Lecture Notes in Computer Science 16246

The series Lecture Notes in Computer Science (LNCS), including its subseries Lecture Notes in Artificial Intelligence (LNAI) and Lecture Notes in Bioinformatics (LNBI), has established itself as a medium for the publication of new developments in computer science and information technology research, teaching, and education.

LNCS enjoys close cooperation with the computer science R & D community, the series counts many renowned academics among its volume editors and paper authors, and collaborates with prestigious societies. Its mission is to serve this international community by providing an invaluable service, mainly focused on the publication of conference and workshop proceedings and postproceedings. LNCS commenced publication in 1973.

Goichiro Hanaoka · Bo-Yin Yang
Editors

Advances in Cryptology – ASIACRYPT 2025

31st International Conference on the Theory
and Application of Cryptology and Information Security
Melbourne, VIC, Australia, December 8–12, 2025
Proceedings, Part II

Springer

Editors

Goichiro Hanaoka
National Institute of Advanced Industrial
Science and Technology
Tokyo, Japan

Bo-Yin Yang
Academia Sinica
Taipei, Taiwan

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-981-95-5095-1 ISBN 978-981-95-5096-8 (eBook)
https://doi.org/10.1007/978-981-95-5096-8

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Preface

The 31st Annual International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt 2025) was held in Melbourne, Australia, on December 8–12, 2025. The conference covered all technical aspects of cryptology and was sponsored by the International Association for Cryptologic Research (IACR).

We received 533 paper submissions for Asiacrypt from around the world, which is exactly 100 more than last year's record-breaking number, setting a new all-time high. The Program Committee (PC) selected 143 papers for publication in the proceedings of the conference. As in the previous year, the Asiacrypt 2025 program had three tracks. Throughout the entire paper selection process, the ten Area Chairs made significant contributions. The two Program Co-chairs express their sincere gratitude to all the Area Chairs. The Area Chairs were Chris Brzuska for Fundamentals and Complexity Theory, Sherman Chow for Real-World Cryptography, Steven Galbraith for Higher Mathematics in Cryptography, Naofumi Homma for Efficient and Secure Implementations, Feng-Hao Liu for Public-Key Primitives with Advanced Functionalities, Takahiro Matsuda for Multi-party Computation and Zero-Knowledge, Manoj M. Prabhakaran for Information-Theoretic Cryptography, Damien Stehlé for Fully Homomorphic Encryption Theory and Practice, Meiqin Wang for Symmetric-Key Cryptography, and Keita Xagawa for Postquantum Cryptography. The Area Chairs kindly recommended excellent candidates for PC members and, in collaboration with the Discussion Leads, consolidated the opinions of the PC members within their respective areas to reach consensus. They then presented important recommendations regarding the acceptance or rejection of each paper to the Program Co-chairs. Furthermore, for submissions requiring additional reviews, they arranged for extra reviewers and, in some cases, conducted the reviews themselves. Beyond these dedicated contributions, they also provided many valuable insights and suggestions to support the Program Co-chairs in making key decisions. We are deeply grateful for their tremendous efforts. For submissions that the Area Chairs could not handle due to conflicts of interest, we asked the following four individuals to serve as substitute Area Chairs: Christian Rechberger, Yu Sasaki, Renaud Sirdey, and Frederik Vercauteren. We also extend our sincere appreciation to them for their dedicated support.

To review and evaluate the submissions, while keeping the load per PC member manageable, we selected as PC members 117 leading experts from all over the world, in all ten topic areas of cryptology, and we also had approximately 443 external reviewers, whose input was critical to the selection of papers. The review process was conducted using double-blind peer review. The conference operated a two-round review system with a rebuttal phase. This year, we continued the interactive rebuttal from Asiacrypt 2024. After the reviews and first-round discussions, PC members and area chairs selected 318 submissions to proceed to the second round. The remaining 215 papers were rejected, including 15 desk rejections. The authors were then invited to participate in a two-step interactive rebuttal phase, where the authors needed to submit a rebuttal in five days and then interact with the reviewers to address questions and concerns the following week. We believe the interactive form of the rebuttal encouraged discussions between the authors and the reviewers to clarify the concerns and contributions of the submissions and improved the review process. Then, after two weeks of second-round discussions (and more than two weeks of the shepherding process), the committee selected the final 143 papers to appear in these proceedings. Submissions received on average three reviews each during this process.

