

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

Gerhard Woeginger 

RWTH Aachen, Aachen, Germany

Moti Yung

Columbia University, New York, NY, USA

More information about this subseries at <http://www.springer.com/series/7410>

Shiho Moriai · Huaxiong Wang (Eds.)

Advances in Cryptology – ASIACRYPT 2020

26th International Conference on the Theory
and Application of Cryptology and Information Security
Daejeon, South Korea, December 7–11, 2020
Proceedings, Part II

Editors

Shiho Moriai
Network Security Research Institute (NICT)
Tokyo, Japan

Huaxiong Wang 
Nanyang Technological University
Singapore, Singapore

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-64833-6 ISBN 978-3-030-64834-3 (eBook)
<https://doi.org/10.1007/978-3-030-64834-3>

LNCS Sublibrary: SL4 – Security and Cryptology

© International Association for Cryptologic Research 2020

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 26th Annual International Conference on Theory and Application of Cryptology and Information Security (ASIACRYPT 2020), was originally planned to be held in Daejeon, South Korea, during December 7–11, 2020. Due to the COVID-19 pandemic, it was shifted to an online-only virtual conference.

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

We received a total of 316 submissions from all over the world, the Program Committee (PC) selected 85 papers for publication in the proceedings of the conference. The two program chairs were supported by a PC consisting of 66 leading experts in aspects of cryptology. Each submission was reviewed by at least three PC members (or their sub-reviewers) and five PC members were assigned to submissions co-authored by PC members. The strong conflict of interest rules imposed by the IACR ensure that papers are not handled by PC members with a close working relationship with authors. The two program chairs were not allowed to submit a paper, and PC members were limited to two submissions each. There were approximately 390 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 205 submissions to proceed to the second round, including 1 submission with early acceptance. The authors of 204 papers were then invited to provide a short rebuttal in response to the referee reports. The second round involved extensive discussions by the PC members.

The three volumes of the conference proceedings contain the revised versions of the 85 papers that were selected, together with the abstracts of 2 invited talks. The final revised versions of papers were not reviewed again and the authors are responsible for their contents.

The program of ASIACRYPT 2020 featured two excellent invited talks by Shweta Agrawal and Jung Hee Cheon. The conference also featured a rump session which contained short presentations on the latest research results of the field.

The PC selected three papers to receive the Best Paper Award, via a voting-based process that took into account conflicts of interest, which were solicited to submit the full versions to the *Journal of Cryptology*: “Finding Collisions in a Quantum World: Quantum Black-Box Separation of Collision-Resistance and One-Wayness” by Akinori Hosoyamada and Takashi Yamakawa; “New results on Gimli: full-permutation distinguishers and improved collisions” by Antonio Flórez Gutiérrez, Gaëtan Leurent, María Naya-Plasencia, Léo Perrin, André Schrottenloher, and Ferdinand Sibleyras; and “SQISign: Compact Post-Quantum signatures from Quaternions and Isogenies” by Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski.

Many people contributed to the success of ASIACRYPT 2020. 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 Kwangjo Kim, the general chair, for his efforts and overall organization. We thank Michel Abdalla, McCurley, Kay McKelly, and members of the IACR's emergency pandemic team for their work in designing and running the virtual format. We thank Steve Galbraith, Joo Young Lee, and Yu Sasaki for expertly organizing and chairing the rump session. We are extremely grateful to Zhenzhen Bao for checking all the latex files and for assembling the files for submission to Springer. Finally, we thank Shai Halevi and the IACR for setting up and maintaining the Web Submission and Review software, used by IACR conferences for the paper submission and review process. We also thank Alfred Hofmann, Anna Kramer, and their colleagues at Springer for handling the publication of these conference proceedings.

