

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, Lancaster, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Zurich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbrücken, Germany

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 III



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 978-3-319-70699-3 ISBN 978-3-319-70700-6 (eBook)
<https://doi.org/10.1007/978-3-319-70700-6>

Library of Congress Control Number: 2017957984

LNCS Sublibrary: SL4 – Security and Cryptology

© International Association for Cryptologic Research 2017

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, express 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.

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
Siu Ming Yiu

CryptoBLK Limited
The University of Hong Kong, SAR China

Program Co-chairs

Tsuyoshi Takagi
Thomas Peyrin

University of Tokyo, Japan
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
Abdelrahman 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 Azizheh	Guido Bertoni	Gizem Çetin
Saikrishna	Sanjay Bhattacharjee	Avik Chakraborti
Badrinarayanan	Jean-Francois Biasse	Nishanth Chandran

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

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

CryptoBLK Limited
The University of Hong Kong, SAR China

Members

Lucas Hui (Chair)
Catherine Chan (Manager)
Jun Zhang
Xuan Wang
Zoe Jiang
Allen Au
Sherman S.M. Chow

The University of Hong Kong, SAR China
The University of Hong Kong, SAR China
The University of Hong Kong, SAR China
Harbin Institute of Technology, Shenzhen, China
Harbin Institute of Technology, Shenzhen, China
The Hong Kong Polytechnic University, SAR China
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.

Contents – Part III

Asiacrypt 2017 Award Paper II

A Subversion-Resistant SNARK	3
<i>Behzad Abdolmaleki, Karim Bagheri, Helger Lipmaa, and Michał Zając</i>	

Cryptographic Protocols

Two-Round PAKE from Approximate SPH and Instantiations from Lattices	37
<i>Jiang Zhang and Yu Yu</i>	
Tightly-Secure Signatures from Five-Move Identification Protocols	68
<i>Eike Kiltz, Julian Loss, and Jiaxin Pan</i>	
On the Untapped Potential of Encoding Predicates by Arithmetic Circuits and Their Applications.	95
<i>Shuichi Katsumata</i>	
The Minimum Number of Cards in Practical Card-Based Protocols	126
<i>Julia Kastner, Alexander Koch, Stefan Walzer, Daiki Miyahara, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone</i>	

Foundations

Succinct Spooky Free Compilers Are Not Black Box Sound	159
<i>Zvika Brakerski, Yael Tauman Kalai, and Renen Perlman</i>	
Non-Interactive Multiparty Computation Without Correlated Randomness . . .	181
<i>Shai Halevi, Yuval Ishai, Abhishek Jain, Ilan Komargodski, Amit Sahai, and Eylon Yogev</i>	
Optimal-Rate Non-Committing Encryption	212
<i>Ran Canetti, Oxana Poburinnaya, and Mariana Raykova</i>	
Preventing CLT Attacks on Obfuscation with Linear Overhead.	242
<i>Rex Fernando, Peter M. R. Rasmussen, and Amit Sahai</i>	

Zero-Knowledge Proofs

Two-Message Witness Indistinguishability and Secure Computation in the Plain Model from New Assumptions	275
<i>Saikrishna Badrinarayanan, Sanjam Garg, Yuval Ishai, Amit Sahai, and Akshay Wadia</i>	

Zero-Knowledge Arguments for Lattice-Based PRFs and Applications to E-Cash.	304
<i>Benoît Libert, San Ling, Khoa Nguyen, and Huaxiong Wang</i>	
Linear-Time Zero-Knowledge Proofs for Arithmetic Circuit Satisfiability	336
<i>Jonathan Bootle, Andrea Cerulli, Essam Ghadafi, Jens Groth, Mohammad Hajiabadi, and Sune K. Jakobsen</i>	
Symmetric Key Designs	
How to Use Metaheuristics for Design of Symmetric-Key Primitives.	369
<i>Ivica Nikolić</i>	
Cycle Slicer: An Algorithm for Building Permutations on Special Domains.	392
<i>Sarah Miracle and Scott Yilek</i>	
Symmetrically and Asymmetrically Hard Cryptography	417
<i>Alex Biryukov and Léo Perrin</i>	
Blockcipher-Based MACs: Beyond the Birthday Bound Without Message Length	446
<i>Yusuke Naito</i>	
Author Index	471