Scalar-product Based Secure Two-party Computation

Chih-Hao Shen*, Justin Zhan†, Tsan-Sheng Hsu*, Churn-Jung Liau*, and Da-Wei Wang*

Institute of Information Science, Academia Sinica, Taiwan
Email: {shench, tshsu, liaucj, wdw}@iis.sinica.edu.tw*

The Heinz School, Carnegie Mellon University, USA
Email: justinzh@andrew.cmu.edu†

Abstract

Secure multiparty computation is a very important research topic in cryptography. The sub-problem of secure multiparty computation that has received special attention by researchers because of its close relation to many cryptographic tasks is secure two-party computation. This area of research is concerned with the question: “Can two party computation be achieved more efficiently and under weaker security assumptions than general multiparty computation?” Yao’s protocol provided security against passive adversaries, while Lindell and Pinkas proposed secure two-party protocols that are secure against active adversaries. In this paper, we would like to propose a set of information theoretically secure protocols based on scalar product protocol. The detailed complexity analysis is also provided.

1. Introduction

Secure multiparty computation is a research topic aiming at the double-edged privacy problem: How can several potentially distrustful parties take advantage of their private data without revealing their privacy? After Yao’s [16] general solution to two-party secure computation was proposed, Goldreich et al. [11] soon gave another general solution to multiparty computation. Both proposals are so elegant that they provide secure two-party/multiparty protocols for binary AND and XOR gates, which can be further generalized to all computable functions. However, despite their academic significance, both solution have computation costs too prohibitive to be feasible in real applications.

A function $f$ is complete if a secure protocol for $f$ implies the existence of secure protocols for all computable functions. Yao and Goldreich et al. propose the idea to solve secure two-party/multiparty computation by giving secure protocols for complete functions. Extended from the idea, the scalar product has gathered more and more attention because of its completeness and integer-based computing power. However, there is no systematic approach to construct all computable functions from scalar products. This paper is organized as follows. In Section 2, we extensively discuss the related works. In Section 3, we introduce the notations and Scalar-product protocol as the building block to all the other protocols. Next, the bottom-up construction of the three primitives—Product, Comparison, and Division protocols—is thoroughly presented in Section 4. We also analyze the round and computation complexity of the three primitives in Section 5. After that, we specifically build up secure protocols for real applications based on our primitives in Section 6. Finally, we conclude the paper and lays out the future work in Section 7.

2. Related Works

After Yao’s and Goldreich et al.’s proposals, researchers have been looking for new complete functions and the foundations of the completeness. Kilian shows that the oblivious transfer is complete [12], and so are the functions with imbedded OR [13]. Furthermore, it is claimed that the integer-based scalar product is more practical to real applications than the binary-based oblivious transfer [5]. In the past decade, proposals for the secure scalar product are flourishing. Du and Zhan [8] propose the invertible-
matrix and the commodity-based approaches. The former approach enables the trade-off between efficiency and privacy, and the latter is based on Beaver’s commodity model [2]. Goethals et al. [9] propose the computationally secure scalar-product protocol, security of which depends on the intractability of the composite residuosity problem.

Moreover, there are many efforts on building various applications on secure scalar products. Atallah and Du reduce geometry problems to scalar products [1]. Du et al. construct secure protocols for statistical analysis [7] and scientific computations [6]. Recently, Bunn and Ostrovsky [3] give a secure k-means clustering protocol based on scalar products under the composite-residuosity approach.

There is also plenty of theoretical studies on scalar products. Based on information theory, Chiang et al. [4] propose a privacy measurement, by which they analyze various scalar-product approaches. They prove that the invertible-matrix approach discloses at least half the information and the commodity-based approach is perfectly secure. Wang et al. [15] prove that there is no information-theoretically secure two-party protocol for the scalar product. Moreover, the closed property of the commodity-based approach is preliminarily verified according to the security definition based on information theory [14].

3. Preliminaries

In this section, we introduce the notation used hereafter and the formulation for the building block—scalar product.