December 2020

Shiho Moriai
Huaxiong Wang

Organization

General Chair

Kwangjo Kim

Korea Advanced Institute of Science and Technology
(KAIST), South Korea

Program Chairs

Shiho Moriai

Network Security Research Institute (NICT), Japan

Huaxiong Wang

Nanyang Technological University, Singapore

Program Committee

Shweta Agrawal

IIT Madras, India

Gorjan Alagic

University of Maryland, USA

Shi Bai

Florida Atlantic University, USA

Zhenzhen Bao

Nanyang Technological University, Singapore

Paulo Barreto

University of Washington Tacoma, USA

Lejla Batina

Radboud University, The Netherlands

Amos Beimel

Ben-Gurion University, Israel

Sonia Belaïd

CryptoExperts, France

Olivier Blazy

University of Limoges, France

Jie Chen

East China Normal University, China

Yilei Chen

Visa Research, USA

Chen-Mou Cheng

Osaka University, Japan

Jun Furukawa

NEC Israel Research Center, Israel

David Galindo

University of Birmingham, Fetch.AI, UK

Jian Guo

Nanyang Technological University, Singapore

Swee-Huay Heng

Multimedia University, Malaysia

Xinyi Huang

Fujian Normal University, China

Andreas Hülsing

TU Eindhoven, The Netherlands

Takanori Isobe

University of Hyogo, Japan

David Jao

University of Waterloo, evolutionQ, Inc., Canada

Jérémy Jean

ANSSI, France

Zhengfeng Ji

University of Technology Sydney, Australia

Hyung Tae Lee

Jeonbuk National University, South Korea

Jooyoung Lee

KAIST, South Korea

Benoît Libert

CNRS, ENS, France

Dongdai Lin

Chinese Academy of Sciences, China

Helger Lipmaa

University of Tartu, Estonia, and Simula UiB, Norway

Feng-Hao Liu

Florida Atlantic University, USA

Georgia Azzurra Marson	University of Bern, Switzerland, and NEC Laboratories Europe, Germany
Daniel Masny	Visa Research, USA
Takahiro Matsuda	AIST, Japan
Brice Minaud	Inria, ENS, France
Shiho Moriai	NICT, Japan
Kartik Nayak	Duke University, VMware Research, USA
Khoa Nguyen	Nanyang Technological University, Singapore
Svetla Nikova	KU Leuven, Belgium
Carles Padró	UPC, Spain
Jiaxin Pan	NTNU, Norway
Arpita Patra	Indian Institute of Science, India
Thomas Peters	UCL, Belgium
Duong Hieu Phan	University of Limoges, France
Raphael C.-W. Phan	Monash University, Malaysia
Josef Pieprzyk	CSIRO, Australia, and Institute of Computer Science, Polish Academy of Sciences, Poland
Ling Ren	VMware Research, University of Illinois at Urbana-Champaign, USA
Carla Ràfols	Universitat Pompeu Fabra, Spain
Rei Safavi-Naini	University of Calgary, Canada
Yu Sasaki	NTT laboratories, Japan
Jae Hong Seo	Hanyang University, South Korea
Ron Steinfeld	Monash University, Australia
Willy Susilo	University of Wollongong, Australia
Qiang Tang	New Jersey Institute of Technology, USA
Mehdi Tibouchi	NTT laboratories, Japan
Huaxiong Wang	Nanyang Technological University, Singapore
Xiaoyun Wang	Tsinghua University, China
Yongge Wang	The University of North Carolina at Charlotte, USA
Chaoping Xing	Shanghai Jiao Tong University, China, and NTU, Singapore
Yu Yu	Shanghai Jiao Tong University, China
Mark Zhandry	Princeton University, NTT Research, USA

External Reviewers

Behzad Abdolmaleki	Marcel Armour	Saikrishna
Parhat Abla	Gilad Asharov	Badrinarayanan
Mamun Akand	Man Ho Au	Mir Ali Rezazadeh Bae
Orestis Alpos	Benedikt Auerbach	Joonsang Baek
Hiroaki Anada	Khin Mi Mi Aung	Karim Bagheri
Benny Applebaum	Sepideh Avizheh	Gustavo Banegas
Diego F. Aranha	Christian Badertscher	Laasya Bangalore

