Lecture Notes in Computer Science **10624**

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

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

Tsuyoshi Takagi · Thomas Peyrin (Eds.)

Advances in Cryptology – ASIACRYPT 2017

23rd International Conference on the Theory and Applications of Cryptology and Information Security
Hong Kong, China, December 3–7, 2017
Proceedings, Part I

Springer

Editors
Tsuyoshi Takagi
The University of Tokyo
Tokyo
Japan

Thomas Peyrin
Nanyang Technological University
Singapore
Singapore

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-70693-1 ISBN 978-3-319-70694-8 (eBook)
https://doi.org/10.1007/978-3-319-70694-8

Library of Congress Control Number: 2017957984

LNCS Sublibrary: SL4 – Security and Cryptology

Printed on acid-free paper

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

Preface

ASIACRYPT 2017, the 23rd Annual International Conference on Theory and Application of Cryptology and Information Security, was held in Hong Kong, SAR China, during December 3–7, 2017.

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

ASIACRYPT 2017 received 243 submissions from all over the world. The Program Committee selected 67 papers (from which two were merged) for publication in the proceedings of this conference. The review process was made by the usual double-blind peer review by the Program Committee consisting of 48 leading experts of the field. Each submission was reviewed by at least three reviewers, and five reviewers were assigned to submissions co-authored by Program Committee members. This year, the conference operated a two-round review system with rebuttal phase. In the first-round review the Program Committee selected the 146 submissions that were considered of value for proceeding to the second round. In the second-round review the Program Committee further reviewed the submissions by taking into account their rebuttal letter from the authors. All the selection process was assisted by 334 external reviewers. These three-volume proceedings contain the revised versions of the papers that were selected. The revised versions were not reviewed again and the authors are responsible for their contents.

The program of ASIACRYPT 2017 featured three excellent invited talks. Dustin Moody gave a talk entitled "The Ship Has Sailed: The NIST Post-Quantum Cryptography 'Competition'," Wang Huaxiong spoke on "Combinatorics in Information-Theoretic Cryptography," and Pascal Paillier gave a third talk. The conference also featured a traditional rump session that contained short presentations on the latest research results of the field. The Program Committee selected the work "Identification Protocols and Signature Schemes Based on Supersingular Isogeny Problems" by Steven D. Galbraith, Christophe Petit, and Javier Silva for the Best Paper Award of ASIACRYPT 2017. Two more papers, "Kummer for Genus One over Prime Order Fields" by Sabyasachi Karati and Palash Sarkar, and "A Subversion-Resistant SNARK" by Behzad Abdolmaleki, Karim Baghery, Helger Lipmaa, and Michał Zając were solicited to submit the full versions to the *Journal of Cryptology*. The program chairs selected Takahiro Matsuda and Bart Mennink for the Best PC Member Award.

Many people have contributed to the success of ASIACRYPT 2017. We would like to thank the authors for submitting their research results to the conference. We are very grateful to all of the Program Committee members as well as the external reviewers for their fruitful comments and discussions on their areas of expertise. We are greatly indebted to Duncan Wong and Siu Ming Yiu, the general co-chairs, for their efforts and overall organization. We would also like to thank Allen Au, Catherine Chan, Sherman S.M. Chow, Lucas Hui, Zoe Jiang, Xuan Wang, and Jun Zhang, the local

Organizing Committee, for their continuous supports. We thank Duncan Wong and Siu Ming Yiu for expertly organizing and chairing the rump session.

Finally, we thank Shai Halevi for letting us use his nice software for supporting all the paper submission and review process. We also thank Alfred Hofmann, Anna Kramer, and their colleagues for handling the editorial process of the proceedings published at Springer LNCS.

December 2017

Tsuyoshi Takagi
Thomas Peyrin

ASIACRYPT 2017

The 23rd Annual International Conference on Theory and Application of Cryptology and Information Security

Sponsored by the International Association for Cryptologic Research (IACR)

December 3–7, 2017, Hong Kong, SAR China

General Co-chairs

Duncan Wong	CryptoBLK Limited
Siu Ming Yiu	The University of Hong Kong, SAR China

Program Co-chairs

Tsuyoshi Takagi	University of Tokyo, Japan
Thomas Peyrin	Nanyang Technological University, Singapore