The PC nominated and voted for papers to receive the Best Paper Awards. The Best Theory Paper Award and the Best Early-Career Paper Award went to Tim Beyne and Michiel Verbauwhede for their paper "Integral cryptanalysis in characteristic p," the Best Practical Paper Award went to Charles Bouillaguet, Claire Delaplace, Mickaël Hamdad, and Damien Vergnaud for their paper "Practical cryptanalysis of pseudorandom correlation generators based on quasi-Abelian syndrome decoding," and the Best Early-Career Paper Award went to Thiago Bergamaschi and Naresh Boddu for their paper "On split-state quantum tamper detection." The authors of those three papers were invited to submit extended versions of their papers to the Journal of Cryptology. At Asiacrypt 2025, we were honored to have three Invited Talks delivered by Sherman Chow, Ron Steinfeld, and Peter Schwabe, respectively. We would like to express our sincere gratitude to these invited speakers as well. Following Asiacrypt 2024, we selected three PC members for the Distinguished PC Members Awards, nominated by the area chairs and program chairs. The Distinguished PC Members Awards went to Julia Kastner, Renaud Sirdey, and Jean-Pierre Tillich. As in the previous year, Asiacrypt 2025 included an artifact evaluation process. Authors of accepted papers were invited to submit associated artifacts, such as software or datasets, for archiving alongside their papers; 23 artifacts were submitted. Markku-Juhani O. Saarinen was the Artifact Chair and led an artifact evaluation committee of 12 members listed below. In the interactive review process between authors and reviewers, the goal was not just to evaluate artifacts but also to improve them. Artifacts that passed successfully through the artifact review process were publicly archived by the IACR at https://artifacts.iacr.org/.

Last, but not least, we would like to once again express our deep gratitude to everyone who contributed to Asiacrypt 2025. Without the diverse and extensive cooperation of all involved, the success of Asiacrypt 2025 would not have been possible. First and foremost, we sincerely thank all authors who submitted their valuable research results to Asiacrypt 2025. This year saw a significantly higher number of submissions than last year, and we understand that many authors may not have received the outcome they had hoped for despite the high quality of their work. To those authors as well, we extend our heartfelt thanks and wish them success in their future submissions. We also deeply appreciate the Area Chairs, PC members, and external reviewers, who actively engaged in discussions based on their highly specialized expertise to review this large volume of submissions. In organizing Asiacrypt 2025, we received tremendous support from General Chair Joseph Liu and his organizing team. Despite the unexpectedly large number of presentations, they provided an excellent venue and arrangements, for which we are truly grateful. Additionally, we would like to thank Kevin McCurley and Kay McKelly for their meticulous support in managing the website and review system. We are also deeply grateful to Kai-Min Chung and Yu Sasaki, who, drawing on their experience as

Program Co-chairs of last year's Asiacrypt, provided extremely helpful advice as Chairs at Large & Emeritus. We are also grateful for the helpful advice and organizational material provided to us by Crypto 2024 Program Co-chairs Leonid Reyzin and Douglas Stebila. We also thank the team at Springer for handling the publication of these conference proceedings.

December 2025

Goichiro Hanaoka
Bo-Yin Yang

Organization

General Chair

Joseph Liu	Monash University, Australia

Program Committee Chairs

Goichiro Hanaoka	AIST, Japan
Bo-Yin Yang	Academia Sinica, Taiwan

Area Chairs

Chris Brzuska	Aalto University, Finland
Sherman S. M. Chow	Chinese University of Hong Kong, China
Steven Galbraith	University of Auckland, New Zealand
Naofumi Homma	Tohoku University, Japan
Feng-Hao Liu	Washington State University, USA
Takahiro Matsuda	AIST, Japan
Manoj M. Prabhakaran	Indian Institute of Technology Bombay, India
Damien Stehlé	CryptoLab Inc., France
Meiqin Wang	Shandong University, China
Keita Xagawa	Technology Innovation Institute, UAE

Chairs at Large and Emeritus

Kai-Min Chung	Academia Sinica, Taiwan
Yu Sasaki	NTT Social Informatics Laboratories, Japan and NIST, USA