The notation \((X_1, X_2) \mapsto (Y_1, Y_2)\) for a secure two-party protocol represents that Party 1 and Party 2 have private inputs \(X_1\) and \(X_2\) respectively. After protocol execution, Party 1 gets output \(Y_1\), while Party 2 gets \(Y_2\). For clarity purpose, footnotes always indicate the data owner. The domain \(\mathbb{Z}_n\) denotes the finite group consisted of elements \(\{0, \ldots, n-1\}\), and the results of addition and multiplication in \(\mathbb{Z}_n\) are the modular summation and the modular product. Our proposal mainly focuses on the computations over \(\mathbb{Z}_n\) and \(n\) is two’s power, namely, \(n = 2^{k+1}, k \in \mathbb{N}\). As a result, without explicit mention, the arithmetic is always defined in \(\mathbb{Z}_n\). Moreover, to extend the domain from natural number to integer, while elements \(\{1, \ldots, \lfloor \frac{n-1}{2} \rfloor\}\) remain positive numbers, elements \(\{n-1, \ldots, n-\lfloor \frac{n-1}{2} \rfloor\}\) are interpreted as negative integers analogous to the binary system in modern computers. As a result, the subtraction to \(p\) is equivalent to the addition to \((n-p)\).

In this paper, the formulation for Scalar Product protocol follows Goldreich’s principle [10] that the intermediate results during a protocol execution are always shared among participants. In a protocol \(\pi\) composed of Scalar Products, current outputs can be inputs to the next Scalar Product, which is actually the intermediate results of \(\pi\) and should be shared. Moreover, the intermediate results are shared by addition rather than multiplication. In finite group \(\mathbb{Z}_n\), the multiplicative sharing reveals information when either the shares is zero, on the other hand, the additive sharing is proven to be perfect [14]. Specifically, we define the secure Scalar Product protocol as

**Definition 3.1 (Scalar Product)** Party 1 and Party 2 want to collaboratively execute the secure protocol

\[ ((x[1], \ldots, x[d_1]), (x[1], \ldots, x[d_2])) \mapsto (y_1, y_2) \]

such that \(y_1 + y_2 = x[1] \cdot x[2] + \cdots + x[d_1] \cdot x[d_2] \) and \(x[i], x[i], y_1, y_2 \in \mathbb{Z}_n, \text{ for } i = 1, \ldots, d\). Note that \(+\) and \(\cdot\) are the addition and the multiplication in \(\mathbb{Z}_n\).

Here we merely define Scalar Product instead of providing a specific approach because we focus on building more protocols on top of Scalar Product. Similar to the software specification, as long as a new subroutine matches the interface, it can replace the old one and work perfectly within a huge program. In our scalar-product based protocols, as long as a new approach matches the Definition 3.1, it can be used as the building block of our proposed protocols. Moreover, our protocols are information-theoretically composed. They are as strong as the specific Scalar Product approach. For example, based on a computationally secure approach, our proposed protocols are also computationally secure.

At last, we need to mention that we do not deal with the problem combining the final results. The combination of the final result involves the fairness problem that the first party who receives the result might disrupt the collaboration prematurely. One of the possible solutions is to adopt the commitment protocols. However, we do not discuss this issue in this paper for it is beyond our focus.

4. Three Primitives

First of all, we would like to explain our construction principles. During our bottom-up construction, the Scalar-product protocol is used as the initial building block. If a protocol is composed of building blocks and its participants only compute locally, the protocol becomes another building block. In other words, we construct a new protocol by executing building blocks or local computation by the participant himself. No communication between participant is allowed during protocol composition. Next, the new protocol becomes another building block used to compose other protocols. Such construction is theoretically secure so that its security strength totally relies on the security of the underlying Scalar-product implementation.

Next, we will introduce our proposed three primitives to secure two-party computation—the Product, the Comparison, and the Division protocols.
4.1. Polynomial Evaluation

To compute a polynomial function collaboratively, we need to be able to perform two-party additions and multiplications. Because we adopt the principle of the additive sharing, the two-party addition is trivial. However, to execute a secure two-party multiplication, it is necessary to use the Scalar Product protocol.

