
   - Compute \((\text{pk}^\text{out}, \text{sk}^\text{out}) = \mathcal{PK}\mathcal{E}.\text{Gen}(1^\lambda; r^4)\);
   - Compute \((\text{st}^\text{in} = \mathcal{PK}\mathcal{E}.\text{Decrypt}(\text{sk}^\text{out}, \text{st}^\text{in}))\);
   - if \((z \leq t \leq i - 1) \text{ and } (d = j)\) then
     - For each bucket \( b \) in \( \mathbf{B}^\text{in} \), search and erase \text{block}^* from \( b \) (and thus \( \mathbf{B}^\text{in} \));
     - if \( t = i - 1 \) then
       - Compute \((\text{st}^\text{out}, \mathbf{I}^\text{out}, \mathbf{B}^\text{out}) = F_{i, y}^{y, 2}(t, \text{st}^\text{in}, \mathbf{I}^\text{in}, \mathbf{B}^\text{in})\);
     - else
       - Compute \((\text{st}^\text{out}, \mathbf{I}^\text{out}, \mathbf{B}^\text{out}) = F_0(t, \text{st}^\text{in}, \mathbf{I}^\text{in}, \mathbf{B}^\text{in})\);
     - Set \( \text{lw}^\text{out} = (t, \ldots, t)\);
     - Compute \((r^1, r^2) = \text{PRF}(K_E, (\text{lw}^\text{out}, h(\mathbf{I}^\text{out})))\);
     - Compute \((\text{pk}', \text{sk}') = \mathcal{PK}\mathcal{E}.\text{Gen}(1^\lambda; r^1)\);
     - Compute \(\mathbf{B}^\text{out} = \mathcal{PK}\mathcal{E}.\text{Encrypt}(\text{pk}', \mathbf{B}^\text{out}; r^2)\);
     - Compute \((r^3, r^4) = \text{PRF}(K_E, t)\);
     - Compute \((\text{pk}', \text{sk}') = \mathcal{PK}\mathcal{E}.\text{Gen}(1^\lambda; r^3)\);
     - Compute \((\text{st}^\text{out} = \mathcal{PK}\mathcal{E}.\text{Encrypt}(\text{pk}', \text{st}^\text{out}; r^4))\);
   - else
     - Compute \((\text{st}^\text{out}, \mathbf{I}^\text{out}, \mathbf{B}^\text{out}) = F_0(t, \text{st}^\text{in}, \mathbf{I}^\text{in}, \mathbf{B}^\text{in})\);
2. Output \( \tilde{\text{st}}^\text{out} = (\text{st}^\text{out}, t + 1) \), \( \tilde{a}_{\text{M}-\text{H}}^\text{out} = (\mathbf{I}^\text{out}, (\mathbf{B}^\text{out}, \text{lw}^\text{out})) \);
Algorithm 76: $F_e^{2,i,0,j,1',z}$

Input: $\mathbf{st}^{in} = (\mathbf{st}^{in}_t, t), \mathbf{z}^{in}_{k,m} = (\mathbf{z}^{in}, (\mathbf{B}^{in}, lw^{in}))$

Data: $T, K_E, t^*, y, z, block^*, h^*_z, b^*_z, K_N, K_Sim, i, j$

1. Compute $t = \lceil t/q_0 \rceil$;
2. If $t > t^*$, output $\mathbf{reject}$;
3. if $t = t^*$ then

   \[ \ldots \]
4. if $i \leq t < t^*$ then

   \[ \ldots \]
5. else

   foreach $h \in [\mathbf{B}^{in}]$ do

      // We expands the vector notation and only modifies red-underlined condition.

5a. if $(t \geq z)$ and $(lw^{in}[h] = z - 1)$ and $(h = h^*_z)$ then

      $\mathbf{B}^{in}[h^*_z] = b^*_z$;

5b. else

      Compute $(r^{in}_1, r^{in}_2) = \mathcal{PRF}(K_E, (lw^{in}[h], h))$;

      Compute $(\mathbf{pk}^{in}, \mathbf{sk}^{in}) = \mathcal{PKE}.Gen(1^\lambda; r^1)$;

      $\mathbf{B}^{in}[h] = \mathcal{PKE}.Decrypt(\mathbf{sk}^{in}, \mathbf{B}^{in}[h])$;

5c. Compute $(r^{t-1}_3, r^{t-1}_4) = \mathcal{PRF}(K_E, t - 1)$;

5d. Compute $(\mathbf{pk}^{st}, \mathbf{sk}^{st}) = \mathcal{PKE}.Gen(1^\lambda; r^{t-1}_3)$;

5e. Compute $\mathbf{st}^{in} = \mathcal{PKE}.Decrypt(\mathbf{sk}^{st}, \mathbf{st}^{in})$;

5f. if $(z \leq i - 1)$ and $(d = j)$ then

      For each bucket $b$ in $\mathbf{B}^{in}$, search and erase $block^*$ from $b$ (and thus $\mathbf{B}^{in}$);