Program Committee

Shweta Agrawal	IIT Madras, India
Céline Blondeau	Aalto University, Finland
Joppe W. Bos	NXP Semiconductors, Belgium
Chris Brzuska	TU Hamburg, Germany
Jie Chen	East China Normal University, China
Sherman S.M. Chow	The Chinese University of Hong Kong, SAR China
Kai-Min Chung	Academia Sinica, Taiwan
Nico Döttling	University of California, Berkeley, USA
Thomas Eisenbarth	Worcester Polytechnic Institute, USA
Dario Fiore	IMDEA Software Institute, Madrid, Spain
Georg Fuchsbauer	Inria and ENS, France
Steven Galbraith	Auckland University, New Zealand
Jian Guo	Nanyang Technological University, Singapore
Viet Tung Hoang	Florida State University, USA
Jérémy Jean	ANSSI, France
Jooyoung Lee	KAIST, South Korea
Dongdai Lin	Chinese Academy of Sciences, China
Feng-Hao Liu	Florida Atlantic University, USA
Stefan Mangard	Graz University of Technology, Austria
Takahiro Matsuda	AIST, Japan
Alexander May	Ruhr University Bochum, Germany
Bart Mennink	Radboud University, The Netherlands

Amir Moradi	Ruhr University Bochum, Germany
Pratyay Mukherjee	Visa Research, USA
Mridul Nandi	Indian Statistical Institute, India
Khoa Nguyen	Nanyang Technological University, Singapore
Miyako Ohkubo	NICT, Japan
Tatsuaki Okamoto	NTT Secure Platform Laboratories, Japan
Arpita Patra	Indian Institute of Science, India
Bart Preneel	KU Leuven, Belgium
Matthieu Rivain	CryptoExperts, France
Reihaneh Safavi-Naini	University of Calgary, Canada
Yu Sasaki	NTT Secure Platform Laboratories, Japan
Peter Schwabe	Radboud University, The Netherlands
Fang Song	Portland State University, USA
Francois-Xavier Standaert	UCL, Belgium
Damien Stehlé	ENS Lyon, France
Ron Steinfeld	Monash University, Australia
Rainer Steinwandt	Florida Atlantic University, USA
Mehdi Tibouchi	NTT Secure Platform Laboratories, Japan
Dominique Unruh	University of Tartu, Estonia
Gilles Van Assche	STMicroelectronics, Belgium
Serge Vaudenay	EPFL, Switzerland
Ingrid Verbauwhede	KU Leuven, Belgium
Ivan Visconti	University of Salerno, Italy
Lei Wang	Shanghai Jiaotong University, China
Meiqin Wang	Shandong University, China
Jiang Zhang	State Key Laboratory of Cryptology, China

Additional Reviewers

Masayuki Abe	Shi Bai	Begül Bilgin
Arash Afshar	Fatih Balli	Olivier Blazy
Divesh Aggarwal	Subhadeep Banik	Johannes Bloemer
Shashank Agrawal	Zhenzhen Bao	Sonia Mihaela Bogos
Ahmad Ahmadi	Hridam Basu	Sasha Boldyreva
Mamun Akand	Alberto Batistello	Charlotte Bonte
Gorjan Alagic	Balthazar Bauer	Raphael Bost
Joel Alwen	Carsten Baum	Leif Both
Abdelrahaman Aly	Georg T. Becker	Florian Bourse
Miguel Ambrona	Christof Beierle	Sébastien Canard
Elena Andreeva	Sonia Beläd	Brent Carmer
Diego Aranha	Fabrice Benhamouda	Wouter Castryck
Nuttapong Attrapadung	Francesco Berti	Dario Catalano
Sepideh Avizheh	Guido Bertoni	Gizem Çetin
Saikrishna Badrinarayanan	Sanjay Bhattacherjee	Avik Chakraborti
	Jean-Francois Biasse	Nishanth Chandran