**Definition 4.1 (Product)** Party 1 and Party 2 share the multiplicand and the multiplier. They want to securely execute the protocol \((x_1, y_1), (x_2, y_2) \mapsto (z_1, z_2)\) such that \(z_1 + z_2 = (x_1 + x_2)(y_1 + y_2)\).

With a little modification, it can be rewritten that \(z_1 + z_2 = x_1y_1 + x_2y_2 + (x_1y_2 + y_1x_2)\). After the factoring, it is obvious that \(x_1y_2 + y_1x_2\) is locally computable to Party \(j\), \(j = 1, 2\), but we need to execute the Scalar-product protocol to compute the other terms. The details are as the follows:

**PROTOCOL Product**

1. Party 1 and Party 2 jointly execute the Scalar-product protocol \(((x_1, y_1), (x_2, y_2)) \mapsto (t_1, t_2)\) such that \(t_1 + t_2 = x_1y_2 + y_1x_2\).
2. Party \(j\) locally computes \(z_j = t_j + x_jy_j\), for \(j = 1, 2\).

A polynomial is a function constructed from variables and constants using the operations of addition, subtraction, and multiplication. With the additive sharing we can easily add and subtract, and with the Product protocol we can multiply, too. Therefore, secure two-party computation on polynomial evaluations can be composed of the Product protocol and the help of additive sharing.

4.2. Comparison

There are many variation of binary comparison: less than (<), greater than (>), less than or equal to (\(\leq\)), greater than or equal to (\(\geq\)), and equal to (\(=\)). However, we know that all of them are reducible to the less than operator. Moreover, in order to compare \(x\) and \(y\), it is intuitive to compare \((x - y)\) and \(0\) since we share the intermediate results additively. It is effortless to subtract under additive sharing. More specifically, our proposal to compare \(x\) and \(y\) is to compute the most significant bit of \((x - y)\). According to the binary system on modern computers, if the most significant bit of \((x - y)\) is 1, \((x - y)\) is a negative number inferring that \(x\) is less than \(y\).

Prior to the introduction of the primitive Comparison protocol, we present two protocols, \(\mathbb{Z}_n\)-to-\(\mathbb{Z}_2\) and \(\mathbb{Z}_2\)-to-\(\mathbb{Z}_n\), which convert to and fro between \(\mathbb{Z}_n\) sharing and bitwise \(\mathbb{Z}_2\) sharing. In addition to be the building blocks of the Comparison protocol, the \(\mathbb{Z}_n\)-to-\(\mathbb{Z}_2\) and \(\mathbb{Z}_2\)-to-\(\mathbb{Z}_n\) protocols establish the possibility of secure computation for all functions. Albeit the inefficiency, we can always apply Yao’s circuit evaluation idea after the \(\mathbb{Z}_n\)-to-\(\mathbb{Z}_2\) protocol and followed by the \(\mathbb{Z}_2\)-to-\(\mathbb{Z}_n\) protocol. These two protocols make our proposal as general as the classic circuit approaches.

**Definition 4.2 (\(\mathbb{Z}_n\)-to-\(\mathbb{Z}_2\))** Party 1 and Party 2 share a number in \(\mathbb{Z}_n\), and they want to securely convert the \(\mathbb{Z}_n\) sharing into bitwise \(\mathbb{Z}_2\) sharing. More specifically, Party 1 and Party 2 want to collaboratively execute the secure protocol \((x_1, x_2) \mapsto ((y_0^1, \ldots, y_k^1), (y_0^2, \ldots, y_k^2))\) such that \((y_k^1 y_k^2 - 1 \cdots y^1 y^0) \equiv x_1 + x_2\), where \(x_1, x_2 \in \mathbb{Z}_n\), \(y_1^1, y_2^1 \in \mathbb{Z}_2\), and \(y^i = y_1^i + y_2^i\) (mod 2).