Program Committee

Adi Akavia	University of Haifa, Israel
Navid Alamati	VISA Research, USA
Elena Andreeva	TU Wien, Austria

Shi Bai	Florida Atlantic University, USA
Zhenzhen Bao	Tsinghua University, China
Ward Beullens	IBM Research Zurich, Switzerland
Tim Beyne	KU Leuven, Belgium
Shivam Bhasin	Nanyang Technological University, Singapore
Alexander Block	University of Illinois Chicago, USA
Jean-Philippe Bossuat	Gauss Labs, Switzerland
Pedro Branco	Bocconi University, Italy
Alex Bredariol Grilo	CNRS, France
Wouter Castryck	KU Leuven, Belgium
Sofía Celi	Brave, Portugal
Binyi Chen	Stanford University, USA
Shiyao Chen	Nanyang Technological University, Singapore
Yilei Chen	Tsinghua University, China
Wutichai Chongchitmate	Chulalongkorn University, Thailand
Tung Chou	Academia Sinica, Taiwan
Arka Rai Choudhuri	Nexus, USA
Chitchanok Chuengsatiansup	University of Klagenfurt, Austria
Michele Ciampi	University of Edinburgh, UK
Valerio Cini	Bocconi University, Italy
Alexandru Cojocaru	University of Edinburgh, UK
Daniel Collins	Texas A&M University, USA
Alain Couvreur	École Polytechnique, France
Bernardo David	IT University of Copenhagen, Denmark
Jean Paul Degabriele	Technology Innovation Institute, UAE
Patrick Derbez	University of Rennes, Inria, CNRS, IRISA, France
Jintai Ding	Xi'an Jiaotong-Liverpool University, China
Kirsten Eisentraeger	Penn State University, USA
Reo Eriguchi	AIST, Japan
Thomas Espitau	PQShield, France
Jun Furukawa	NEC Corporation, Japan
Rachit Garg	New York University, USA
Benedikt Gierlichs	KU Leuven, Belgium
Aarushi Goel	Purdue University, USA
Dawu Gu	Shanghai Jiao Tong University, China
Mohammad Hajiabadi	University of Waterloo, Canada
Minki Hhan	University of Texas at Austin, USA
Kai Hu	Shandong University, China
Michael Hutter	University of the Bundeswehr Munich & PQShield, Germany
Yasuhiko Ikematsu	Kyushu University, Japan

Takanori Isobe	University of Osaka, Japan
Tibor Jager	Wuppertal University, Germany
Ashwin Jha	Ruhr-University of Bochum, Germany
Haodong Jiang	Henan Key Laboratory of Network Cryptography Technology, China
Zhenzhong Jin	Northeastern University, USA
Fatih Kaleoglu	JPMorganChase, USA
Chethan Kamath	IIT Bombay, India
Matthias J. Kannwischer	Chelpis Quantum Corp, Taiwan
Julia Kastner	CWI, Netherlands
Miran Kim	Hanyang University, South Korea
Elena Kirshanova	Technology Innovation Institute, UAE
David Kohel	Aix-Marseille Université, France
Srijita Kundu	University of Waterloo, Canada
Qiqi Lai	Shaanxi Normal University, China
Keewoo Lee	University of California, Berkeley, USA
Tancrède Lepoint	Amazon Web Services (Security), USA
Xiao Liang	City University of Hong Kong, China
Wei-Kai Lin	University of Virginia, USA
Tianren Liu	Peking University, China
Fukang Liu	Science Tokyo, Japan
Chen-Da Liu-Zhang	Lucerne University of Applied Sciences and Arts & Web3 Foundation, Switzerland
Julian Loss	CISPA, Germany
Stefan Lucks	Bauhaus-Universität Weimar, Germany
Hemanta Maji	Purdue University, USA
Florian Mendel	Infineon Technologies, Germany
Bart Mennink	Radboud University, Netherlands
Hart Montgomery	Linux Foundation, USA
Thorben Moos	UCLouvain, Belgium
Tomoyuki Morimae	Kyoto University, Japan
Khoa Nguyen	University of Wollongong, Australia
Maciej Obremski	National University of Singapore, Singapore
Hiroshi Onuki	University of Tokyo, Japan
Anat Paskin-Cherniavsky	Ariel University, Israel
Peter Pessl	Infineon Technologies, Germany
Christophe Petit	University of Birmingham, UK and Université libre de Bruxelles, Belgium
Rachel Player	Royal Holloway, University of London, UK
Bertram Poettering	IBM Research Europe – Zurich, Switzerland
Antigoni Polychroniadou	J.P. Morgan AI Research & AlgoCRYPT CoE, USA

