Lecture Notes in Computer Science 12492

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

Springer

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

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

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

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

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

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

Contents – Part II

Public Key Cryptography

Lattice-Based Cryptography

Isogeny-Based Cryptography

Quantum Algorithms

Authenticated Key Exchange