

Founding Editors

Gerhard Goos

Karlsruhe Institute of Technology, Karlsruhe, Germany

Juris Hartmanis

Cornell University, Ithaca, NY, USA

Editorial Board Members

Elisa Bertino

Purdue University, West Lafayette, IN, USA

Wen Gao

Peking University, Beijing, China

Bernhard Steffen 

TU Dortmund University, Dortmund, Germany

Moti Yung 

Columbia University, New York, NY, USA

More information about this series at <https://link.springer.com/bookseries/558>

Shweta Agrawal · Dongdai Lin (Eds.)

Advances in Cryptology – ASIACRYPT 2022

28th International Conference on the Theory
and Application of Cryptology and Information Security
Taipei, Taiwan, December 5–9, 2022
Proceedings, Part I

Editors

Shweta Agrawal
Indian Institute of Technology Madras
Chennai, India

Dongdai Lin
Chinese Academy of Sciences
Beijing, China

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-031-22962-6

ISBN 978-3-031-22963-3 (eBook)

<https://doi.org/10.1007/978-3-031-22963-3>

© International Association for Cryptologic Research 2022

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The 28th Annual International Conference on Theory and Application of Cryptology and Information Security (ASIACRYPT 2022) was held in Taiwan during December 5–9, 2022.

The conference covered all technical aspects of cryptology, and was sponsored by the International Association for Cryptologic Research (IACR).

We received a total of 364 submissions from all over the world, and the Program Committee (PC) selected 98 papers for publication in the proceedings of the conference. The two program chairs were supported by a PC consisting of 79 leading experts in aspects of cryptology. Each submission was reviewed by at least three PC members (or their sub-reviewers). The strong conflict of interest rules imposed by IACR ensure that papers are not handled by PC members with a close working relationship with the authors. The two program chairs were not allowed to submit a paper, and PC members were limited to two submissions each. There were approximately 331 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. After the reviews and first-round discussions the PC selected 224 submissions to proceed to the second round and the authors were then invited to participate in an interactive rebuttal phase with the reviewers to clarify questions and concerns. The second round involved extensive discussions by the PC members.

Alongside the presentations of the accepted papers, the program of ASIACRYPT 2022 featured two invited talks by Jian Guo and Damien Stehlé. The conference also featured a rump session which contained short presentations on the latest research results of the field.

The four volumes of the conference proceedings contain the revised versions of the 98 papers that were selected. The final revised versions of papers were not reviewed again and the authors are responsible for their contents.

Using a voting-based process that took into account conflicts of interest, the PC selected the three top papers of the conference: “Full Quantum Equivalence of Group Action DLog and CDH, and More” by Hart Montgomery and Mark Zhandry, “Cryptographic Primitives with Hinting Property” by Navid Alamati and Sikhar Patranabis, and “SwiftEC: Shallue–van de Woestijne Indifferentiable Function to Elliptic Curves” by Jorge Chavez-Saab, Francisco Rodriguez-Henriquez, and Mehdi Tibouchi. The authors of all three papers were invited to submit extended versions of their manuscripts to the *Journal of Cryptology*.

Many people have contributed to the success of ASIACRYPT 2022. We would like to thank the authors for submitting their research results to the conference. We are very grateful to the PC members and external reviewers for contributing their knowledge and expertise, and for the tremendous amount of work that was done with reading papers and contributing to the discussions. We are greatly indebted to Kai-Min Chung and Bo-Yin Yang, the General Chairs, for their efforts and overall organization. We thank

Bart Preneel, Ron Steinfeld, Mehdi Tibouchi, Jian Guo, and Huaxiong Wang for their valuable suggestions and help. We are extremely grateful to Shuaishuai Li for checking all the \LaTeX files and for assembling the files for submission to Springer. We also thank the team at Springer for handling the publication of these conference proceedings.