To convert from \(\mathbb{Z}_n\) sharing to bitwise \(\mathbb{Z}_2\) sharing, we emulate the carry ripple adder with binary Scalar-product protocol, whose \(n = 2\). Let \(x_1 = (x_1^1 \cdots x_1^k), x_2 = (x_2^1 \cdots x_2^k),\) and the adder operates as long addition:

\[
\begin{align*}
&\phantom{=} c^{k+1} \quad c^k \ldots \quad c_1 \quad c^0 \\
= &\quad x_1^1 \ldots \quad x_1^k \quad x_1^0 \\
&\quad + \quad x_2^1 \ldots \quad x_2^k \quad x_2^0 \\
= &\quad y^1 \ldots \quad y^k \quad y^0
\end{align*}
\]

where \(c^0 = 0\) and \(c^{i+1} = c^i x_1^i + c^i x_2^i + x_1^i x_2^i\) (mod 2) are the carry bits; \(y^i = c^i + x_1^i + x_2^i\) (mod 2) is the \(i\)-th summation bit. Next, the \(\mathbb{Z}_n\)-to-\(\mathbb{Z}_2\) protocol is as follows:

**PROTOCOL \(\mathbb{Z}_n\)-to-\(\mathbb{Z}_2\) (\(n = 2^{k+1}\))**

1. Party \(j\) sets \(c_j^0 = 0\), and \(y_j^0 = x_j^0\), for \(j = 1, 2\).
2. For \(i = 0, \ldots, k - 1\), repeat Step 2a to Step 2b.

(a) The two parties jointly execute the binary Scalar-product protocol

\[
((c_1^i, x_1^i, x_1^0), (x_2^i, c_2^i, x_2^0)) \mapsto (t_1^i, t_2^i),
\]

where

\[
t_1^i + t_2^i \equiv x_1^i x_2^i + x_1^i c_2^i + x_1^i x_2^i \pmod{2}.
\]

(b) For \(j = 1, 2\), Party \(j\) computes

\[
c_j^{i+1} = c_j^i x_1^i + t_j^i \pmod{2}
\]

\[
y_j^{i+1} = x_j^{i+1} + c_j^{i+1} \pmod{2}
\]

**Definition 4.3 (\(\mathbb{Z}_2\)-to-\(\mathbb{Z}_n\))** Party 1 and Party 2 share a number in \(\mathbb{Z}_2\), and they want to securely convert the bitwise \(\mathbb{Z}_2\) sharing into the \(\mathbb{Z}_n\) sharing. More specifically, the two parties want to execute the secure protocol \(((x_1^1, \ldots, x_1^k), (x_2^1, \ldots, x_2^k)) \mapsto (y_1, y_2)\) such that \(y_1 + y_2 = (x_1^k x_2^k - 1 \cdots x_1 x_2)\), where \(x_1^i, x_2^i \in \mathbb{Z}_2, y_1, y_2 \in \mathbb{Z}_n\), and \(x^i = x_1^i + x_2^i\) (mod 2).

\[\text{Since } n = 2^{k+1}, \text{ the overflow bit } c^{k+1} \text{ is discarded.}\]
According to the above requirement, the outputs can be rewritten as the following function:

\[ y_1 + y_2 = \sum_{i=0}^{k} x_i \cdot 2^i = \sum_{i=0}^{k} (x_1 + x_2 \mod 2) \cdot 2^i = \sum_{i=0}^{k} (x_1 + x_2 - 2x_1^2) \cdot 2^i = \sum_{i=0}^{k} x_i \cdot 2^i + \sum_{i=0}^{k} x_i \cdot 2^i - \sum_{i=0}^{k} x_i^2 \cdot 2^{i+1} \]

The principle of the above function rewrite is to divide the computation into two parts: locally computable part \((\sum x_i, 2^i)\) and the collaboration part \((\sum x_i^2 \cdot 2^{i+1})\).