5g. if $t = i - 1$ then

      Compute $(\mathbf{st}^{out}, \mathbf{I}^{out}, \mathbf{B}^{out}) \leftarrow F^{1/2}_{o,y}(t, \mathbf{st}^{in}, \mathbf{I}^{in}, \mathbf{B}^{in})$;

5h. else

      Compute $(\mathbf{st}^{out}, \mathbf{I}^{out}, \mathbf{B}^{out}) = F_o(t, \mathbf{st}^{in}, \mathbf{I}^{in}, \mathbf{B}^{in})$;

      Set $lw^{out} = (t, \ldots, t)$;

      Compute $(\mathbf{r}^{out}_1, \mathbf{r}^{out}_2) = \mathcal{PRF}(K_E, (lw^{out}[h(\mathbf{I}^{out}))), h)$;

      Compute $(\mathbf{pk}', \mathbf{sk}') = \mathcal{PKE}.Gen(1^\lambda; r^{out}_1)$;

      Compute $\mathbf{B}^{out} = \mathcal{PKE}.Encrypt(\mathbf{pk}', \mathbf{B}^{out}; r^{out}_2)$;

      If $t = z - 1$, set $\mathbf{B}^{out}[h^*_z] = b^*_z$;

      Compute $(r^t_3, r^t_4) = \mathcal{PRF}(K_E, t)$;

      Compute $(\mathbf{pk}', \mathbf{sk}') = \mathcal{PKE}.Gen(1^\lambda; r^t_3)$;

      Compute $\mathbf{st}^{out} = \mathcal{PKE}.Encrypt(\mathbf{pk}', \mathbf{st}^{out}; r^t_4)$;

5i. Output $\mathbf{st}^{out} = (\mathbf{st}^{out}, t + 1), \mathbf{z}^{out}_{m-k} = (\mathbf{I}^{out}, (\mathbf{B}^{out}, lw^{out}))$;
Algorithm 77: $F^\alpha_{e,0,0,1''}$

Input : $\tilde{\text{st}}^\text{in} = (\text{st}^\text{in}, t), \tilde{\alpha}^\text{in} = (\tilde{\text{I}}^\text{in}, (\text{B}^\text{in}, \text{lw}^\text{in}))$

Data: $T, K_E, t^*, y, z, \text{block}^*, h^*_{z-1}, b^*_{z-1}, K_N, K_{Sim}, i, j$

1. Compute $t = \lceil t / q_0 \rceil$;
2. If $t > t^*$, output Reject;
3. if $t = t^*$ then
4. \[ \ldots \]
5. if $i \leq t < t^*$ then
6. \[ \ldots \]
7. else
8. Compute $(r_1^t, r_2^t) = \text{PRF}(K_E, (\text{lw}^\text{in}, h(\tilde{\text{I}}^\text{in})))$;
9. Compute $(\text{pk}^\text{in}, \text{sk}^\text{in}) = \mathcal{PKE}.\text{Gen}(1^\lambda; r_1^t)$;
10. Compute $\text{B}^\text{in} = \mathcal{PKE}.\text{Decrypt}(\text{sk}^\text{in}, \text{B}^\text{in})$;
11. Compute $(r_{3^t-1}, r_{4^t-1}) = \text{PRF}(K_E, t-1)$;
12. Compute $(\text{pk}_{\text{st}}, \text{sk}_{\text{st}}) = \mathcal{PKE}.\text{Gen}(1^\lambda; r_{3^t-1})$;
13. Compute $\tilde{\text{st}}^\text{in} = \mathcal{PKE}.\text{Decrypt}(\text{sk}_{\text{st}}, \tilde{\text{st}}^\text{in})$;
14. if $(z \leq t \leq i - 1)$ and $(d = j)$ then
15. \[ \ldots \] For each bucket $b$ in $\text{B}^\text{in}$, search and erase $\text{block}^*$ from $b$ (and thus $\text{B}^\text{in}$);
16. if $t = i - 1$ then
17. Compute $(\text{st}^\text{out}, \text{I}^\text{out}, \text{B}^\text{out}) \leftarrow F^{j/2}_{o,\text{hyb}}(t, \tilde{\text{st}}^\text{in}, \tilde{\text{I}}^\text{in}, \text{B}^\text{in})$;
18. else
19. Compute $(\text{st}^\text{out}, \text{I}^\text{out}, \text{B}^\text{out}) = F_o(t, \text{st}^\text{in}, \tilde{\text{I}}^\text{in}, \text{B}^\text{in})$;
20. Set $\text{lw}^\text{out} = (t, \ldots, t)$;
21. Compute $(r_1^t, r_2^t) = \text{PRF}(K_E, (\text{lw}^\text{out}, h(\text{I}^\text{out})))$;
22. Compute $(\text{pk}'^t, \text{sk}'^t) = \mathcal{PKE}.\text{Gen}(1^\lambda; r_1^t)$;
23. Compute $\text{B}^\text{out} = \mathcal{PKE}.\text{Encrypt}((\text{pk}'^t, \text{B}^\text{out}; r_2^t)$;
24. if $t = z - 1$, set $\text{B}^\text{out}_{[h^*_{z-1}]} = b^*_{z-1}$;
25. Compute $(r_{3^t}^t, r_{4^t}^t) = \text{PRF}(K_E, t)$;
26. Compute $(\text{pk}'^t, \text{sk}'^t) = \mathcal{PKE}.\text{Gen}(1^\lambda; r_{3^t}^t)$;
27. Compute $\tilde{\text{st}}^\text{out} = \mathcal{PKE}.\text{Encrypt}(\text{pk}'^t, \text{st}^\text{out}; r_{4^t}^t)$;
28. Output $\tilde{\text{st}}^\text{out} = (\text{st}^\text{out}, t + 1), \tilde{\alpha}^\text{out} = (\text{I}^\text{out}, (\text{B}^\text{out}, \text{lw}^\text{out}))$.
From $Hyb_{2,i,0,j,1}$ to $Hyb_{2,i,0,j,1,i−1}$: The difference is at time $i−1$, but the output simulated by $F^{2,2}_{o,hyb}$, which hardwires $pos$*, has the identical computation trace. By Theorem 6.2, these two hybrids are computationally indistinguishable.