December 2022

Shweta Agrawal
Dongdai Lin

Organization

General Chairs

Kai-Min Chung

Academia Sinica, Taiwan

Bo-Yin Yang

Academia Sinica, Taiwan

Program Committee Chairs

Shweta Agrawal

Indian Institute of Technology, Madras, India

Dongdai Lin

Institute of Information Engineering, Chinese
Academy of Sciences, China

Program Committee

Divesh Aggarwal

National University of Singapore, Singapore

Adi Akavia

University of Haifa, Israel

Martin Albrecht

Royal Holloway, University of London, UK

Ghada Almashaqbeh

University of Connecticut, USA

Benny Applebaum

Tel Aviv University, Israel

Lejla Batina

Radboud University, Netherlands

Carsten Baum

Aarhus University, Denmark

Sonia Belaïd

CryptoExperts, France

Mihir Bellare

University of California, San Diego, USA

Andrej Bogdanov

Chinese University of Hong Kong, China

Christina Boura

Université de Versailles, France

Ran Canetti

Boston University, USA

Jie Chen

East China Normal University, China

Yilei Chen

Tsinghua University, China

Jung Hee Cheon

Seoul National University, South Korea

Ilaria Chillotti

Zama, France

Michele Ciampi

The University of Edinburgh, UK

Craig Costello

Microsoft Research, USA

Itai Dinur

Ben-Gurion University, Israel

Nico Döttling

Helmholtz Center for Information Security
(CISPA), Germany

Maria Eichlseder

Graz University of Technology, Austria

Saba Eskandarian

University of North Carolina at Chapel Hill, USA

Marc Fischlin

TU Darmstadt, Germany

Pierre-Alain Fouque	Rennes University and Institut Universitaire de France, France
Steven D. Galbraith	University of Auckland, New Zealand
Chaya Ganesh	Indian Institute of Science, India
Juan Garay	Texas A&M University, USA
Sanjam Garg	University of California, Berkeley and NTT Research, USA
Daniel Genkin	Georgia Institute of Technology, USA
Jian Guo	Nanyang Technological University, Singapore
Siyao Guo	New York University Shanghai, China
Mohammad Hajiabadi	University of Waterloo, Canada
Mike Hamburg	Rambus Inc, USA
David Heath	Georgia Institute of Technology, USA
Viet Tung Hoang	Florida State University, USA
Xinyi Huang	Fujian Normal University, China
Takanori Isobe	University of Hyogo, Japan
Tetsu Iwata	Nagoya University, Japan
Khoongming Khoo	DSO National Laboratories, Singapore
Elena Kirshanova	Immanuel Kant Baltic Federal University, Russia
Ilan Komargodski	Hebrew University of Jerusalem and NTT Research, Israel
Gregor Leander	Ruhr-Universität Bochum, Germany
Qipeng Liu	Simons Institute for the Theory of Computing, USA
Tianren Liu	Peking University, China
Shengli Liu	Shanghai Jiao Tong University, China
Zhe Liu	Nanjing University of Aeronautics and Astronautics, China
Hemanta Maji	Purdue University, USA
Giulio Malavolta	Max Planck Institute for Security and Privacy, Germany
Bart Mennink	Radboud University Nijmegen, Netherlands
Tal Moran	Reichman University, Israel
Pratyay Mukherjee	Swirls/Hedera, USA
Omkant Pandey	State University of New York at Stony Brook, USA
Anat Paskin-Cherniavsky	Ariel University, Israel
Alain Passelègue	Inria and ENS Lyon, France
Svetla Petkova-Nikova	KU Leuven, Belgium and University of Bergen, Norway
Duong Hieu Phan	Télécom Paris, France
Cécile Pierrot	Inria, France
Silas Richelson	UC Riverside, USA

Yu Sasaki	NTT Corporation, Japan
Tobias Schneider	NXP Semiconductors, Austria
Dominique Schröder	Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany
abhi shelat	Northeastern University, USA
Mark Simkin	Ethereum Foundation, USA
Ling Song	Jinan University, Guangzhou, China
Fang Song	Portland State University, USA
Pratik Soni	Carnegie Mellon University, USA
Akshayaram Srinivasan	Tata Institute of Fundamental Research, India
Damien Stehlé	ENS de Lyon, France
Ron Steinfeld	Monash University, Australia
Qiang Tang	University of Sydney, Australia
Yiannis Tselekounis	Carnegie Mellon University, USA
Meiqin Wang	Shandong University, China
Xiaoyun Wang	Tsinghua University, China
David Wu	University of Texas at Austin, USA
Wenling Wu	Institute of Software, Chinese Academy of Sciences, China
Shota Yamada	AIST, Japan
Takashi Yamakawa	NTT Corporation, Japan
Jiang Zhang	State Key Laboratory of Cryptology, China

