

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, 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, 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 the PC members consisting of 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.



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 Verbauwheide for their paper “Integral cryptanalysis in characteristic p ,” the Best Practical Paper Award went to Charles Bouil-laguet, 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 are 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	The Chinese University of Hong Kong, Hong Kong
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	TII, UAE

Chairs at Large & Emeritus

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

Program Committee

Adi Akavia	U. 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 at Chicago, USA	
	Jean-Philippe Bossuat	Gauss Labs, Switzerland	
	Pedro Branco	Bocconi, Italy	
	Alex Bredariol Grilo	CNRS, France	
	Wouter Castryck	Leuven, Belgium	
	Sofia Celi	Brave, Portugal	
	Binyi Chen	Stanford University, USA	
	Shiyao Chen	Nanyang Technological University, Singapore	
	Yilei Chen	Tsinghua University, China	
	Wutichai Chongchitmate	Chulalongkorn University, Thai	
	Tung Chou	Academia Sinica, Taiwan	
	Arka Rai Choudhuri	Nexus, USA	
	Chitchanok Chuengsatian	The University of Klagenfurt, Austria	
	sup		
	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	Ecole Polytechnique, France	
	Bernardo David	IT University of Copenhagen, Denmark	
	Jean Paul Degabriele	TII, UAE	
	Patrick Derbez	Univ Rennes, Inria, CNRS, IRISA, France	
	Jintai Ding	the Xian Jiao Tong – Liverpool University, China	
	Kirsten Eisentraeger	Penn State, 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	UT Austin, USA	
	Kai Hu	Shandong University, China	
	Michael Hutter	UniBwM & PQShield, Germany	
	Yasuhiko Ikematsu	Kyushu Univ., Japan	
	Takanori Isobe	The 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, 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, Korea
Elena Kirshanova	Technology Innovation Institute, UAE
 David Kohel	Marseille , France
Srijita Kundu	University of Waterloo, Canada
Qiqi Lai	School of Computer Science , Shaanxi Normal University, China
 Keewoo Lee	UC Berkeley, USA
Jancrede Lepoint	Amazon Web Services (Security), USA
Xiao Liang	CUHK , Hong Kong
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 U , Japan
Khoa Nguyen	University of Wollongong, Australia
Maciej Obremski	National University of Singapore, Singapore
Hiroshi Onuki	The University of Tokyo, Japan
Anat Paskin-Cherniavsky	Ariel University, Israel
Peter Pessl	Infineon Technologies, Germany
Christophe Petit	Birmingham/Brussels , UK/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, France
Lawrence Roy	Aarhus University, Denmark
Sujoy Sinha Roy	Graz University of Technology, Austria
Markku-Juhani Saarinen	Tampere University, Finland
Amin Sakzad	Monash U , 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, Korea
Ron Steinfeld	Monash University, Australia
Qiang Tang	The 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 Jiaotong University, China
Hong-Sheng Zhou	Virginia Commonwealth University, USA
Aron van Baarsen	Aarhus University, Denmark
Akin Ünal	ISTA , Austria


Additional Reviewers

Balthazar Bauer	Daniel Augot
Sidhant Saraogi	Gennaro Avitabile
Michel Abdalla	Karen Azari
Damiano Abram	Renas Bacho
Hamza Abusalah	Kano Bacho
Anasuya Acharya	David Balbás
Amit Agarwal	Shalini Banerjee
Aikata Aikata	Fabio Banfi
Nouri Alnahawi	Laasya Bangalore
Saed Alsayigh	Subhadeep Banik
Hiroaki Anada	Anaïs Barthoulot
Ravi Anand	James Bartusek
Yoshinori Aono	Andrea Basso
Evan Apinis	Michele Battagliola
Sarah Arpin	Kit Battarbee
Roderick Asselineau	Carsten Baum
Thomas Attema	Tamar Ben-David
Benedikt Auerbach	Adda-Akram Bendoukha

