

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>

Michel Abdalla · Ricardo Dahab (Eds.)

Public-Key Cryptography – PKC 2018

21st IACR International Conference
on Practice and Theory of Public-Key Cryptography
Rio de Janeiro, Brazil, March 25–29, 2018
Proceedings, Part I

Editors

Michel Abdalla 
CNRS and École Normale Supérieure
Paris
France

Ricardo Dahab
University of Campinas
Campinas, SP
Brazil

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-76577-8 ISBN 978-3-319-76578-5 (eBook)
<https://doi.org/10.1007/978-3-319-76578-5>

Library of Congress Control Number: 2018934351

LNCS Sublibrary: SL4 – Security and Cryptology

© International Association for Cryptologic Research 2018

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 the registered company Springer International Publishing AG
part of Springer Nature
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The 21st IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC 2018) was held March 25–29, 2018, in Rio de Janeiro, Brazil. The conference is sponsored by the International Association for Cryptologic Research (IACR) and focuses on all technical aspects of public-key cryptography.

These proceedings consist of two volumes including 49 papers that were selected by the Program Committee from 186 submissions. Each submission was assigned to at least three reviewers while submissions co-authored by Program Committee members received at least four reviews. Following the initial reviewing phase, the submissions were discussed over a period of five weeks. During this discussion phase, the Program Committee used quite intensively a recent feature of the review system, which allows Program Committee members to anonymously ask questions to the authors.

The reviewing and selection process was a challenging task and I am deeply grateful to the Program Committee members and external reviewers for their hard and thorough work. Many thanks also to Shai Halevi for his assistance with the Web submission and review software and for his constant availability.

The conference program also included invited talks by Elette Boyle (IDC Herzliya, Israel) and Hugo Krawczyk (IBM Research, USA). I would like to thank both of them as well as all the other speakers for their contributions to the program.

Finally, I would like to thank Ricardo Dahab, the general chair, for organizing a great conference and all the conference attendees for making this a truly intellectually stimulating event through their active participation.

March 2018

Michel Abdalla

PKC 2018

21st International Conference on Practice and Theory of Public-Key Cryptography

Rio de Janeiro, Brazil
March 25–29, 2018

Sponsored by
The International Association of Cryptologic Research

General Chair

Ricardo Dahab University of Campinas, Brazil

Program Chair

Michel Abdalla CNRS and École Normale Supérieure, France

Program Committee

Shweta Agrawal	Indian Institute of Technology, Madras, India
Prabhanjan Ananth	UCLA and MIT, USA
Diego Aranha	University of Campinas, Brazil
Mihir Bellare	University of California, San Diego, USA
Chris Brzuska	Hamburg University of Technology, Germany
Dario Catalano	Università di Catania, Italy
Jie Chen	East China Normal University, China
Yilei Chen	Boston University, USA
Céline Chevalier	Université Panthéon-Assas Paris 2, France
Kai-Min Chung	Academia Sinica, Taiwan
Dana Dachman-Soled	University of Maryland, USA
Bernardo David	Tokyo Institute of Technology, Japan
Léo Ducas	CWI Amsterdam, The Netherlands
Nico Döttling	FAU Erlangen-Nürnberg, Germany
Pierre-Alain Fouque	Rennes 1 University, France
Sergey Gorbunov	University of Waterloo, Canada
Aurore Guillevic	Inria, France
Carmit Hazay	Bar-Ilan University, Israel
Julia Hesse	Karlsruhe Institute of Technology, Germany
Zahra Jafargholi	Aarhus University, Denmark
Tibor Jager	Paderborn University, Germany
Bhavana Kanukurthi	Indian Institute of Science, India
Markulf Kohlweiss	Microsoft Research and University of Edinburgh, UK

Adeline Langlois	CNRS and Rennes 1 University, France
Payman Mohassel	Visa Research, USA
Ryo Nishimaki	NTT Secure Platform Labs, Japan
Alain Passelègue	UCLA, USA
Arpita Patra	Indian Institute of Science, India
Antigoni Polychroniadou	Cornell University, USA
Carla Ràfols Salvador	Universitat Pompeu Fabra, Spain
Alessandra Scafuro	North Carolina State University, USA
Christian Schaffner	University of Amsterdam & QuSoft, The Netherlands
Gil Segev	Hebrew University, Israel
Jae Hong Seo	Myongji University, South Korea
Qiang Tang	New Jersey Institute of Technology, USA
Mehdi Tibouchi	NTT Secure Platform Laboratories, Japan
Bogdan Warinschi	University of Bristol, UK
Mor Weiss	Northeastern University, USA