Manoj M. Prabhakaran	Indian Institute of Technology Bombay, India
Luowen Qian	NTT Research, Inc., USA
Sebastian Ramacher	AIT Austrian Institute of Technology, Austria
Christian Rechberger	TU Graz, Austria
Adeline Roux-Langlois	CNRS, GREYC, France
Lawrence Roy	Aarhus University, Denmark
Sujoy Sinha Roy	Graz University of Technology, Austria
Markku-Juhani Saarinen	Tampere University, Finland
Amin Sakzad	Monash University, Australia
Simona Samardjiska	Radboud University, Netherlands
Paolo Santini	Marche Polytechnic University, Italy
Pascal Sasdrich	Ruhr University Bochum, Germany
André Schrottenloher	Inria Rennes, France
Sruthi Sekar	IIT Bombay, India
Srinath Setty	Microsoft Research, USA
Renaud Sirdey	CEA, France
Daniel Slamanig	Universität der Bundeswehr München, Germany
Ling Song	Jinan University, China
Yongsoo Song	Seoul National University, South Korea
Ron Steinfeld	Monash University, Australia
Qiang Tang	University of Sydney, Australia
Jean-Pierre Tillich	Inria de Paris, France
Ha Tran	University of Alberta, Canada
Monika Trimoska	Eindhoven University of Technology, Netherlands
Yiannis Tselekounis	Royal Holloway, University of London, UK
Rei Ueno	Kyoto University, Japan
Frederik Vercauteren	KU Leuven, Belgium
Benedikt Wagner	Ethereum Foundation, Germany
Mingyuan Wang	NYU Shanghai, China
Zhedong Wang	Shanghai Jiao Tong University, China
Thom Wiggers	PQShield, Netherlands
Shota Yamada	AIST, Japan
Takashi Yamakawa	NTT, Japan
Yu Yu	Shanghai Jiao Tong University, China
Hong-Sheng Zhou	Virginia Commonwealth University, USA
Aron van Baarsen	Aarhus University, Denmark
Akin Ünal	Institute of Science and Technology Austria, Austria

Additional Reviewers

Balthazar Bauer
Sidhant Saraogi
Michel Abdalla
Damiano Abram
Hamza Abusalah
Anasuya Acharya
Amit Agarwal
Aikata Aikata
Nouri Alnahawi
Saed Alsayigh
Hiroaki Anada
Ravi Anand
Yoshinori Aono
Evan Apinis
Sarah Arpin
Roderick Asselineau
Thomas Attema
Benedikt Auerbach
Daniel Augot
Gennaro Avitabile
Karen Azari
Renas Bacho
Kano Bacho
David Balbás
Shalini Banerjee
Fabio Banfi
Laasya Bangalore
Subhadeep Banik
Anaïs Barthoulot
James Bartusek
Andrea Basso
Michele Battagliola
Kit Battarbee
Carsten Baum
Tamar Ben-David
Adda-Akram Bendoukha
Barbara Jiabao Benedikt
Francesco Berti
Rishabh Bhadauria
Amit Singh Bhati
Amit Singh Bhati
Arghya Bhattacharjee
Rishiraj Bhattacharyya
Ritam Bhaumik
Alexander Bienstock
Estelle Blin
Maxime Bombar
Antonina Bondarchuk
Jonathan Bootle
Sebastiano Boscardin
Vincenzo Botta
Samuel Bouaziz-Ermann
Aymen Boudguiga
Alexandre Bouez
Christina Boura
Konstantinos Brazitikos
Pierre Briaud
Colten Brunner
Dung Bui
Jean-Paul Bultel
Julien Béguinot
Luca Campa
Isaac Andres Canales Martínez
Kevin Carrier
Ignacio Cascudo
Gaëtan Cassiers
Enrique Cervero-Martin
Rutchathon Chairattana-Apirom
Avik Chakraborti
Olive Chakraborty
Kaushik Chakraborty
Suvradip Chakraborty
Debasmita Chakraborty
Hubert Chan
Rohit Chatterjee
Marina Checri
Mingjie Chen
Long Chen
Jie Chen
Yincen Chen
Liyan Chen
Clémence Chevignard
James Chiang
James Hsin-yu Chiang
Sohto Chiku
Wonhee Cho