Additional Reviewers

Behzad Abdolmaleki	Charlotte Bonte	Nai-Hui Chia
Calvin Abou Haidar	Carl Bootland	Arka Rai Choudhuri
Damiano Abram	Katharina Boudgoust	Jiali Choy
Bar Alon	Lennart Braun	Qiaohan Chu
Pedro Alves	Marek Broll	Hien Chu
Ravi Anand	Chris Brzuska	Eldon Chung
Anurag Anshu	BinBin Cai	Sandro Coretti-Drayton
Victor Arribas	Matteo Campanelli	Arjan Cornelissen
Thomas Attema	Federico Canale	Maria Corte-Real Santos
Christian Badertscher	Avik Chakraborti	Anamaria Costache
Anubhab Baksi	Suvradip Chakraborty	Alain Couvreur
Zhenzhen Bao	John Chan	Nan Cui
James Bartusek	Rohit Chatterjee	Benjamin R. Curtis
Christof Beierle	Long Chen	Jan-Pieter D'Anvers
Ritam Bhaumik	Yu Long Chen	Joan Daemen
Alexander Bienstock	Hongyin Chen	Wangchen Dai
Olivier Blazy	Shan Chen	Hannah Davis
Alex Block	Shiyao Chen	Luca De Feo
Maxime Bombar	Rongmao Chen	Gabrielle De Micheli

Thomas Debris-Alazard	Lucjan Hanzlik	Hanjun Li
Amit Deo	Yonglin Hao	Shun Li
Patrick Derbez	Keisuke Hara	Xingjian Li
Julien Devevey	Patrick Harasser	Xiao Liang
Siemen Dhooghe	Jingnan He	Benoît Libert
Benjamin Dowling	Rachelle Heim-Boissier	Damien Ligier
Leo Ducas	Minki Hhan	Chao Lin
Yen Ling Ee	Shoichi Hirose	Chengjun Lin
Jonathan Eriksen	Seungwan Hong	Yunhao Ling
Daniel Escudero	Akinori Hosoyamada	Eik List
Muhammed F. Esgin	James Hsin-Yu Chiang	Jiahui Liu
Thomas Espitau	Zhicong Huang	Feng-Hao Liu
Andre Esser	Senyang Huang	Guozhen Liu
Hulya Evkan	Chloé Hébant	Xiangyu Liu
Jaiden Fairoze	Iliia Iliashenko	Meicheng Liu
Joël Felderhoff	Laurent Imbert	Alex Lombardi
Hanwen Feng	Joseph Jaeger	Patrick Longa
Joe Fitzsimons	Palak Jain	Wen-jie Lu
Antonio Flórez-Gutiérrez	Ashwin Jha	Yuan Lu
Pouyan Forghani	Mingming Jiang	Donghang Lu
Cody Freitag	Zhengzhong Jin	You Lyu
Georg Fuchsbauer	Antoine Joux	Reinhard Lüftenegger
Pierre Galissant	Eliran Kachlon	Bernardo Magri
Tommaso Gagliardoni	Bhavana Kanukurthi	Monosij Maitra
Daniel Gardham	Alexander Karenin	Mary Maller
Pierrick Gaudry	Shuichi Katsumata	Lenka Mareková
Romain Gay	Mojtaba Khalili	Mark Marson
Chunpeng Ge	Hamidreza Khorasgani	Takahiro Matsuda
Rosario Gennaro	Dongwoo Kim	Alireza Mehrdad
Paul Gerhart	Duhyeong Kim	Simon-Philipp Merz
Satrajit Ghosh	Young-Sik Kim	Pierre Meyer
Ashrujit Ghoshal	Fuyuki Kitagawa	Michael Meyer
Niv Gilboa	Kamil Kluczniak	Peihan Miao
Aarushi Goel	Yashvanth Kondi	Tarik Moataz
Aron Gohr	Rajendra Kumar	Hart Montgomery
Jesse Goodman	Noboru Kunihiro	Tomoyuki Morimae
Mike Graf	Fukang Liu	Fabrice Mouhartem
Milos Grujic	Russell W. F. Lai	Tamer Mour
Aurore Guillevic	Jason LeGrow	Marta Mularczyk
Aldo Gunsing	Jooyoung Lee	Michael Naehrig
Chun Guo	Hyung Tae Lee	Marcel Nageler
Hosein Hadipour	Byeonghak Lee	Yusuke Naito
Mathias Hall-Andersen	Charlotte Lefevre	Mridul Nandi
Shuai Han	Zeyong Li	Patrick Neumann
Helena Handschuh	Yiming Li	Ruth Ng