Barbara Jiabao Benedikt	Clémence Chevignard
Francesco Berti	James Chiang
Rishabh Bhadauria	James Hsin-yu Chiang
Amit Singh Bhati	Sohto Chiku
Amit Singh Bhati	Wonhee Cho
Arghya Bhattacharjee	Hyeongmin Choe
Rishiraj Bhattacharyya	Antoine Choffrut
Ritam Bhaumik	Wonseok Choi
Alexander Bienstock	Hao Chung
Estelle Blin	Pierre-Emmanuel Clet
Maxime Bombar	Léo Colisson
Antonina Bondarchuk	Craig Costello
Jonathan Bootle	Jolijn Cottaar
Sebastiano Boscardin	Elizabeth Crites
Vincenzo Botta	Miguel Cueto Noval
Samuel Bouaziz–Ermann	Shujie Cui
Aymen Boudguiga	Hongrui Cui
Alexandre Bouez	Jiamin Cui
Christina Boura	Pierrick Dartois
Konstantinos Brazitikos	Dipayan Das
Pierre Briaud	Thomas Debris-Alazard
Colten Brunner	Thomas Decru
Dung Bui	Mathieu Degre
Jean-Paul Bultel	Hugo Delavenne
Julien Béguinot	Pierpaolo Della Monica
Luca Campa	Gabriel Dettling
Isaac Andres Canales Martínez	Lalita Devadas
Kevin Carrier	Xiaohui Ding
Ignacio Cascudo	Lin Ding
Gaëtan Cassiers	Joao Diogoduarte
Enrique Cervero-Martin	Christoph Dobraunig
Rutchathon Chairattana-Apirom	Jack Doerner
Avik Chakraborti	Antoine Douteau
Olive Chakraborty	Rafael Dowsley
Kaushik Chakraborty	Minxin Du
Suvradip Chakraborty	Qiuyan Du
Debasmita Chakraborty	Li Duan
Hubert Chan	Léo Ducas
Rohit Chatterjee	Clement Ducros
Marina Checchi	Jesko Dujmovic
Mingjie Chen	Jules Dumezy
Long Chen	Dung Hoang Duong
Jie Chen	Moumita Dutta
Yincen Chen	Maria Eichlseder
Liyan Chen	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 Korpai
 Katharina Koschatko
 Veronika Kuchta
 Naman Kumar
 Dilip Kumar **SV**
 Simran Kumari
 Po-Chun Kuo
 Péter Kutas
~~Péter Kutas~~
 Paweł Kedzior
 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
~~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
 ~~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 Schl  ffer
 Fabian Schmid
 Phil Schmieder
 Peter Scholl
 Jan Schoone
 Jacob C.N. Schuldt
 Robert Sch  dlich
 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
~~Miha Stopar~~
 Roy Stracovsky
 Patrick Struck
 Marc St  ttinger
 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
 Daphn   Trama
 Nam Tran
 Stefano Trevisani
 Ni Trieu
 Ida Tucker
 Nirvan Tyagi
 Ioannis Tzannetos



Aleksei Udovenko	Haiyang Xue
Dominique Unruh	Aayush Yadav
Bart Van Vulpen	Anshu Yadav
Marloes Venema	Saikumar Yadugiri
Michiel Verbauwhede	Sophia Yakoubov
Javier Verbel	Kyosuke Yamashita
Psi Vesely	Yingfei Yan
Hilder Vitor Lima Pereira	Luhan Yan
Jelle Vos	Naoto Yanai
Quoc-Huy Vu	Rupeng Yang
Hendrik Waldner	Kang Yang
Alexandre Wallet	Yu Yang
Linya Wang	Qianqian Yang
Yuyu Wang	Masaya Yasuda
Xiaoyu Wang	Xiaxi Ye
Zhiheng Wang	Randy Yee
Hongxiao Wang	Yongdong Yeo
Qingju Wang	Kevin Yeo
Yuntao Wang	Kazuki Yoneyama
Jianhua Wang	William Youmans
Geng Wang	Yuanzhuo Yu
Libo Wang	Albert Yu
Xinzhou Wang	Aaram Yun
Chenke Wang	Chak Fai Yung
Shichang Wang	Álvaro Yángüez
Gaoli Wang	Thomas Zacharias
Haoyang Wang	Hadas Zeilberger
Jiafan Wang	Runzhi Zeng
Violetta Weger	Yinuo Zhang
Christian Weinert	Yanhua Zhang
Weiqiang Wen	Tianyu Zhang
Chenkai Weng	Liu Zhang
Andreas Weninger	Yingjie Zhang
Stella Wahnig	Kai Zhang
Harry W. H. Wong	Yinuo Zhang
David Wu	Ziyu Zhao
Ke Wu	Yi Zhao
Zhili Wu	Raymond Zhao
Yu Xia	Mingxun Zhou
Wenwen Xia	Biming Zhou
Zejun Xiang	Zhelei Zhou
Yuting Xiao	Chenzhi Zhu
Jiajun Xin	Floyd Zweydinger
Jiayu Xu	Thomas den Hollander
Yanhong Xu	Wessel van Woerden

XVIII Preface

Jonas von der Heyden
Marius Årdal

Alper Çakan

Artifact Chair



Markku-Juhani
Saarinen

O.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	EChelpis Quantum Corporation, Taiwan
Katharina Koschatko	Graz University of Technology, Austria
Pablo Navarro-Torrero	Instituto de Microelectrónica de Sevilla, Spain



Reyhaneh **Rabbanine-**
jad Tampere University, Finland

Krijn Reijnders	KU Leuven, Belgium
Sachin Shukla	Microsoft, USA
Mohamed Soliman	Tampere University, Finland
Mert Yassi	Monash University, Australia