Subhadeep Banik	Jan Czajkowski	Kristian Gjøsteen
James Bartusek	João Paulo da Silva	Aarushi Goel
Carsten Baum	Jan-Pieter D'anvers	Huijing Gong
Rouzbeh Behnia	Joan Daemen	Junqing Gong
Aner Ben-Efraim	Ricardo Dahab	Zheng Gong
Fabrice Benhamouda	Nilanjan Datta	Alonso González
Francesco Berti	Bernardo David	Rishab Goyal
Luk Bettale	Gareth Davies	Benjamin Grégoire
Tim Beyne	Yi Deng	Jiaxin Guan
Shivam Bhasin	Amit Deo	Cyprien de Saint Guilhem
Nina Bindel	Patrick Derbez	Aldo Gunsing
Nir Bitansky	Siemen Dhooghe	Chun Guo
Xavier Bonnetain	Hang Dinh	Fuchun Guo
Katharina Boudgoust	Christoph Dobraunig	Qian Guo
Florian Bourse	Javad Doliskani	Felix Günther
Zvika Brakerski	Jelle Don	Ariel Hamlin
Jaqueline Brendel	Xiaoyang Dong	Ben Hamlin
Olivier Bronchain	Dung Duong	Jinguang Han
Benedikt Bunz	Betül Durak	Kyoohyung Han
Seyit Camtepe	Avijit Dutta	Keisuke Hara
Ignacio Cascudo	Sabyasachi Dutta	Debiao He
Gaëtan Cassiers	Sébastien Duval	Chloé Héban
Suvradip Chakraborty	Ted Eaton	Javier Herranz
Jorge Chávez Saab	Keita Emura	Shoichi Hirose
Hao Chen	Muhammed F. Esgin	Deukjo Hong
Hua Chen	Thomas Espitau	Akinori Hosoyamada
Long Chen	Xiong Fan	Hector Hougaard
Rongmao Chen	Antonio Faonio	Qiong Huang
Yu Chen	Prastudy Fauzi	Shih-Han Hung
Yuan Chen	Hanwen Feng	Kathrin Hövelmanns
Ding-Yuan Cheng	Shengyuan Feng	Akiko Inoue
Ji-Jian Chin	Tamara Finogina	Tetsu Iwata
Seongbong Choi	Apostolos Fournaris	Ashwin Jha
Wonseok Choi	Ashley Fraser	Dingding Jia
Ashish Choudhury	Philippe Gaborit	Shaoquan Jiang
Sherman S. M. Chow	Steven Galbraith	Chanyang Ju
Heewon Chung	Pierre Galissant	Eliran Kachlon
Michele Ciampi	Chaya Ganesh	Saqib A. Kakvi
Benoît Cogliati	Romain Gay	Ghassan Karame
Craig Costello	Chunpeng Ge	Sabyasachi Karati
Nicholas Courtois	Kai Gellert	Angshuman Karmakar
Geoffroy Couteau	Nicholas Genise	Shuichi Katsumata
Alain Couvreur	Alexandru Gheorghiu	Marcel Keller
Daniele Cozzo	Hossein Ghodosi	Dongwoo Kim
Hongrui Cui	Satrajit Ghosh	Jihye Kim
Edouard Cuvelier	Benedikt Gierlichs	Jinsu Kim

Jiseung Kim	Julian Loss	Shravani Patil
Jongkil Kim	Yuan Lu	Sikhar Patranabis
Minkyu Kim	Zhenliang Lu	Kateryna Pavlyk
Myungsun Kim	Lin Lyu	Alice Pellet-Mary
Seongkwang Kim	Fermi Ma	Geovandro Pereira
Taechan Kim	Hui Ma	Thomas Peyrin
Elena Kirshanova	Xuecheng Ma	Phuong Pham
Fuyuki Kitagawa	Bernardo Magri	Stjepan Picek
Susumu Kiyoshima	Monosij Maitra	Zaira Pindado
Michael Kloss	Christian Majenz	Rafael del Pino
François Koeune	Nathan Manohar	Rachel Player
Lisa Kohl	Ange Martinelli	Geong Sen Poh
Markulf Kohlweiss	Zdenek Martinasek	David Pointcheval
Chelsea Komlo	Ramiro Martinez	Yuriy Polyakov
Yashvanth Kondi	Pedro Maat C. Massolino	Ali Poostindouz
Nishat Koti	Loïc Masure	Frédéric de Portzamparc
Toomas Krips	Bart Mennink	Chen Qian
Veronika Kuchta	Lauren De Meyer	Tian Qiu
Thijs Laarhoven	Peihan Miao	Sai Rahul Rachuri
Jianchang Lai	Kazuhiko Minematsu	Adrian Ranea
Qiqi Lai	Rafael Misoczki	Divya Ravi
Huy Quoc Le	Tarik Moataz	Jean-René Reinhard
Byeonghak Lee	Tal Moran	Peter Rindal
Changmin Lee	Tomoyuki Morimae	Francisco
Moon Sung Lee	Hiraku Morita	Rodríguez-Henríquez
Liang Li	Travis Morrison	Mélissa Rossi
Shuaishuai Li	Pratyay Mukherjee	Partha Sarathy Roy
Shun Li	Sayantan Mukherjee	Ajith S.
Xiangxue Li	Pierrick Méaux	Yusuke Sakai
Xinyu Li	Helen Möllering	Kosei Sakamoto
Ya-Nan Li	Michael Naehrig	Amin Sakzad
Zhe Li	Yusuke Naito	Simona Samardjiska
Bei Liang	Maria Naya-Plasencia	Olivier Sanders
Cheng-Jun Lin	Ngoc Khanh Nguyen	Partik Sarkar
Fuchun Lin	Jianting Ning	Santanu Sarkar
Wei-Kai Lin	Ryo Nishimaki	John Schanck
Dongxi Liu	Ariel Nof	André Schrottenloher
Fukang Liu	Kazuma Ohara	Jacob Schuldt
Guozhen Liu	Daniel Esteban Escudero	Mahdi Sedaghat
Jia Liu	Ospina	Ignacio Amores Sesar
Joseph K. Liu	Giorgos Panagiotakos	Siamak Shahandashti
Meicheng Liu	Bo Pang	Setareh Sharifian
Qipeng Liu	Lorenz Panny	Yaobin Shen
Shengli Liu	Anna Pappa	Sina Shiehian
Yunwen Liu	Anat Paskin-Cherniavsky	Kazumasa Shinagawa
Zhen Liu	Alain Passelègue	Janno Siim