From $Hyb_{2,i,0,j,1,z}$ to $Hyb_{2,i,0,j,1,z}$: Since $F^{2,2}_{e}$ is obtained by hardwiring the same outputs computed from $F^{2,2}_{e}$, the computations defined by the two programs have identical computation trace. Therefore, by Theorem 6.2, the hybrids are computationally indistinguishable.

From $Hyb_{2,i,0,j,1,z}$ to $Hyb_{2,i,0,j,1,z−1}$: The indistinguishability is established via a series of intermediate hybrids, which we will describe in text:

1. $F^{2,2}_{e,0,j,1,z} \{K_{E}\{(z−1,h_{z−1})\}, h_{z−1}, b_{z−1}, [b]^{*}_{z−1}\}$. In the first hybrid, the input $(z−1,h_{z−1})$ is punctured from the PRF key $K_{E}$. The pseudo-randomness computed from $K_{E}$ is hardwired in the program. Since the computation defined by this program has identical computation trace as that in $Hyb_{2,i,0,j,1,z}$, by Theorem 6.2, the two hybrids are computationally indistinguishable.

2. $F^{2,2}_{e,0,j,1,z} \{K_{E}\{(z−1,h_{z−1})\}, h_{z−1}, b_{z−1}, [b; r]^{*}_{z−1}\}$. In the next hybrid, we replace the hardwired ciphertext by a ciphertext encrypted with true randomness. Indistinguishability is guaranteed by the selective security of PPRF.

3. $F^{2,2}_{e,0,j,1,z} \{K_{E}\{(z−1,h_{z−1})\}, h_{z−1}, b_{z−1}, [r]^{*}_{z−1}\}$. Next, we change the hardwired ciphertext $[b; r]^{*}_{z−1}$ to its counterpart $[b; r]^{*}_{z−1}$ with block* erased. Indistinguishability is guaranteed by the IND-CPA security of the $PK$ because $F^{2,2}_{e,0,j,1,z}$ would never use the private key of $(z−1,h_{z−1})$.

4. $F^{2,2}_{e,0,j,1,z} \{K_{E}, h_{z−1}, b_{z−1}, [b]^{*}_{z−1}\}$. Then, we un-puncture the PRF. Indistinguishability is guaranteed by the security of the puncturable PRF.

5. $F^{2,2}_{e,0,j,1,z} \{K_{E}, h_{z−1}, b_{z−1}\}$. We remove Line 10 and the honest plaintext $b_{z−1}$ that contains block* (Algorithm 77). The computation defined by this program has identical computation trace as the previous hybrid, and two hybrids are computationally indistinguishable by Theorem 6.2. To show two traces are identical, we observe the only difference is the input bucket $b_{z−1}$ was replaced by $b_{z−1}$, which is decrypted from $[b]^{*}_{z−1}$. For all $z \leq t \leq i−1$, however, input to $F_{o}$ are always have block* erased in advance, and it follows that double-erasing yields the identical input $B^{in}$.

6. At this point, the computation trace defined by $F^{2,2}_{e,0,j,1,z} \{K_{E}, h_{z−1}, b_{z−1}\}$ is identical to that in $Hyb_{2,i,0,j,1,z−1}$, and two hybrids are computationally indistinguishable by Theorem 6.2. It is because the “commute property of erasure”, where any computation step from time $t_{pos}$ to $i−1$ does not “compute” on block*, and block* is transferred literally from input to output through $F_{o}$. Therefore, erasing block* from output is identical to erasing block* from input.