Hyeongmin Choe
Antoine Choffrut
Wonseok Choi
Hao Chung
Pierre-Emmanuel Clet
Léo Colisson
Craig Costello
Jolijn Cottaar
Elizabeth Crites
Miguel Cueto Noval
Shujie Cui
Hongrui Cui
Jiamin Cui
Pierrick Dartois
Dipayan Das
Thomas Debris-Alazard
Thomas Decru
Mathieu Degre
Hugo Delavenne
Pierpaolo Della Monica
Gabriel Dettling
Lalita Devadas
Xiaohui Ding
Lin Ding
Joao Diogoduarte
Christoph Dobraunig
Jack Doerner
Antoine Douteau
Rafael Dowsley
Minxin Du
Qiuyan Du
Li Duan
Léo Ducas
Clement Ducros
Jesko Dujmovic
Jules Dumezy
Dung Hoang Duong
Moumita Dutta
Maria Eichlseder
Fatima Elsheimy
Saroja Erabelli
Daniel Escudero
Andre Esser
Marie Euler
Frederic Ezerman
Zhang Fahong
Sebastian Faller
Antonio Faonio
Joël Felderhoff
Jakob Feldtkeller
Yansong Feng
Hanwen Feng
Houda Ferradi
Chase Fickes
Marc Fischlin
Christian Forler
Tore Kasper Frederiksen
Daniele Friolo
Masayuki Fukumitsu
Hiroki Furue
Philippe Gaborit
Phillip Gajland
Mariana Gama
Shuhong Gao
Gayathri Garimella
Christina Garman
Robin Geelen
Baptiste Germon
Diana Ghinea
Ashrujit Ghoshal
Valerie Gilchrist
Emanuele Giunta
Eli Goldin
Junqing Gong
Boru Gong
Suchetana Goswami
Rishab Goyal
Lorenzo Grassi
Milos Grujic
Jiaxin Guan
Aurore Guillevic
Antonio Guimaraes
Aditya Gulati
Chun Guo
Yue Guo
Hao Guo
Christoph U. Günther
Hosein Hadipour
Mike Hamburg
Shuai Han

Lucas Hanouz
Lucjan Hanzlik
Keisuke Hara
Shingo Hasegawa
Keitaro Hashimoto
Valerian Hatey
Jinye He
Jiahui He
Aditya Hegde
Rachelle Heim
Lena Heimberger
Raphael Heitjohann
Julius Hermelink
Taiga Hiroka
Keitaro Hiwatashi
Christian Holler
Alexander Hoover
Akinori Hosoyamada
Kristina Hostakova
Chengan Hou
Shiqi Hou
Marc Houben
Martha Hovd
Yao-Ching Hsieh
Yuncong Hu
Yu-Hsuan Huang
Akiko Inoue
Akira Ito
Ryoma Ito
Samuel Jose Garcia Garcia
Nikai Jagganath
Fatemeh Jalalvand
Amit Jana
Hansraj Jangir
Jake Januzelli
Weidan Ji
Liheng Ji
Haoxiang Jin
Hyungrok Jo
Eda Kirimli
Daniel Kales
Anders Kallesøe
Dina Kamel
Simon Kamp
Jiayi Kang

Minsik Kang
Bhavana Kanukurthi
Upendra Kapshikar
Alexandr Karenin
Harish Karthikeyan
Shuichi Katsumata
Jonathan Katz
Yutaka Kawai
Andes Y. L. Kei
Mahimna Kelkar
John Kelsey
Mustafa Khairallah
Dmitry Khovratovich
Duhyeong Kim
Taeseong Kim
Fuyuki Kitagawa
Ivana Klasovita
Christian Knabenhans
Lisa Kohl
Sebastian Kolby
Jonathan Komada Eriksen
Swastik Kopparty
Thomas Korak
Gaurish Korpal
Katharina Koschatko
Veronika Kuchta
Naman Kumar
Dilip Kumar S. V.
Simran Kumari
Po-Chun Kuo
Péter Kutas
Paweł Kędzior
Yi-Fu Lai
Nathalie Lang
Roman Langrehr
Oleksandra Lapiha
Jun Bo Lau
Abel Laval
Dania Lazzarini
Jason LeGrow
Joon-Woo Lee
Yongwoo Lee
Changmin Lee
Hyeonbum Lee
Charlotte Lefevre