Javier Silva	Srinivas Vivek	Jianhua Yan
Ricardo Dahab	Misha Volkhov	Zhenbin Yan
Siang Meng Sim	Quoc Huy Vu	Bo-Yin Yang
Leonie Simpson	Alexandre Wallet	Guomin Yang
Daniel Slamanig	Ming Wan	Kang Yang
Daniel Smith-Tone	Chenyu Wang	Rupeng Yang
Fang Song	Han Wang	Shao-Jun Yang
Yongcheng Song	Junwei Wang	Wei-Chuen Yau
Florian Speelman	Lei Wang	Kisoon Yoon
Akshayaram Srinivasan	Luping Wang	Yong Yu
Jun Xu	Qingju Wang	Zuoxia Yu
Igors Stepanovs	Weijia Wang	Chen Yuan
Ling Sun	Wenhao Wang	Tsz Hon Yuen
Shi-Feng Sun	Yang Wang	Aaram Yun
Akira Takahashi	Yuyu Wang	Alexandros Zacharakis
Katsuyuki Takashima	Zhedong Wang	Michal Zajac
Benjamin Hong	Gaven Watson	Luca Zanolini
Meng Tan	Florian Weber	Arantxa Zapico
Syh-Yuan Tan	Man Wei	Ming Zeng
Titouan Tanguy	Weiqiang Wen	Bin Zhang
Adrian Thillard	Thom Wiggers	Bingsheng Zhang
Miaomiao Tian	Zac Williamson	Cong Zhang
Ivan Tjuawinata	Lennert Wouters	Hailong Zhang
Yosuke Todo	Qianhong Wu	Jiang Zhang
Alin Tomescu	Keita Xagawa	Liang Feng Zhang
Junichi Tomida	Zejun Xiang	Xue Zhang
Ni Trieu	Hanshen Xiao	Zhenfei Zhang
Viet Cuong Trinh	Xiang Xie	Zhifang Zhang
Ida Tucker	Yanhong Xu	Changan Zhao
Aleksei Udovenko	Haiyang Xue	Yongjun Zhao
Bogdan Ursu	Shota Yamada	Zhongxiang Zheng
Damien Vergnaud	Takashi Yamakawa	Yihong Zhu
Fernando Virdia	Sravya Yandamuri	Arne Tobias Ødegaard