Additional Reviewers

Masayuki Abe	Binyi Chen
Shashank Agrawal	Long Chen
Erdem Alkim	Rongmao Chen
Nuttapong Attrapadung	Yu Chen
Saikrishna Badrinarayanan	Nai-Hui Chia
Shi Bai	Arka Rai Choudhuri
Christian Bardertscher	Ashish Choudhury
Hridam Basu	Peter Chvojka
Balthazar Bauer	Michele Ciampi
Carsten Baum	Ran Cohen
Pascal Bemmman	Sandro Coretti
Fabrice Benhamouda	Craig Costello
David Bernhard	Geoffroy Couteau
Pauline Bert	Jan Czajkowski
Olivier Blazy	Anders Dalskov
Guillaume Bonnoron	Luca De Feo
Niek Bouman	Jean Paul Degabriele
Florian Bourse	David Derler
Jacqueline Brendel	Apoorva Deshpande
Ran Canetti	Mario Di Raimondo
Guilhem Castagnos	Luis J. Dominguez Perez
Suvradip Chakraborty	Rafael Dowsley
Nishanth Chandran	Yfke Dulek
Sanjit Chatterjee	Lisa Ekey

Andrew Ellis	Aaron Hutchinson
Lucas Enloe	Ilia Iliashenko
Naomi Ephraim	Sorina Ionica
Thomas Espitau	Malika Izabachène
Leo Fan	Michael Jacobson
Xiong Fan	Joseph Jaeger
Antonio Faonio	Aayush Jain
Prastudy Fauzi	Christian Janson
Armando Faz-Hernández	Stacey Jeffery
Rex Fernando	Saqib Kakvi
Houda Ferradi	Shuichi Katsumata
Claus Fieker	Natasha Kharchenko
Dario Fiore	Sam Kim
Marc Fischlin	Taechan Kim
Benjamin Fuller	Elena Kirshanova
Philippe Gaborit	Fuyuki Kitagawa
Nicolas Gama	Susumu Kiyoshima
Chaya Ganesh	Konrad Kohbrok
Romain Gay	Lisa Kohl
Kai Gellert	Ilan Komargodski
Ran Gelles	Stephan Krenn
Nicholas Genise	Ashutosh Kumar
Paul Germouty	Rafael Kurek
Essam Ghadafi	Eyal Kushilevitz
Satrajit Ghosh	Russell Lai
Irene Giacomelli	Kim Laine
Huijing Gong	Mario Larangeira
Junqing Gong	Changmin Lee
Alonso González	Hyung Tae Lee
Conrado Porto Lopes Gouvêa	Kwangsu Lee
Rishab Goyal	Moon Sung Lee
Paul Grubbs	Nikos Leonardos
Siyao Guo	Iraklis Leontiadis
Divya Gupta	Qinyi Li
Kyoohyung Han	Benoît Libert
Javier Herranz	Weikai Lin
Justin Holmgren	Feng-Hao Liu
Kristina Hostakova	Shengli Liu
Zhengan Huang	Tianren Liu
Andreas Huelsing	Alex Lombardi
Robin Hui	Vadim Lyubashevsky
Shih-Han Hung	Fermi Ma

Gilles Macario-Rat
 Varun Madathil
 Bernardo Magri
 Monosij Maitra
 Christian Majenz
 Hemanta K. Maji
 Giulio Malavolta
 Mary Maller
 Mark Manulis
 Giorgia Azzurra Marson
 Takahiro Matsuda
 Sogol Mazaheri
 Thierry Mefenza
 Peihan Miao
 Ian Miers
 Ameer Mohammed
 Paz Morillo
 Fabrice Mouhartem
 Pratyay Mukherjee
 Pierrick Méaux
 Gregory Neven
 Khoa Nguyen
 David Niehues
 Luca Nizzardo
 Sai Lakshmi Bhavana Obbattu
 Cristina Onete
 Michele Orrù
 Emmanuela Orsini
 Jheyne N. Ortiz
 Daniel Escudero Ospina
 Maris Ozols
 Jiaxin Pan
 Tapas Pandit
 Dimitris Papadopoulos
 Filip Pawlega
 Thomas Peters
 Doung Hieu Phan
 Cecile Pierrot
 Zaira Pindado
 Oxana Poburinnaya
 Chen Qian
 Elizabeth Quaglia
 Liz Quaglia
 Ananth Raghunathan
 Srinivasan Raghuraman
 Somindu C. Ramanna