Melissa Chase
Binyi Chen
Cong Chen
Long Chen
Yi-Hsiu Chen
Yu Chen
Yu-Chi Chen
Nai-Hui Chia
Gwangbae Choi
Wutichai Chongchitmate
Chi-Ning Chou
Ashish Choudhury
Chitchanok
Chuengsatiansup
Hao Chung
Michele Ciampi
Thomas De Cnudde
Katriel Cohn-Gordon
Henry Corrigan-Gibbs
Craig Costello
Geoffroy Couteau
Eric Crockett
Tingting Cui
Edouard Cuvelier
Joan Daemen
Wei Dai
Pratish Datta
Bernardo David
Marguerite Delcourt
Jeroen Delvaux
Yi Deng
David Derler
Julien Devigne
Claus Diem
Christoph Dobraunig
Yarkin Doroz
Léo Ducas
Dung H. Duong
Ratna Dutta
Stefan Dziembowski
Maria Eichlseder
Muhammed Esgin
Thomas Espitau
Xiong Fan
Antonio Faonio
Sebastian Faust
Björn Fay
Serge Fehr
Luca De Feo
Nils Fleischhacker
Jean-Pierre Flori
Tore Kasper Frederiksen
Thomas Fuhr
Marc Fyrbiak
Tommaso Gagliardoni
Chaya Ganesh
Flavio Garcia
Pierrick Gaudry
Rémi Géraud
Satrajit Ghosh
Irene Giacomelli
Benedikt Gierlichs
Junqing Gong
Louis Goubin
Alex Grilo
Hannes Gross
Vincent Grosso
Chun Guo
Hui Guo
Helene Haagh
Patrick Haddad
Harry Halpin
Shuai Han
Yoshikazu Hanatani
Jens Hermans
Gottfried Herold
Julia Hesse
Felix Heuer
Minki Hhan
Fumitaka Hoshino
Yin-Hsun Huang
Zhenyu Huang
Andreas Hülsing
Jung Yeon Hwang
Ilia Iliashenko
Mehmet Inci
Vincenzo Iovino
Ai Ishida
Takanori Isobe
Tetsu Iwata
Malika Izabachène
Michael Jacobson
Abhishek Jain
David Jao
Zhengfeng Ji
Dingding Jia
Shaoquan Jiang
Anthony Journault
Jean-Gabriel Kammerer
Sabyasachi Karati
Handan Kilinç
Dongwoo Kim
Jihye Kim
Jon-Lark Kim
Sam Kim
Taechan Kim
Elena Kirshanova
Ágnes Kiss
Fuyuki Kitagawa
Susumu Kiyoshima
Thorsten Kleinjung
Miroslav Knezevic
Alexander Koch
François Koeune
Konrad Kohbrok
Lisa Kohl
Ilan Komargodski
Yashvanth Kondi
Robert Kuebler
Frédéric Lafitte
Ching-Yi Lai
Russell W.F. Lai
Adeline Langlois
Gregor Leander
Changmin Lee
Hyung Tae Lee
Iraklis Leontiadis
Tancrède Lepoint
Debbie Leung
Yongqiang Li
Jyun-Jie Liao
Benoit Libert
Fuchun Lin
Wei-Kai Lin
Patrick Longa

Julian Loss
Steve Lu
Xianhui Lu
Atul Luykx
Chang Lv
Vadim Lyubashevsky
Monosij Maitra
Mary Maller
Giorgia Azzurra Marson
Marco Martinoli
Daniel Masny
Sarah Meiklejohn
Peihan Miao
Michele Minelli
Takaaki Mizuki
Ahmad Moghimi
Payman Mohassel
Maria Chiara Molteni
Seyyed Amir Mortazavi
Fabrice Mouhartem
Köksal Mus
Michael Naehrig
Ryo Nishimaki
Anca Nitulescu
Luca Nizzardo
Koji Nuida
Kaisa Nyberg
Adam O'Neill
Tobias Oder
Olya Ohrimenko
Emmanuela Orsini
Elisabeth Oswald
Elena Pagnin
Pascal Paillier
Jiaxin Pan
Alain Passelègue
Sikhar Patranabis
Roel Peeters
Chris Peikert
Alice Pellet-Mary
Ludovic Perret
Peter Pessl
Thomas Peters
Christophe Petit
Duong Hieu Phan
Antigoni Polychroniadou
Romain Poussier
Ali Poustindouz
Emmanuel Prouff
Kexin Qiao
Baodong Qin
Sebastian Ramacher
Somindu C. Ramanna
Shahram Rasoolzadeh
Divya Ravi
Francesco Regazzoni
Jean-René Reinhard
Ling Ren
Joost Renes
Oscar Reparaz
Joost Rijneveld
Damien Robert
Jérémie Roland
Arnab Roy
Sujoy Sinha Roy
Vladimir Rozic
Joeri de Ruiter
Yusuke Sakai
Amin Sakzad
Simona Samardjiska
Olivier Sanders
Pascal Sasdrich
Alessandra Scafuro
John Schanck
Tobias Schneider
Jacob Schuldt
Gil Segev
Okan Seker
Binanda Sengupta
Sourav Sengupta
Jae Hong Seo
Masoumeh Shafienejad
Setareh Sharifian
Sina Shiehian
Kazumasa Shinagawa
Dave Singelée
Shashank Singh
Javier Silva
Luisa Siniscalchi
Daniel Slamanig
Benjamin Smith
Ling Song
Pratik Soni
Koutarou Suzuki
Alan Szepieniec
Björn Tackmann
Mostafa Taha
Raymond K.H. Tai
Katsuyuki Takashima
Atsushi Takayasu
Benjamin Hong Meng Tan
Qiang Tang
Yan Bo Ti
Yosuke Todo
Ni Trieu
Roberto Trifiletti
Thomas Unterluggauer
John van de Wetering
Muthuramakrishnan Venkitasubramaniam
Daniele Venturi
Dhinakaran Vinayagamurthy
Vanessa Vitse
Damian Vizár
Satyanarayana Vusirikala
Sebastian Wallat
Alexandre Wallet
Haoyang Wang
Minqian Wang
Wenhao Wang
Xiuhua Wang
Yuyu Wang
Felix Wegener
Puwen Wei
Weiqiang Wen
Mario Werner
Benjamin Wesolowski
Baofeng Wu
David Wu
Keita Xagawa
Zejun Xiang
Chengbo Xu
Shota Yamada
Kan Yang
Kang Yang
Kan Yasuda