Ky Nguyen	Yusuke Sakai	Monika Trimoska
Khoa Nguyen	Kosei Sakamoto	Yi Tu
Ngoc Khanh Nguyen	Amin Sakzad	Aleksei Udovenko
Jianting Ning	Simona Samardjiska	Rei Ueno
Oded Nir	Olga Sanina	Mayank Varia
Ryo Nishimaki	Roozbeh Sarenche	Daniele Venturi
Olga Nissenbaum	Santanu Sarker	Riad Wahby
Semyon Novoselov	Tobias Schmalz	Roman Walch
Julian Nowakowski	Markus Schofnegger	Mingyuan Wang
Tabitha Ogilvie	Jacob Schuldt	Haoyang Wang
Eran Omri	Sruthi Sekar	Luping Wang
Hiroshi Onuki	Nicolas Sendrier	Xiao Wang
Jean-Baptiste Orfila	Akash Shah	Yuejun Wang
Mahak Pancholi	Yaobin Shen	Yuyu Wang
Omer Paneth	Yixin Shen	Weiqiang Wen
Lorenz Panny	Yu Shen	Chenkai Weng
Roberto Parisella	Danping Shi	Benjamin Wesolowski
Jeongeun Park	Rentaro Shiba	Yusai Wu
Rutvik Patel	Kazumasa Shinagawa	Yu Xia
Sikhar Patranabis	Omri Shmueli	Zhiye Xie
Alice Pellet-Mary	Ferdinand Sibleyras	Shengmin Xu
Hilder Vitor Lima Pereira	Janno Siim	Guangwu Xu
Ludovic Perret	Siang Meng Sim	Sophia Yakoubov
Thomas Peyrin	Luisa Siniscalchi	Hailun Yan
Phuong Pham	Yongsoo Song	Rupeng Yang
Guru Vamsi Policharla	Douglas Stebila	Kang Yang
Sihang Pu	Lukas Stennes	Qianqian Yang
Luowen Qian	Igors Stepanovs	Shao-Jun Yang
Chen Qian	Christoph Striecks	Li Yao
Kexin Qiao	Ling Sun	Hui Hui Yap
Willy Quach	Siwei Sun	Kan Yasuda
Rahul Rachuri	Bing Sun	Weijing You
Srinivasan Raghuraman	Shi-Feng Sun	Thomas Zacharias
Adrian Ranea	Akira Takahashi	Yupeng Zhang
Shahram Rasoolzadeh	Abdul Rahman Taleb	Kai Zhang
Christian Rechberger	Chik How Tan	Lei Zhang
Krijn Reijnders	Adrian Thillard	Yunlei Zhao
Maxime Remaud	Sri Aravinda Krishnan	Yu Zhou
Ling Ren	Thyagarajan	Chenzhi Zhu
Mahshid Riahinia	Yan Bo Ti	Paul Zimmermann
Peter Rindal	Elmar Tischhauser	Lukas Zobernig
Mike Rosulek	Yosuke Todo	matthieu rambaud
Adeline Roux-Langlois	Junichi Tomida	Hendrik Waldner
Paul Rösler	Ni Trieu	Yafei Zheng

Sponsoring Institutions

- Platinum Sponsor: ZAMA
- Gold Sponsor: BTQ, Hackers in Taiwan, Technology Innovation Institute
- Silver Sponsor: Meta (Facebook), Casper Networks, PQShield, NTT Research, WiSECURE
- Bronze Sponsor: Mitsubishi Electric, Algorand Foundation, LatticeX Foundation, Intel, QSancus, IOG (Input/Output Global), IBM

Contents – Part I

Award Papers

Full Quantum Equivalence of Group Action DLog and CDH, and More	3
<i>Hart Montgomery and Mark Zhandry</i>	
Cryptographic Primitives with Hinting Property	33
<i>Navid Alamati and Sikhar Patranabis</i>	
SWIFTEC: Shallue-van de Woestijne Indifferentiable Function to Elliptic Curves: Faster Indifferentiable Hashing to Elliptic Curves	63
<i>Jorge Chavez-Saab, Francisco Rodríguez-Henríquez, and Mehdi Tibouchi</i>	