**PROTOCOL Z_2-to-Z_n (n = 2^{k+1})**

1. Party 1 and Party 2 jointly run the Scalar-product protocol \(((2x_1^1, \ldots, 2^{k+1} x_1^k), (x_2^1, \ldots, x_2^k)) \Rightarrow (t_1, t_2)\) such that \(t_1 + t_2 = 2x_1^1 \cdot x_2^1 + \ldots + 2^{k+1} x_1^k \cdot x_2^k\).
2. Party 2 computes \(y_2 = \sum_{i=0}^{k} x_i \cdot 2^i - t_j\), for \(i = 1, 2\).

**Definition 4.4 (Comparison)** Party 1 and Party 2 share a number in \(Z_n\), and they want to know the sign of the number. In other words, they want to collaboratively execute the secure protocol \((x_1, x_2) \Rightarrow (y_1, y_2)\) such that

\[ y_1 + y_2 = \begin{cases} 1 & \text{if } x_1 + x_2 < 0, \\ 0 & \text{otherwise.} \end{cases} \]

The protocol details are as follows:

**PROTOCOL Comparison**

1. Two parties collaboratively execute the \(Z_n\)-to-\(Z_2\) protocol \((x_1, x_2) \Rightarrow ((b_1, b_2), (b_3, b_4))\), such that \(b' = b_1 + b_2 \mod 2\), and \((b^k \cdot b^k_2) = x_1 + x_2\).
2. Party 1 and Party 2 collaboratively execute the \(Z_2\)-to-\(Z_n\) protocol \((b_1, b_2) \Rightarrow (y_1, y_2)\), such that \(y_1 + y_2 = (b^k)_2\) and \(b^k = b_1 + b_2 (\mod 2)\).

### 4.3 Integer Division

We construct our protocols over the finite group \(Z_n\), in which the division is normally defined as the multiplicative inverse to divisor’s multiplicative inverse. However, such definition is not practical, and neither is it feasible since element \(t \in Z_n\) may not even have multiplicative inverse if \(t\) and \(n\) are not coprime. As a result, we need to give division a practical and feasible definition, and we choose to follow the integer division in modern computers. Given two integers \(x, y \in \mathbb{N}\), the integer division is defined as the follows:

\[ \left\lfloor \frac{y}{x} \right\rfloor = q, \text{ where } y = q \cdot x + r, \text{ and } 0 \leq r < x. \]

Our solution to the Division protocol is actually an emulation for a \((k + 1)\)-bit divider. During the computation of \(\left\lfloor \frac{y}{x} \right\rfloor\), we iteratively check whether \(y \geq x \cdot 2^i\), for \(i = k - 1, \ldots, 0\). If it is true, the \(i\)-th bit of \(q\) is 1, and \(y\) is subtracted by \(x \cdot 2^i\); otherwise, the \(i\)-th bit of \(q\) is 0, and \(y\) remains untouched. This iterative method is actually the algorithm for long division.

However, we need to mention that it is not feasible to compute \(x \cdot 2^i\) in \(Z_n\) since we need double precision to correctly represent \(x \cdot 2^i\); for \(i = k - 1, \ldots, 0\); otherwise, \(x \cdot 2^i (\mod n)\) will give us unpredictable results. Therefore, in our solution we first convert both the dividend and the divisor from \(Z_n\) sharing to \(Z_n^2\) sharing, by which \(x \cdot 2^i\) can always be correctly represented. After the conversion, we emulate the divider with the Scalar-product protocol.

Before the Division protocol, we present the If-Then-Else protocol, which is not only the building block for the Division protocol but also useful for the function with alternatives.

