Shweta Agrawal
Dongdai Lin (Eds.)

LNCS 13791

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

1 Part I

INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH

i a c r

Springer

Lecture Notes in Computer Science 13791

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

Springer

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

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

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

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

Cryptographic Primitives with Hinting Property 33
Navid Alamati and Sikhar Patranabis

SWIFTEC: Shallue-van de Woestijne Indifferentiable Function to Elliptic Curves: Faster Indifferentiable Hashing to Elliptic Curves 63
Jorge Chavez-Saab, Francisco Rodríguez-Henríquez, and Mehdi Tibouchi

Functional and Witness Encryption

Multi-Client Functional Encryption with Fine-Grained Access Control 95
Ky Nguyen, Duong Hieu Phan, and David Pointcheval

Compact FE for Unbounded Attribute-Weighted Sums for Logspace from SXDH 126
Pratish Datta, Tapas Pal, and Katsuyuki Takashima

Collusion-Resistant Functional Encryption for RAMs 160
Prabhanjan Ananth, Kai-Min Chung, Xiong Fan, and Luowen Qian

Witness Encryption and Null-IO from Evasive LWE 195
Vinod Vaikuntanathan, Hoeteck Wee, and Daniel Wichs

Symmetric Key Cryptanalysis

Algebraic Meet-in-the-Middle Attack on LowMC 225
Fukang Liu, Santanu Sarkar, Gaoli Wang, Willi Meier, and Takanori Isobe

Latin Dances Reloaded: Improved Cryptanalysis Against Salsa and ChaCha, and the Proposal of Forró 256
Murilo Coutinho, Iago Passos, Juan C. Grados Vásquez, Fábio L. L. de Mendonça, Rafael Timteo de Sousa Jr., and Fábio Borges

Mind the TWEAKEY Schedule: Cryptanalysis on SKINNYe-64-256 287
Lingyue Qin, Xiaoyang Dong, Anyu Wang, Jialiang Hua, and Xiaoyun Wang

Enhancing Differential-Neural Cryptanalysis 318
Zhenzhen Bao, Jian Guo, Meicheng Liu, Li Ma, and Yi Tu

Towards Tight Security Bounds for OMAC, XCBC and TMAC 348
Soumya Chattopadhyay, Ashwin Jha, and Mridul Nandi

A Modular Approach to the Security Analysis of Two-Permutation Constructions 379
Yu Long Chen

Optimizing Rectangle Attacks: A Unified and Generic Framework for Key Recovery 410
Ling Song, Nana Zhang, Qianqian Yang, Danping Shi, Jiahao Zhao, Lei Hu, and Jian Weng

Multiparty Computation

Random Sources in Private Computation 443
Geoffroy Couteau and Adi Rosén

Non-interactive Secure Computation of Inner-Product from LPN and LWE 474
Geoffroy Couteau and Maryam Zarezadeh

Efficient Adaptively-Secure Byzantine Agreement for Long Messages 504
Amey Bhangale, Chen-Da Liu-Zhang, Julian Loss, and Kartik Nayak

Concurrently Composable Non-interactive Secure Computation 526
Andrew Morgan and Rafael Pass

Attaining GOD Beyond Honest Majority with Friends and Foes 556
Aditya Hegde, Nishat Koti, Varsha Bhat Kukkala, Shravani Patil, Arpita Patra, and Protik Paul

Towards Practical Topology-Hiding Computation 588
Shuaishuai Li

Real World Protocols

Key-Schedule Security for the TLS 1.3 Standard 621
Chris Brzuska, Antoine Delignat-Lavaud, Christoph Egger, Cédric Fournet, Konrad Kohbrok, and Markulf Kohlweiss

YOLO YOSO: Fast and Simple Encryption and Secret Sharing in the YOSO Model 651
Ignacio Cascudo, Bernardo David, Lydia Garms, and Anders Konring

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