From $Hyb_{2,i,0,j,1,z−1}$ to $Hyb_{2,i,0,j,1,z−1}$: By the same argument from $Hyb_{2,i,0,j,1,z−1}$ to $Hyb_{2,i,0,j,1,z}$, we can see that $Hyb_{2,i,0,j,1,z}$ is indistinguishable from $Hyb_{2,i,0,j,1,z−1}$. Note that the only difference between $Hyb_{2,i,0,j,1,z−1}$ and $Hyb_{2,i,0,j,1,z}$ is the erase of block* in $F^{2,2}_{e,0,j,1}[,t_{pos}]^{+1}$ implemented in $OACCESS_{punct}$, and they have identical computation trace. By Theorem 6.2, the two hybrids are computationally indistinguishable.
From Hyb\textsubscript{2,i,0,j,1}'pos to Hyb\textsubscript{2,i,0,j,2}: Our task here is to remove the information corresponding to pos\textsuperscript{*} from position map, which has pos\textsuperscript{*} stored in the next recursion layer of the ORAM tree. The approach is similar as above, as we need to remove this information that pos\textsuperscript{*} is accessed for each time z in the next layer of ORAM tree. To show these two hybrids are computationally indistinguishable, we therefore define Hyb\textsubscript{2,i,0,j,1}'pos.z similar to Hyb\textsubscript{2,i,0,j,1,z}, and the argument is analogous to that from Hyb\textsubscript{2,i,0,j,1} to Hyb\textsubscript{2,i,0,j,1}'pos'. The sketched proof is proposed as follows:

- Hyb\textsubscript{2,i,0,j,1}'pos \approx Hyb\textsubscript{2,i,0,j,1}'pos.z with z = i − 1 is analogous to the series of hybrids from Hyb\textsubscript{2,i,0,j,1} to Hyb\textsubscript{2,i,0,j,1,i−1}, where the indistinguishability is guaranteed by the indistinguishability of CiØ (Theorem 6.2).

- Hyb\textsubscript{2,i,0,j,1}'pos.z \approx Hyb\textsubscript{2,i,0,j,1}'pos.z−1 for time z that t\textsubscript{pos} < z ≤ i − 1 is analogous to the series of hybrids from Hyb\textsubscript{2,i,0,j,1} to Hyb\textsubscript{2,i,0,j,1,z−1}, where the indistinguishability is guaranteed by the indistinguishability of CiØ (Theorem 6.2), the selective security of PPRF, the IND-CPA security of \textit{PRAM}, and the “commute property of erasure” of ORAM construction.

- Hyb\textsubscript{2,i,0,j,1}'pos.z \approx Hyb\textsubscript{2,i,0,j,2} with z = t\textsubscript{pos} + 1 is analogous to the series of hybrids from Hyb\textsubscript{2,i,0,j,1}'pos+1 to Hyb\textsubscript{2,i,0,j,1}'pos, where the indistinguishability is guaranteed by the indistinguishability of CiØ (Theorem 6.2), the selective security of PPRF, and the IND-CPA security of \textit{PRAM}.

These hybrids and arguments are one-to-one mapping to their previous analogous, where the only difference here is we erase the memory cell \texttt{loc\textsuperscript{*}} storing pos\textsuperscript{*} (rather than the memory block \texttt{block\textsuperscript{*}} contains pos\textsuperscript{*}). The details are omitted here.

\[\square\]

B.6 Proof Sketch of Theorem 9.1 (Security for \textit{RE}-PRAM)

The above \textit{RE}-PRAM is built in the same manner with that of \textit{RE}-RAM. Both of them depend on three levels of compilers, ORAM/OPRAM, \textit{PRAM}, and finally CiØ-RAM/PRAM. To argue the security of \textit{RE}-PRAM, we use similar proof techniques to go through hybrids except that we insert an additional layer to deal with each CPU agent respectively.

Let Real be the real security game in which the adversary is given ENC\textsubscript{Real}, and Ideal be the security game in which the adversary is given ENC\textsubscript{Ideal}. The intermediate hybrids between Real and Ideal are similar to those in Section B.5. Roughly, we have the following hybrids Real ≈ Hyb\textsubscript{0} ≈ Hyb\textsubscript{1} ≈ Hyb\textsubscript{2,1}~ ≈ ... ≈ Hyb\textsubscript{2,0} = Ideal.

Let \(F^x_e\), \(\Pi^x_e\), and ENC\textsubscript{x} be the stateful function, computation system, and encoding in Hyb\textsubscript{x}.

Hyb\textsubscript{1}. In this hybrid, \(F^1_e\) hardwires the output st = (halt, y). It always returns \(⊥\) if \(t > t^*\). At time \(t^*\), the special CPU agent returns st = (halt, y). From Hyb\textsubscript{0} to Hyb\textsubscript{1}, \(\Pi^0_e\) and \(\Pi^1_e\) have the same computation traces, and thus by applying CiØ-PRAM, ENC and ENC\textsubscript{1} are computationally indistinguishable.