**Definition 4.5 (If-Then-Else)** Party 1 and Party 2 additively share the predicate, IF-clause value, and the ELSE-clause value. They want to securely execute the protocol \(((b_1, x_1, y_1), (b_1, x_2, y_2)) \Rightarrow (z_1, z_2)\) such that

\[ z_1 + z_2 = \begin{cases} x_1 + x_2 & \text{if } b_1 + b_2 = 1 \\ y_1 + y_2 & \text{if } b_1 + b_2 = 0 \end{cases} \]

According to the above requirement, the outputs can be rewritten as the following function:

\[ z_1 + z_2 = (b_1 + b_2)(x_1 + x_2) + (1 - b_1 - b_2)(y_1 + y_2) = (x_1 + x_2) + (b_1 + b_2)(x_1 - y_1 + x_2 - y_2) \]

Again, with the strategy that dividing the components into locally computable ones and those need the Scalar-product protocols, we propose the following If-Then-Else protocol.

**PROTOCOL If-Then-Else**

1. Party \(j\) locally computes \(s_j = x_j - y_j\), for \(j = 1, 2\).
2. Party 1 and Party 2 collaboratively execute a Product protocol \(((b_1, s_1), (b_2, s_2)) \Rightarrow (t_1, t_2)\) such that \(t_1 + t_2 = (b_1 + b_2)(s_1 + s_2)\).
3. Party \(j\) locally computes \(z_j = t_j + x_j\), for \(j = 1, 2\).

Based on the Comparison, If-Then-Else, \(Z_2\)-to-\(Z_n\), and \(Z_n\)-to-\(Z_2\) protocols, we next define and introduce the following Division/Remainder protocol.

**Definition 4.6 (Integer Division/Remainder)** Two parties share the dividend and the divisor in \(Z_n\), and they want to jointly execute the secure protocol \(((x_1, y_1), (x_2, y_2)) \Rightarrow ((q_1, r_1), (q_2, r_2))\), where \(y_1 + y_2 = (q_1 + q_2)(x_1 + x_2) + (r_1 + r_2)\) and \(0 \leq (r_1 + r_2) < (q_1 + q_2)\).

**PROTOCOL Division/Remainder**
1. Party 1 and Party 2 collaboratively execute the $\mathbb{Z}_n$-to-$\mathbb{Z}_2$ protocol followed by the $\mathbb{Z}_2$-to-$\mathbb{Z}_n$ protocol,

$$(x_1, x_2) \mapsto ((b_1^0, \ldots, b_1^k), (b_2^0, \ldots, b_2^k))$$

$$\Rightarrow ((b_1^0, \ldots, b_1^{k+1}, 0, \ldots, 0), (b_2^0, \ldots, b_2^k, 0, \ldots, 0))$$

$$\mapsto (X_1, X_2),$$

where $X_1 + X_2 \pmod{n^2} = x_1 + x_2 \pmod{n}$.  

2. Party 1 and Party 2 collaboratively execute the $\mathbb{Z}_n$-to-$\mathbb{Z}_2$ protocol followed by the $\mathbb{Z}_2$-to-$\mathbb{Z}_n$ protocol,

$$(y_1, y_2) \mapsto ((c_1^0, \ldots, c_1^k), (c_2^0, \ldots, c_2^k))$$

$$\Rightarrow ((c_1^0, \ldots, c_1^{k+1}, 0, \ldots, 0), (c_2^0, \ldots, c_2^k, 0, \ldots, 0))$$

$$\mapsto (Y_1, Y_2),$$

where $Y_1 + Y_2 \pmod{n^2} = y_1 + y_2 \pmod{n}$.  

3. Party $j$ sets $Y_j = Y_j$, for $j = 1, 2$.  

4. For $i = k - 1, k - 2, \ldots, 0$, repeat Step 4a to Step 4d.

(a) Party $j$ computes $t_j = Y_j^{i+1} - X_j \cdot 2^i \pmod{n^2}$, for $j = 1, 2$.  