Contents – Part II

Public Key Cryptography

Incrementally Aggregatable Vector Commitments and Applications to Verifiable Decentralized Storage	3
<i>Matteo Campanelli, Dario Fiore, Nicola Greco, Dimitris Kolonelos, and Luca Nizzardo</i>	
Non-committing Encryption with Constant Ciphertext Expansion from Standard Assumptions	36
<i>Yusuke Yoshida, Fuyuki Kitagawa, Keita Xagawa, and Keisuke Tanaka</i>	
Collusion Resistant Trace-and-Revoke for Arbitrary Identities from Standard Assumptions	66
<i>Sam Kim and David J. Wu</i>	
Subvert KEM to Break DEM: Practical Algorithm-Substitution Attacks on Public-Key Encryption	98
<i>Rongmao Chen, Xinyi Huang, and Moti Yung</i>	
Unbounded HIBE with Tight Security	129
<i>Roman Langrehr and Jiaxin Pan</i>	
Multi-client Oblivious RAM with Poly-logarithmic Communication	160
<i>Sherman S. M. Chow, Katharina Feh, Russell W. F. Lai, and Giulio Malavolta</i>	
Privacy-Preserving Pattern Matching on Encrypted Data	191
<i>Anis Bkakria, Nora Cuppens, and Frédéric Cuppens</i>	
Efficient Homomorphic Comparison Methods with Optimal Complexity	221
<i>Jung Hee Cheon, Dongwoo Kim, and Duhyeong Kim</i>	

Lattice-Based Cryptography

Practical Exact Proofs from Lattices: New Techniques to Exploit Fully-Splitting Rings	259
<i>Muhammed F. Esgin, Ngoc Khanh Nguyen, and Gregor Seiler</i>	
Towards Classical Hardness of Module-LWE: The Linear Rank Case	289
<i>Katharina Boudgoust, Corentin Jeudy, Adeline Roux-Langlois, and Weiqiang Wen</i>	

Lattice-Based E-Cash, Revisited	318
<i>Amit Deo, Benoît Libert, Khoa Nguyen, and Olivier Sanders</i>	
Twisted-PHS: Using the Product Formula to Solve Approx-SVP in Ideal Lattices	349
<i>Olivier Bernard and Adeline Roux-Langlois</i>	
Simpler Statistically Sender Private Oblivious Transfer from Ideals of Cyclotomic Integers.	381
<i>Daniele Micciancio and Jessica Sorrell</i>	
Isogeny-Based Cryptography	
Cryptographic Group Actions and Applications.	411
<i>Navid Alamati, Luca De Feo, Hart Montgomery, and Sikhar Patranabis</i>	
B-SIDH: Supersingular Isogeny Diffie-Hellman Using Twisted Torsion	440
<i>Craig Costello</i>	
Calamari and Falafel: Logarithmic (Linkable) Ring Signatures from Isogenies and Lattices	464
<i>Ward Beullens, Shuichi Katsumata, and Federico Pintore</i>	
Radical Isogenies	493
<i>Wouter Castryck, Thomas Decru, and Frederik Vercauteren</i>	
Oblivious Pseudorandom Functions from Isogenies	520
<i>Dan Boneh, Dmitry Kogan, and Katharine Woo</i>	
SiGamal: A Supersingular Isogeny-Based PKE and Its Application to a PRF	551
<i>Tomoki Moriya, Hiroshi Onuki, and Tsuyoshi Takagi</i>	
Quantum Algorithms	
Estimating Quantum Speedups for Lattice Sieves	583
<i>Martin R. Albrecht, Vlad Gheorghiu, Eamonn W. Postlethwaite, and John M. Schanck</i>	
A Combinatorial Approach to Quantum Random Functions	614
<i>Nico Döttling, Giulio Malavolta, and Sihang Pu</i>	
Improved Classical and Quantum Algorithms for Subset-Sum.	633
<i>Xavier Bonnetain, Rémi Bricout, André Schrottenloher, and Yixin Shen</i>	
Security Limitations of Classical-Client Delegated Quantum Computing	667
<i>Christian Badertscher, Alexandru Cojocaru, Léo Colisson, Elham Kashefi, Dominik Leichtle, Atul Mantri, and Petros Wallden</i>	

Quantum Circuit Implementations of AES with Fewer Qubits.	697
<i>Jian Zou, Zihao Wei, Siwei Sun, Ximeng Liu, and Wenling Wu</i>	
Quantum Collision Attacks on AES-Like Hashing with Low Quantum Random Access Memories	727
<i>Xiaoyang Dong, Siwei Sun, Danping Shi, Fei Gao, Xiaoyun Wang, and Lei Hu</i>	
Authenticated Key Exchange	
Fuzzy Asymmetric Password-Authenticated Key Exchange	761
<i>Andreas Erwig, Julia Hesse, Maximilian Orlt, and Siavash Riahi</i>	
Two-Pass Authenticated Key Exchange with Explicit Authentication and Tight Security.	785
<i>Xiangyu Liu, Shengli Liu, Dawu Gu, and Jian Weng</i>	
Author Index	815