Hyb\textsubscript{2,2}. In this hybrid, at time \(t, i ≤ t ≤ t^*\), \(F^2_e\textsuperscript{j}\)'s access pattern is a simulated access pattern provided by the ORAM simulator, and the output state is replaced by an encryption of a special symbol dummy. From Hyb\textsubscript{1} to Hyb\textsubscript{2,t^*}, we directly apply CiØ-PRAM to claim that ENC\textsubscript{1} and ENC\textsubscript{2,t^*} are computationally indistinguishable due to \(\text{Trace}(\Pi^1_e) = \text{Trace}(\Pi^2_{t^*})\). However, from Hyb\textsubscript{2,j} to Hyb\textsubscript{2,1−1}, we define the next layer \(\text{Hyb}\textsubscript{2,i,k}\) in which \(k\) is indexed by a CPU.

Hyb\textsubscript{2,i,k}. In this hybrid at time \(t = i − 1, F^2_e\textsuperscript{i,k}\)'s access pattern is a simulated access pattern provided by the ORAM simulator if CPU \(A < k\), while its access pattern is a real access pattern if CPU \(A ≥ k\). For the time \(i\) and CPU \(k\), we consider the following cases.
Algorithm 78: $F_{c,0,j,1',t_{pos}}^{2,i,0,j,1',t_{pos}}$

Input : $\tilde{\mathbf{s}}_{\text{in}} = (\mathbf{s}_{\text{in}}, t)$, $\tilde{\mathbf{a}}_{k_{\text{st}}}^{\text{in}} = (\mathbf{I}_{\text{in}}, (\mathbf{B}_{\text{in}}, \mathbf{l}_{\text{w}}^{\text{in}}))$

Data: $T, K_{E}, t^*, y, t_{pos}, K_N, K_{\text{Sim}}, i, j$

1. Compute $t = \lceil t / q \rceil$;
2. If $t > t^*$, output Reject;
3. if $t = t^*$ then
   4. ... 
5. if $i \leq t < t^*$ then
   6. ... 
   7. else
   8. Compute $(r_{1}^{\text{in}}, r_{2}^{\text{in}}) = \text{PRF}(K_{E}, (\mathbf{l}_{\text{w}}^{\text{in}}, h(\mathbf{I}_{\text{in}})))$;
   9. Compute $(\mathbf{pk}^{\text{in}}, \mathbf{sk}^{\text{in}}) = \mathcal{PKE}.\text{Gen}(1^{\lambda}; r_{1}^{\text{in}})$;
10. Compute $\mathbf{B}_{\text{in}} = \mathcal{PKE}.\text{Decrypt}(\mathbf{sk}^{\text{in}}, \mathbf{B}_{\text{in}})$;
11. Compute $(r_{3}^{t-1}, r_{4}^{t-1}) = \text{PRF}(K_{E}, t - 1)$;
12. Compute $(\mathbf{pk}_{\text{st}}, \mathbf{sk}_{\text{st}}) = \mathcal{PKE}.\text{Gen}(1^{\lambda}; r_{3}^{t-1})$;
13. Compute $\mathbf{s}_{\text{in}} = \mathcal{PKE}.\text{Decrypt}(\mathbf{sk}_{\text{st}}, \mathbf{st}_{\text{in}})$;
   14. if $t = i - 1$ then
      15. Compute $(\mathbf{st}_{\text{out}}, \mathbf{I}_{\text{out}}, \mathbf{B}_{\text{out}}) \leftarrow F_{o,\text{hyb}}^{2,j/2}(t, \mathbf{s}_{\text{in}}, \mathbf{I}_{\text{in}}, \mathbf{B}_{\text{in}})$;
   16. else if $t = t_{\text{out}}$ then
      17. Compute $(\mathbf{st}_{\text{out}}, \mathbf{I}_{\text{out}}, \mathbf{B}_{\text{out}}) = F_{o,\text{punct}}^{j/2}(t, \mathbf{s}_{\text{in}}, \mathbf{I}_{\text{in}}, \mathbf{B}_{\text{in}});$
         // $F_{o,\text{punct}}^{j/2} = \text{CP-ORAM}.\text{Compile}(F, O\text{ACCESS}_{j,\text{punct}}^{j/2})$
   18. else
      19. Compute $(\mathbf{st}_{\text{out}}, \mathbf{I}_{\text{out}}, \mathbf{B}_{\text{out}}) = F_{o}(t, \mathbf{s}_{\text{in}}, \mathbf{I}_{\text{in}}, \mathbf{B}_{\text{in}})$;
   20. Set $\mathbf{l}_{\text{w}}^{\text{out}} = (t, \ldots, t)$;
   21. Compute $(r_{1}^{\text{out}}, r_{2}^{\text{out}}) = \text{PRF}(K_{E}, (\mathbf{l}_{\text{w}}^{\text{out}}, h(\mathbf{I}_{\text{out}})))$;
   22. Compute $(\mathbf{pk}', \mathbf{sk}') = \mathcal{PKE}.\text{Gen}(1^{\lambda}, r_{1}^{\text{out}})$;
   23. Compute $\mathbf{B}_{\text{out}} = \mathcal{PKE}.\text{Encrypt}(\mathbf{pk}', \mathbf{B}_{\text{out}}; r_{2}^{\text{out}})$;
   24. Compute $(r_{3}', r_{4}') = \text{PRF}(K_{E}, t)$;
   25. Compute $(\mathbf{pk}', \mathbf{sk}') = \mathcal{PKE}.\text{Gen}(1^{\lambda}; r_{3}')$;
   26. Compute $\mathbf{st}_{\text{out}} = \mathcal{PKE}.\text{Encrypt}(\mathbf{pk}', \mathbf{st}_{\text{out}}; r_{4}')$;
27. Output $\tilde{\mathbf{s}}_{\text{out}} = (\mathbf{st}_{\text{out}}, t + 1)$, $\tilde{\mathbf{a}}_{k_{\text{st}}}^{\text{out}} = (\mathbf{I}_{\text{out}}, (\mathbf{B}_{\text{out}}, \mathbf{l}_{\text{w}}^{\text{out}}))$;
Algorithm 79: \textsc{Oaccess}^{j, punct}$^\prime\{K_N\}$