Functional and Witness Encryption

Multi-Client Functional Encryption with Fine-Grained Access Control	95
<i>Ky Nguyen, Duong Hieu Phan, and David Pointcheval</i>	
Compact FE for Unbounded Attribute-Weighted Sums for Logspace from SXDH	126
<i>Pratish Datta, Tapas Pal, and Katsuyuki Takashima</i>	
Collusion-Resistant Functional Encryption for RAMs	160
<i>Prabhanjan Ananth, Kai-Min Chung, Xiong Fan, and Luowen Qian</i>	
Witness Encryption and Null-IO from Evasive LWE	195
<i>Vinod Vaikuntanathan, Hoeteck Wee, and Daniel Wichs</i>	

Symmetric Key Cryptanalysis

Algebraic Meet-in-the-Middle Attack on LowMC	225
<i>Fukang Liu, Santanu Sarkar, Gaoli Wang, Willi Meier, and Takanori Isobe</i>	
Latin Dances Reloaded: Improved Cryptanalysis Against Salsa and ChaCha, and the Proposal of Forró	256
<i>Murilo Coutinho, Iago Passos, Juan C. Grados Vásquez, Fábio L. L. de Mendonça, Rafael Timteo de Sousa Jr., and Fábio Borges</i>	
Mind the TWEAKEY Schedule: Cryptanalysis on SKINNYe-64-256	287
<i>Lingyue Qin, Xiaoyang Dong, Anyu Wang, Jialiang Hua, and Xiaoyun Wang</i>	

Enhancing Differential-Neural Cryptanalysis	318
<i>Zhenzhen Bao, Jian Guo, Meicheng Liu, Li Ma, and Yi Tu</i>	
Towards Tight Security Bounds for OMAC, XCBC and TMAC	348
<i>Soumya Chattopadhyay, Ashwin Jha, and Mridul Nandi</i>	
A Modular Approach to the Security Analysis of Two-Permutation Constructions	379
<i>Yu Long Chen</i>	
Optimizing Rectangle Attacks: A Unified and Generic Framework for Key Recovery	410
<i>Ling Song, Nana Zhang, Qianqian Yang, Danping Shi, Jiahao Zhao, Lei Hu, and Jian Weng</i>	
Multiparty Computation	
Random Sources in Private Computation	443
<i>Geoffroy Couteau and Adi Rosén</i>	
Non-interactive Secure Computation of Inner-Product from LPN and LWE	474
<i>Geoffroy Couteau and Maryam Zarezadeh</i>	
Efficient Adaptively-Secure Byzantine Agreement for Long Messages	504
<i>Amey Bhangale, Chen-Da Liu-Zhang, Julian Loss, and Kartik Nayak</i>	
Concurrently Composable Non-interactive Secure Computation	526
<i>Andrew Morgan and Rafael Pass</i>	
Attaining GOD Beyond Honest Majority with Friends and Foes	556
<i>Aditya Hegde, Nishat Koti, Varsha Bhat Kukkala, Shravani Patil, Arpita Patra, and Protik Paul</i>	
Towards Practical Topology-Hiding Computation	588
<i>Shuaishuai Li</i>	
Real World Protocols	
Key-Schedule Security for the TLS 1.3 Standard	621
<i>Chris Brzuska, Antoine Delignat-Lavaud, Christoph Egger, Cédric Fournet, Konrad Kohbrok, and Markulf Kohlweiss</i>	
YOLO YOSO: Fast and Simple Encryption and Secret Sharing in the YOSO Model	651
<i>Ignacio Cascudo, Bernardo David, Lydia Garms, and Anders Konring</i>	

State Machine Replication Under Changing Network Conditions 681
Andreea B. Alexandru, Erica Blum, Jonathan Katz, and Julian Loss

Blockchains and Cryptocurrencies

Non-interactive Mimblewimble Transactions, Revisited 713
Georg Fuchsbauer and Michele Orrù

A Universally Composable Non-interactive Aggregate Cash System 745
Yanxue Jia, Shi-Feng Sun, Hong-Sheng Zhou, and Dawu Gu

Practical Provably Secure Flooding for Blockchains 774
*Chen-Da Liu-Zhang, Christian Matt, Ueli Maurer, Guilherme Rito,
and Søren Eller Thomsen*

SNACKS: Leveraging Proofs of Sequential Work for Blockchain Light
Clients 806
Hamza Abusalah, Georg Fuchsbauer, Peter Gaži, and Karen Klein

Author Index 837