(b) Party 1 and Party 2 jointly run the Comparison protocol $(t_1, t_2) \mapsto (s_1, s_2)$, where

$$s_1 + s_2 \pmod{n^2} = \begin{cases} 1 & \text{if } t_1 + t_2 < 0 \\ 0 & \text{otherwise.} \end{cases}$$

(c) Party 1 and Party 2 run the If-Then-Else protocol $((s_1^0, 0, 0), (s_2^0, 0, 1)) \mapsto (q_1^0, q_2^0)$, where

$$q_1^0 + q_2^0 \pmod{n^2} = \begin{cases} 0 & \text{if } s_1^0 + s_2^0 = 1 \\ 1 & \text{if } s_1^0 + s_2^0 = 0 \end{cases}$$

(d) Party 1 and Party 2 run the If-Then-Else protocol $((s_1^0, Y_1^{i+1}, t_1), (s_2^0, Y_2^{i+1}, t_2)) \mapsto (Y_1', Y_2')$, where

$$Y_1' + Y_2' = \begin{cases} Y_1^{i+1} + Y_2^{i+1} & \text{if } s_1^0 + s_2^0 = 1 \\ t_1 + t_2 & \text{if } s_1^0 + s_2^0 = 0 \end{cases}$$

5. For $j = 1, 2$, Party $j$ computes $r_j = Y_j^0 \pmod{n}$, and

$$q_i = \sum_{j=0}^{k-1} q_j \cdot 2^j \pmod{n}.$$  

Finally, figure 1 gives the hierarchy of our construction.

5. Analysis

In Section 4 we elaborate on the protocol instructions, and we then list the table of complexity summarization here in Table 1. The complexity is measured in proportion to the Scalar-product protocol. The “Domain” and the “Dimension” are the inputs’ domain and the number of vector elements. Moreover, the “Round” is actually measured as the number of the Scalar-product protocol executions. According to the table, the Product, the $\mathbb{Z}_2$-to-$\mathbb{Z}_n$, and the If-Then-Else protocols have constant round complexity $O(1)$; the $\mathbb{Z}_n$-to-$\mathbb{Z}_2$ and the Comparison protocols have linear round complexity $O(k)$; and the Division protocol has quadratic round complexity $O(k^2)$. Recalled that $n = 2^{k+1}$, thus the round complexity here is based on the bit length of $n$.

![Figure 1. The hierarchy of our scalar-product-based protocols.](image)

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Domain</th>
<th>Dimension</th>
<th>Round</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product</td>
<td>$\mathbb{Z}_n$</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>$\mathbb{Z}_n$-to-$\mathbb{Z}_2$</td>
<td>$\mathbb{Z}_2$</td>
<td>3</td>
<td>$k$</td>
</tr>
<tr>
<td>$\mathbb{Z}_2$-to-$\mathbb{Z}_n$</td>
<td>$\mathbb{Z}_n$</td>
<td>$k+1$</td>
<td>1</td>
</tr>
<tr>
<td>If-Then-Else</td>
<td>$\mathbb{Z}_n$</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Comparison</td>
<td>$\mathbb{Z}_2$</td>
<td>3</td>
<td>$k$</td>
</tr>
<tr>
<td>$\mathbb{Z}_n$</td>
<td>$\mathbb{Z}_n$</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Division</td>
<td>$\mathbb{Z}_n$</td>
<td>$2k+2$</td>
<td>2</td>
</tr>
<tr>
<td>$\mathbb{Z}_n$</td>
<td>1</td>
<td>$k$</td>
<td></td>
</tr>
<tr>
<td>$\mathbb{Z}_n$</td>
<td>1</td>
<td>$k$</td>
<td></td>
</tr>
<tr>
<td>$\mathbb{Z}_n$</td>
<td>2</td>
<td>$2k$</td>
<td></td>
</tr>
</tbody>
</table>

Table 1. The complexity of our protocols

6. Specific Examples

To demonstrate the power of the primitives: the Product, the Comparison, and the Division protocols, we practically give two examples of real world computation and compose them with the primitives.