\textbf{Input}: $t, d, \text{loc}, \text{val}$

\textbf{Output}: $\text{oldval}$

\textbf{Data}: $K_N, \alpha, \text{MaxDepth}$ (Memory size $S = \alpha^{\text{MaxDepth}}$, loc$_{i-1,j}$)

1. \textbf{if} $d \geq \text{MaxDepth}$ \textbf{then}
   2. \textbf{return} 0
3. \textbf{Pick leaf} $\text{newpos}$ \textbf{at recursion level} $d$ \textbf{based on} \text{PRF}($K_N, (t, d, \text{FetchR})$); \hfill \text{// Update position map}
4. $\text{pos} \leftarrow \text{Oaccess}(d + 1, \lfloor \text{loc}/\alpha \rfloor, \text{newpos})$; \hfill \text{// Fetch}
5. $\text{I}_{\text{fetch}} \leftarrow \text{PATH}(d, \text{pos})$;
6. $\text{B}_{\text{fetch}} \leftarrow \text{READ}(\text{I}_{\text{fetch}})$;
7. \textbf{if} $(d = j)$ \textbf{then}
   8. $\text{(B}_{\text{fetch},-}, \text{oldval}) \leftarrow \text{REMOVEBLOCK}(\text{B}_{\text{fetch}}, \text{loc}, \alpha, \text{pos})$;
   9. $\text{WRITE}(\text{I}_{\text{fetch}}, \text{B}_{\text{fetch},-})$;
8. \textbf{else}
   11. $\text{(B}_{\text{fetch},-}, \text{oldval}) \leftarrow \text{FETCHANDUPDATE}(\text{B}_{\text{fetch}}, \text{loc}, \text{val}, \alpha, \text{pos}, \text{newpos})$;
   12. $\text{WRITE}(\text{I}_{\text{fetch}}, \text{B}_{\text{fetch},-})$;
13. \textbf{Pick leaf} $\text{pos''}$ \textbf{at recursion level} $d$ \textbf{based on} \text{PRF}($K_N, (t, d, \text{FlushR})$); \hfill \text{// Flush}
14. $\text{I}_{\text{flush}} \leftarrow \text{PATH}(d, \text{pos''})$;
15. $\text{B}_{\text{flush}} \leftarrow \text{READ}(\text{I}_{\text{flush}})$;
16. $\text{B}_{\text{flush}} \leftarrow \text{FLUSH}(\text{B}_{\text{flush}}, \text{pos''})$;
17. $\text{WRITE}(\text{I}_{\text{flush}}, \text{B}_{\text{flush}})$;
18. \textbf{return} $\text{oldval}$;
Algorithm 80: $F_{\mathcal{E}}^{2,i,0,j,1,t_{\text{pos}},z}$