Donggeon Yhee
Kazuki Yoneyama
Kisoon Yoon
Yu Yu
Zuoxia Yu
Henry Yuen
Aaram Yun
Mahdi Zamani
Greg Zaverucha
Cong Zhang
Jie Zhang
Kai Zhang
Ren Zhang
Wentao Zhang
Yongjun Zhao
Yuqing Zhu

Local Organizing Committee

Co-chairs

Duncan Wong	CryptoBLK Limited
Siu Ming Yiu	The University of Hong Kong, SAR China

Members

Lucas Hui (Chair)	The University of Hong Kong, SAR China
Catherine Chan (Manager)	The University of Hong Kong, SAR China
Jun Zhang	The University of Hong Kong, SAR China
Xuan Wang	Harbin Institute of Technology, Shenzhen, China
Zoe Jiang	Harbin Institute of Technology, Shenzhen, China
Allen Au	The Hong Kong Polytechnic University, SAR China
Sherman S.M. Chow	The Chinese University of Hong Kong, SAR China

Invited Speakers

The Ship Has Sailed: the NIST Post-quantum Cryptography "Competition"

Dustin Moody

Computer Security Division, National Institute of Standards and Technology

Abstract. In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will compromise the security of many commonly used cryptographic algorithms. In particular, quantum computers would completely break many public-key cryptosystems, including those standardized by NIST and other standards organizations.

Due to this concern, many researchers have begun to investigate post-quantum cryptography (also called quantum-resistant cryptography). The goal of this research is to develop cryptographic algorithms that would be secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks. A significant effort will be required to develop, standardize, and deploy new post-quantum algorithms. In addition, this transition needs to take place well before any large-scale quantum computers are built, so that any information that is later compromised by quantum cryptanalysis is no longer sensitive when that compromise occurs.

NIST has taken several steps in response to this potential threat. In 2015, NIST held a public workshop and later published NISTIR 8105, Report on Post-Quantum Cryptography, which shares NIST's understanding of the status of quantum computing and post-quantum cryptography. NIST also decided to develop additional public-key cryptographic algorithms through a public standardization process, similar to the development processes for the hash function SHA-3 and the Advanced Encryption Standard (AES). To begin the process, NIST issued a detailed set of minimum acceptability requirements, submission requirements, and evaluation criteria for candidate algorithms, available at http://www.nist.gov/pqcrypto. The deadline for algorithms to be submitted was November 30, 2017.

In this talk, I will share the rationale on the major decisions NIST has made, such as excluding hybrid and (stateful) hash-based signature schemes. I will also talk about some open research questions and their potential impact on the standardization effort, in addition to some of the practical issues that arose while creating the API. Finally, I will give some preliminary information about the submitted algorithms, and discuss what we've learned during the first part of the standardization process.

Combinatorics in Information-Theoretic Cryptography

Huaxiong Wang

School of Physical and Mathematical Sciences,
Nanyang Technological University, Singapore
hxwang@ntu.edu.sg

Abstract. Information-theoretic cryptography is an area that studies cryptographic functionalities whose security does not rely on hardness assumptions from computational intractability of mathematical problems. It covers a wide range of cryptographic research topics such as one-time pad, authentication code, secret sharing schemes, secure multiparty computation, private information retrieval and post-quantum security etc., just to mention a few. Moreover, many areas in complexity-based cryptography are well known to benefit or stem from information-theoretic methods. On the other hand, combinatorics has been playing an active role in cryptography, for example, the hardness of Hamiltonian cycle existence in graph theory is used to design zero-knowledge proofs. In this talk, I will focus on the connections between combinatorics and information-theoretic cryptography. After a brief (incomplete) overview on their various connections, I will present a few concrete examples to illustrate how combinatorial objects and techniques are applied to the constructions and characterizations of information-theoretic schemes. Specifically, I will show

1. how perfect hash families and cover-free families lead to better performance in certain secret sharing schemes;
2. how graph colouring from planar graphs is used in constructing secure multiparty computation protocols over non-abelian groups;
3. how regular intersecting families are applied to the constructions of private information retrieval schemes.

Part of this research was funded by Singapore Ministry of Education under Research Grant MOE2016-T2-2-014(S).

Contents – Part I

Lattices

Homomorphic Encryptions

Access Control

Oblivious Protocols

Contents – Part II

Contents – Part III

Symmetric Key Designs