Anja Lehmann
Dominik Leichtle
Axel Lemoine
Doryan Lesaignoux
Andrea Lesavourey
Jannis Leuther
Laura Lewis
Yu Li
Muzhou Li
Muzhou Li
Afonso Li
Peigen Li
Shiyu Li
Yang Li
Junru Li
Yanan Li
Xiling Li
Zeyong Li
Yao-Ting Lin
Eik List
Zeyu Liu
Xiangyu Liu
Qun Liu
Qipeng Liu
Chen Lotan
Yu-Cheng Lu
Jinyu Lu
Mingqi Lu
George Lu
Vihaan Luhariwala
Ji Luo
Zhongtang Luo
Yingjie Lyu
Shanxiang Lyu
Saswata Mukherjee
Yiping Ma
Lorenzo Magliocco
Bernardo Magri
Luciano Maino
Monosij Maitra
Janmajaya Mal
Mary Maller
Sougata Mandal
Varun Maram
Laurane Marco
Elizabeth Margolin
Chloe Martindale
Christian Matt
Noam Mazor
Willi Meier
Fredrik Meisingseth
Nikolas Melissaris
Fei Meng
Antoine Mesnard
Pierre Meyer
Francesco Migliaro
Kazuhiko Minematsu
Omid Mir
Anuja Modi
Deep Inder Mohan
Charles Momin
Rocco Mora
Tomoki Moriya
Travis Morrison
Tamer Mour
Changrui Mu
Garazi Muguruza
Anisha Mukherjee
Ananta Mukherjee
Guilhem Mureau
Mari Muurman
Gina Muuss
Anne Müller
Jordan Naccache (Ethan)
Michael Naehrig
Marcel Nageler
Yusuke Naito
Kohei Nakagawa
Wenjie Nan
Shintaro Narisada
Shafik Nassar
María Naya-Plasencia
Tom Neuschulten
Tran Ngo
Ruben Niederhagen
Guilhem Niot
Aysan Nishaburi
Ryo Nishimaki
Zhongfeng Niu
Wakaha Ogata

Kazuma Ohara
Ryo Ohashi
Shinya Okumura
Michał Osadnik
Alex Ozdemir
Adam O'Neill
Hugo Pacheco
Tapas Pal
Jiaxin Pan
Lorenz Panny
Charalampos Papamanthou
Eugenio Paracucchi
Jai Hyun Park
Jeongeun Park
Aditi Partap
Alain Passelègue
Sikhar Patranabis
Alice Pellet-Mary
Olivier Pereira
Octavio Perez Kempner
Ray Perlner
Simone Perriello
Thomas Peters
Minh Pham
Duc Tu Pham
Xuanrong Piao
Aurel Pichollet-Mugnier
Rafael del Pino
Simon Pohmann
Guru Vamsi Policharla
Yuriy Polyakov
Thomas Prest
Daniel Pöllmann
Yue Qin
Tian Qiu
Sarawathy R. V.
Seyoon Ragavan
Mostafizar Rahman
Lars Ran
Shahram Rasoolzadeh
Divya Ravi
Michael Reichle
Krijn Reijnders
Marc Renard
Omar Renawi
Emeline Repel
Jan Richter-Brockmann
Peter Rindal
Silvia Ritsch
Michael Rosenberg
Arnab Roy
Ryan Rueger
Yusuke Sakai
Kosei Sakamoto
Samipa Samanta
Giacomo Santato
Bagus Santoso
Santanu Sarkar
Swagata Sasmal
Rahul Satish
Shingo Sato
Leonard Schild
Martin Schläffer
Fabian Schmid
Phil Schmieder
Peter Scholl
Jan Schoone
Jacob C. N. Schuldt
Robert Schädlich
Gabrielle Scullard
Melvin Seitner
Nicolas Sendrier
Hwajeong Seo
Yaobin Shen
Yipeng Shi
Kaiyan Shi
SeongHan Shin
Igor Shparlinski
Mark Simkin
Priyanshu Singh
Satvinder Singh
Adi Sireesh
Mathias Soeken
Nada Somswasdi
Yongha Son
Pratik Soni
Jannik Spiessens
Sebastian A. Spindler
Gabriele Spini
Sriram Sridhar