\begin{algorithmic}
  \State \textbf{Input} : $\tilde{st}^{in} = (\tilde{st}^{in}, t)$, $\tilde{a}^{in}_{k=1} = (\tilde{I}^{in}, (\tilde{B}^{in}, Iw^{in}))$
  \State \textbf{Data}: $T, KE, t^*, y, t_{\text{pos}}, \text{loc}^*, K_N, K_{\text{Sim}}, i, j$
  \State Compute $t = \lceil t/q_0 \rceil$;
  \State If $t > t^*$, output \texttt{Reject};
  \State if $t = t^*$ then
  \hspace{1em} \ldots
  \State if $i \leq t < t^*$ then
  \hspace{1em} \ldots
  \State else
  \hspace{1em} Compute $(r_1^{in}, r_2^{in}) = \text{PRF}(KE, (Iw^{in}, h(I^{in})))$;
  \hspace{1em} Compute $(pk^{in}, sk^{in}) = \mathcal{PKE}.\text{Gen}(1^\lambda, r_1^{in})$;
  \hspace{1em} Compute $B^{in} = \mathcal{PKE}.\text{Encrypt}(sk^{in}, B^{in})$;
  \hspace{1em} Compute $(r_3^{t-1}, r_4^{t-1}) = \text{PRF}(KE, t - 1)$;
  \hspace{1em} Compute $(pk_{st}, sk_{st}) = \mathcal{PKE}.\text{Gen}(1^{\lambda}; r_3^{t-1})$;
  \hspace{1em} Compute $st^{in} = \mathcal{PKE}.\text{Encrypt}(sk_{st}, st^{in})$;
  \hspace{1em} if $(z \leq t < i - 1)$ and $(d = j + 1)$ then
  \hspace{2em} For each bucket $b$ in $B^{in}$, search for block of the form $(\lfloor \text{loc}^* / \alpha \rfloor, \cdot, v)$, and erase the $(\text{loc}^* \mod \alpha)$-th cell in $v$ (and thus in $B^{in}$) with symbol \texttt{dummy};
  \hspace{1em} if $t = i - 1$ then
  \hspace{2em} Compute $(st^{out}, I^{out}, B^{out}) \leftarrow F_{\mathcal{E}}^{2,i,0,j,1}(t, st^{in}, I^{in}, B^{in})$;
  \hspace{1em} else if $t = t_{pos}$ then
  \hspace{2em} Compute $(st^{out}, I^{out}, B^{out}) = F_{\mathcal{E}}^{j,\text{punct}}(t, st^{in}, I^{in}, B^{in})$;
  \hspace{2em} // $F_{\mathcal{E}}^{j,\text{punct}} = \text{CP-ORAM.\text{Compile}}(F, \text{ACCESS}_{j,\text{punct}})$
  \hspace{1em} else
  \hspace{2em} Compute $(st^{out}, I^{out}, B^{out}) = F_{\mathcal{E}}(t, st^{in}, I^{in}, B^{in})$;
  \hspace{1em} Set $Iw^{out} = (t, \ldots, t)$;
  \hspace{2em} Compute $(r_1^{out}, r_2^{out}) = \text{PRF}(KE, (Iw^{out}, h(I^{out})))$;
  \hspace{2em} Compute $(pk', sk') = \mathcal{PKE}.\text{Gen}(1^{\lambda}; r_1^{out})$;
  \hspace{2em} Compute $B^{out} = \mathcal{PKE}.\text{Encrypt}(pk', B^{out}; r_2^{out})$;
  \hspace{2em} Compute $(r_3^{j}, r_4^{j}) = \text{PRF}(KE, t)$;
  \hspace{2em} Compute $(pk', sk') = \mathcal{PKE}.\text{Gen}(1^{\lambda}; r_3^{j})$;
  \hspace{2em} Compute $st^{out} = \mathcal{PKE}.\text{Encrypt}(pk', st^{out}; r_4^{j})$;
  \hspace{1em} Output $\tilde{st}^{out} = (\tilde{st}^{out}, t + 1)$, $\tilde{a}^{out}_{k=1} = (\tilde{I}^{out}, (\tilde{B}^{out}, Iw^{out}))$
\end{algorithmic}
- If CPU \( k \) is not a representative to access its corresponding memory location \( \text{loc}_k \), \( \text{Hyb}_{2,i,k} \) and \( \text{Hyb}_{2,i,k+1} \) are identical.

- If CPU \( k \) is a representative to access its corresponding memory location \( \text{loc}_k \) and that memory block of \( \text{loc}_k \) is stored at the OPRAM tree path \( \text{pos}^* \), we need to argue that \( F^2_{e,i,k} \) and \( F^2_{e,i,k+1} \) are computational indistinguishable. Therefore, we define the four layer hybrids \( \text{Hyb}_{2,i,k,0,j} \) later where \( j \) is the recursive level.

\[
\text{Hyb}_{2,i,k} = \text{Hyb}_{2,i,k,0,0} \approx \ldots \approx \text{Hyb}_{2,i,k,0,d_{\text{max}}} \approx \text{Hyb}_{2,i,k,0',d_{\text{max}}} \approx \ldots \approx \text{Hyb}_{2,i,k,0',0} = \text{Hyb}_{2,i,k+1}.
\]

In the construction, the access pattern of the OPAccess depends on the paths (stored in the public state \( \text{st}_1 \)) that each CPU wants to access. Note that the access pattern is fully determined by \( \text{st}_1 \)'s to simulate the access pattern, and this can be done by injecting a puncturing code. This can be done CPU by CPU. Namely, for each \( p_k \) accessed by CPU \( k \), we can inject a puncturing code at the corresponding time step \( t_k \) that the value \( p_k \) is generated, to remove the generation of \( p_k \). Moreover, we can move to this punctured hybrid by a sequence of partially punctured hybrids as before (Section B.5.4), by gradually puncturing the value of \( p_k \) backwards in time, per time step and per CPU. Upon reaching this punctured hybrid, we can switch \( p_k \) to a simulated one, undo the puncturing, and move to the next CPU. The argument from \( \text{Hyb}_{2,i,k,0,j} \) to \( \text{Hyb}_{2,i,k,0,j+1} \) is identical to that in Section B.5.4.