6.1. Example: Point Inclusion

Party 1 is located at $(x[1], x[2])$, and Party 2 has a circle described by its center $(x[1], x[2])$ and radius $r_2$. They want to know whether Part 1 is inside Party 2’s circle, but Party 1 will not disclose his location, and neither will Party 2 reveal the circle’s information. Therefore, they need a secure protocol $((x[1], x[2]), (x[1], x[2], r_2)) \mapsto (p_1, p_2)$ to satisfy the conditions such that

$$p_1 + p_2 = \begin{cases} 1 & \text{if } \sum_{i=1}^{2}(x[i] - x[i])^2 - r_2^2 < 0 \\ 0 & \text{otherwise.} \end{cases}$$

Based on the primitives proposed in Section 4, the Point-inclusion protocol can be constructed as the follows:

1. Party 1 and Party 2 collaboratively run the Product protocol

$$((k_1, x[1]), (n - x[k], n - x[k])) \mapsto (y[k], y[k])$$

where $y[k] = x[k] - x[k]^2$, for $k = 1, 2$.  

5

Authorized licensed use limited to: ACADEMIA SINICA COMPUTING CENTRE. Downloaded on January 2, 2009 at 20:01 from IEEE Xplore. Restrictions apply.
2. Party 1 computes \( t_1 = y[1]_1 + y[2]_1 \).
3. Party 2 computes \( t_2 = y[1]_2 + y[2]_2 - r_2^2 \).
4. Party 1 and Party 2 run the Comparison protocol \((t_1, t_2) \mapsto (p_1, p_2)\) such that \( p_1 + p_2 = \begin{cases} 1 & \text{if } t_1 + t_2 < 0 \\ 0 & \text{otherwise.} \end{cases} \)

6.2. Example: Variance

Party 1 has private input \( x[1]_1, \ldots, x[p_1]_1 \) and Party 2 has private input \( x[1]_2, \ldots, x[p_2]_2 \). They want to collaboratively and securely compute the variance of the union of their private inputs. More specifically, they need a protocol \(((x[1]_1, \ldots, x[p_1]_1), (x[1]_2, \ldots, x[p_2]_2)) \mapsto (q_1, q_2)\), where \( q_1 + q_2 = \sum_{i=1}^{p_1} x[i]_1^2 + \sum_{j=1}^{p_2} x[j]_2^2 \), with \( s_j = (p_1 + p_2) x[j], s_j = (p_1 + p_2) x[j] \), for \( j = 1, 2 \). Based on the primitives proposed in Section 4, the Variance protocol can be constructed as the follows:

1. Party \( j \) computes \( s_j = \sum_{i=1}^{p_j} x[i]_j^2 \), \( t_j = \sum_{i=1}^{p_j} x[i]_j \), for \( j = 1, 2 \).
2. Party 1 and Party 2 collaboratively execute the Product protocol \((p_1, s_1), (p_2, s_2) \mapsto (u_1, u_2)\) such that \( u_1 + u_2 = (p_1 + p_2)(s_1 + s_2) \).
3. Party 1 and Party 2 collaboratively run the Product protocol \(((t_1, t_2), (t', t')_2) \mapsto (v_1, v_2)\) such that \( v_1 + v_2 = (t_1 + t_2)(t_1 + t_2) \).
4. Party 1 and Party 2 collaboratively execute the Product protocol \((p_1, p_1), (p_2, p_2) \mapsto (w_1, w_2)\) such that \( w_1 + w_2 = (p_1 + p_2)(p_1 + p_2) \).
5. Party \( j \) computes \( z_j = u_j - v_j \), for \( j = 1, 2 \).
6. Party 1 and Party 2 jointly execute the Division protocol \(((w', z_1), (w_2, z_2)) \mapsto ((q_1, r_1), (q_2, r_2))\), such that \( q_1 + q_2 = \frac{x_1 + x_2}{w_1 + w_2} \).

7. Conclusions and Future Works

In this paper, a set of information theoretically secure two party protocols have been developed based on scalar product. The ultimate goal to design such protocols is to build a compiler for secure multiparty computation environments. The protocols presented in this paper is part of protocol along this line. More protocols need to be designed to achieve the ultimate goal.

References