Adwaiya Srivastav
Oana Stan
Francois-Xavier Standaert
Miha Stopar
Roy Stracovsky
Patrick Struck
Marc Stöttinger
Ling Sun
Shi-Feng Sun
Siwei Sun
Bing Sun
Erkan Tairi
Akira Takahashi
Taisei Takahashi
Atsushi Takayasu
Kaoru Takemure
Ernest Tan
Yuhao Tang
Khai Hanh Tang
Gang Tang
Chengdong Tao
Brady Testa
Lea Thiemt
Tian Tian
Mehdi Tibouchi
Marcel Tiepelt
Tyge Tiessen
Saliha Tokat
Toi Tomita
Daphné Trama
Nam Tran
Stefano Trevisani
Ni Trieu
Ida Tucker
Nirvan Tyagi
Ioannis Tzannetos
Aleksei Udovenko
Dominique Unruh
Bart Van Vulpen
Marloes Venema
Michiel Verbauwhede
Javier Verbel
Psi Vesely
Hilder Vitor Lima Pereira
Jelle Vos
Quoc-Huy Vu
Hendrik Waldner
Alexandre Wallet
Linya Wang
Yuyu Wang
Xiaoyu Wang
Zhiheng Wang
Hongxiao Wang
Qingju Wang
Yuntao Wang
Jianhua Wang
Geng Wang
Libo Wang
Xinzhou Wang
Chenke Wang
Shichang Wang
Gaoli Wang
Haoyang Wang
Jiafan Wang
Violetta Weger
Christian Weinert
Weiqiang Wen
Chenkai Weng
Andreas Weninger
Stella Wohnig
Harry W. H. Wong
David Wu
Ke Wu
Zhili Wu
Yu Xia
Wenwen Xia
Zejun Xiang
Yuting Xiao
Jiajun Xin
Jiayu Xu
Yanhong Xu
Haiyang Xue
Aayush Yadav
Anshu Yadav
Saikumar Yadugiri
Sophia Yakoubov
Kyosuke Yamashita
Yingfei Yan
Luhan Yan
Naoto Yanai

Rupeng Yang
Kang Yang
Yu Yang
Qianqian Yang
Masaya Yasuda
Xiaxi Ye
Randy Yee
Yongdong Yeo
Kevin Yeo
Kazuki Yoneyama
William Youmans
Yuanzhuo Yu
Albert Yu
Aaram Yun
Chak Fai Yung
Álvaro Yángüez
Thomas Zacharias
Hadas Zeilberger
Runzhi Zeng
Yinuo Zhang
Yanhua Zhang
Tianyu Zhang
Liu Zhang
Yingjie Zhang
Kai Zhang
Yinuo Zhang
Ziyu Zhao
Yi Zhao
Raymond Zhao
Mingxun Zhou
Biming Zhou
Zhelei Zhou
Chenzhi Zhu
Floyd Zweydinger
Thomas den Hollander
Wessel van Woerden
Jonas von der Heyden
Marius Årdal
Alper Çakan

Artifact Chair

Markku-Juhani O. Saarinen	Tampere University, Finland

Artifact Evaluation Committee

Sebastiano Boscardin	Eindhoven University of Technology, Netherlands
Charles Bouillaguet	Sorbonne University, France
Eros Camacho-Ruiz	Instituto de Microelectrónica de Sevilla, Spain
Fabrizio De Santis	Siemens AG, Germany
Matthias Kannwischer	Chelpis Quantum Corporation, Taiwan
Katharina Koschatko	Graz University of Technology, Austria
Pablo Navarro-Torrero	Instituto de Microelectrónica de Sevilla, Spain
Reyhaneh Rabbaninejad	Tampere University, Finland
Krijn Reijnders	KU Leuven, Belgium
Sachin Shukla	Microsoft, USA
Mohamed Soliman	Tampere University, Finland
Mert Yassi	Monash University, Australia

Contents

Secure Messaging

Formalization and Key Exchange

Data Structures

Blockchain

Secure Implementations

Design and Analysis of Implementations