**B.7 Proof of Theorem 10.4 (Security for \( \forall \mathcal{E} \))**

*Proof.* Let \( \text{Adv}_A^\beta \) denote the advantage of the adversary \( A \) in the hybrid \( \text{Hyb}_\beta \).

\( \text{Hyb}_0 \). This is the real security experiment. The challenger chooses randomness \( r_1, r_2, r_3 \), and computes \( (\text{vk}, \text{sk}) \leftarrow \text{SIG.Gen}(1^\lambda; r_1) \), and \( \text{ENC} \leftarrow \text{CiO.Obf}((\Pi; r_3)) \). Note that here \( F \) has \( (r_1, r_2, \text{sk}) \) hardcoded. Then the challenger returns \( (\text{ENC}, \text{vk}) \) to the adversary \( A \). The adversary wins the game if it returns \( (\pi, \tilde{y}) \) so that \( \mathcal{E}.\text{Verify}(\text{vk}, \pi, \tilde{y}) = 1 \) and \( \tilde{y} \neq P(x) \).

\( \text{Hyb}_1 \). The challenger chooses randomness \( r_1, r_2, r_3 \), and computes \( (\text{vk}, \text{sk}) \leftarrow \text{SIG.Gen}(1^\lambda; r_1), y = P(x), \sigma = \text{SIG.Sign}(\text{sk}, y; r_2) \), and \( \text{ENC} \leftarrow \text{CiO.Obf}((\hat{\Pi}; r_3)) \), where \( \hat{\Pi} \) (corresponds to \( \hat{\Pi}' \)) has \( \sigma \) (rather than \( (r_1, r_2, \text{sk}) \)) hardcoded; see Algorithm 81.

\[ \Box \]

**Analysis.** Our goal here is to show \( \text{Adv}_A^0 \leq \text{negl}(\lambda) \). To achieve this goal, we prove the following lemmas.

**Lemma B.55.** If \( \text{CiO} \) is a secure indistinguishability obfuscation for computation scheme in the RAM / PRAM model, then we have \( |\text{Adv}_A^0 - \text{Adv}_A^1| \leq \text{negl}(\lambda) \).

*Proof.* Assume there is an adversary \( A \), who can distinguish the two hybrids with non-negligible probability. By average argument, there exist \( r_1, r_2 \) such that \( A \) can distinguish \( \text{Hyb}_0^{r_1,r_2} \) from \( \text{Hyb}_1^{r_1,r_2} \). That means \( A \) can distinguish \( \text{CiO}(\hat{\Pi}) \) from \( \text{CiO}(\hat{\Pi}') \).

\[ \Box \]

**Lemma B.56.** If \( \text{SIG} \) is a secure digital signature scheme, then we have \( \text{Adv}_A^1 \leq \text{negl}(\lambda) \).
Algorithm 81: $\hat{F}'$  // this program is used in Hyb₁

\begin{algorithm}
\begin{algorithmic}
\State \textbf{Input :} $\text{st}^\text{in} = (\text{st}^\text{in}, t), a^\text{in}$
\State \textbf{Data :} $T, \sigma$
\State Compute $(\text{st}^\text{out}, a^\text{out}) = F(\text{st}^\text{in}, a^\text{in})$;
\If{$\text{st}^\text{out} \neq (\text{halt}, \cdot)$}
\State Set $\hat{\text{st}}^\text{out} = (\text{st}^\text{out}, t + 1)$;
\Else
\If{$y = \bot$}
\State Set $\hat{\text{st}}^\text{out} = \text{st}^\text{out}$;
\Else
\State Set $\hat{\text{st}}^\text{out} = (\text{st}^\text{out}, \sigma)$;
\EndIf
\State Set $a^\text{out} = \bot$;
\EndIf
\EndIf
\Endalgorithmic
\end{algorithm}

Proof. Assume there is an adversary $A$ who wins the game in Hyb₁. Based on such adversary $A$, we show how to construct a forger $B$ to break the unforgeability of SIG as follows.

$B$ internally simulates a copy of Hyb₁. Upon receiving $\text{vk}$ from $B$’s SIG challenger, $B$ chooses $F$ and $x$, and computes $y = F(x)$. Now $B$ queries its challenger with message $y$ to obtain the corresponding signature $\sigma$. Then $B$ based on $F$ and $\sigma$, constructs $\hat{F}'$, and return $\text{ENC} \leftarrow \text{CiO.Obf(}\hat{\Pi}'\text{)}$ and $\text{vk}$ to the adversary $A$. Whenever $A$ returns $(\tilde{y}, \tilde{\pi})$, $B$ returns $(\tilde{y}, \hat{\pi}) = (\tilde{y}, \tilde{\pi})$ to SIG challenger.

\qed

References