Divya Ravi
 Guénaél Renault
 Peter Rindal
 Miruna Rosca
 Lior Rotem
 Kai Samelin
 Pratik Sarkar
 Sajin Sasy
 John Schanck
 Peter Scholl
 Dominique Schröder
 Adam Sealton
 Sruthi Sekar
 Nicolas Sendrier
 Barak Shani
 Abhishek Shetty
 Javier Silva
 Mark Simkin
 Luisa Siniscalchi
 Daniel Slamanig
 Ben Smith
 Fang Song
 Eduardo Soria-Vazquez
 Akshayaram Srinivasan
 Ron Steinfeld
 Mario Streifer
 Christoph Striecks
 Atsushi Takayasu
 Benjamin Hong Meng Tan
 Emmanuel Thomé
 Sri Aravinda Thyagarajan
 Ni Trieu
 Rotem Tsabary
 Jorge L. Villar
 Dhinakaran Vinayagamurthy
 Satyanarayana Vusirikala
 Riad S. Wahby
 Kun-Peng Wang
 Mingyuan Wang
 Xiao Wang
 Yuyu Wang
 Yohei Watanabe
 Weiqiang Wen
 Benjamin Wesolowski
 David Wu
 Keita Xagawa

Fan Xiong
Sophia Yakoubov
Shota Yamada
Takashi Yamakawa
Avishay Yanai
Rupeng Yang
Arkady Yerukhimovich
Eylon Yogev
Zuoxia Yu

Aaram Yun
Mohammad Zaheri
Mark Zhandry
Daode Zhang
Jiang Zhang
Kai Zhang
Ren Zhang
Linfeng Zhou

Sponsoring Institutions

Accenture Digital (<https://www.accenture.com/br-pt/digital-index>)
ERC CryptoCloud (<http://www.di.ens.fr/users/pointche/cryptocloud.php>)
Scyphir Unipessoal, LDA (<http://scyphir.pt>)

Contents – Part I

Key-Dependent-Message and Selective-Opening Security

New Constructions of Identity-Based and Key-Dependent Message Secure Encryption Schemes	3
<i>Nico Döttling, Sanjam Garg, Mohammad Hajiabadi, and Daniel Masny</i>	
Key Dependent Message Security and Receiver Selective Opening Security for Identity-Based Encryption	32
<i>Fuyuki Kitagawa and Keisuke Tanaka</i>	
Tightly SIM-SO-CCA Secure Public Key Encryption from Standard Assumptions	62
<i>Lin Lyu, Shengli Liu, Shuai Han, and Dawu Gu</i>	

Searchable and Fully Homomorphic Encryption

Multi-Key Searchable Encryption, Revisited	95
<i>Ariel Hamlin, Abhi Shelat, Mor Weiss, and Daniel Wichs</i>	
Fully Homomorphic Encryption from the Finite Field Isomorphism Problem	125
<i>Yarkin Doröz, Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman, Berk Sunar, William Whyte, and Zhenfei Zhang</i>	

Public-Key Encryption

Hybrid Encryption in a Multi-user Setting, Revisited	159
<i>Federico Giacon, Eike Kiltz, and Bertram Poettering</i>	
KEM Combiners	190
<i>Federico Giacon, Felix Heuer, and Bertram Poettering</i>	
Revisiting Proxy Re-encryption: Forward Secrecy, Improved Security, and Applications	219
<i>David Derler, Stephan Krenn, Thomas Lorünser, Sebastian Ramacher, Daniel Slamanig, and Christoph Striecks</i>	

Encryption with Bad Randomness

Hedged Nonce-Based Public-Key Encryption: Adaptive Security Under Randomness Failures	253
<i>Zhengan Huang, Junzuo Lai, Wenbin Chen, Man Ho Au, Zhen Peng, and Jin Li</i>	
Related Randomness Security for Public Key Encryption, Revisited	280
<i>Takahiro Matsuda and Jacob C. N. Schuldt</i>	

Subversion Resistance

Subversion-Zero-Knowledge SNARKs.	315
<i>Georg Fuchsbauer</i>	
Public-Key Encryption Resistant to Parameter Subversion and Its Realization from Efficiently-Embeddable Groups	348
<i>Benedikt Auerbach, Mihir Bellare, and Eike Kiltz</i>	

Cryptanalysis

A Practical Cryptanalysis of WalnutDSA TM	381
<i>Daniel Hart, DoHoon Kim, Giacomo Micheli, Guillermo Pascual-Perez, Christophe Petit, and Yuxuan Quek</i>	
Speed-Ups and Time–Memory Trade-Offs for Tuple Lattice Sieving	407
<i>Gottfried Herold, Elena Kirshanova, and Thijs Laarhoven</i>	
Fast Lattice Basis Reduction Suitable for Massive Parallelization and Its Application to the Shortest Vector Problem	437
<i>Tadanori Teruya, Kenji Kashiwabara, and Goichiro Hanaoka</i>	

Composable Security

Reusing Tamper-Proof Hardware in UC-Secure Protocols	463
<i>Jeremias Mechler, Jörn Müller-Quade, and Tobias Nilges</i>	
On Composable Security for Digital Signatures.	494
<i>Christian Badertscher, Ueli Maurer, and Björn Tackmann</i>	

Oblivious Transfer

Equational Security Proofs of Oblivious Transfer Protocols	527
<i>Baiyu Li and Daniele Micciancio</i>	

Extending Oblivious Transfer with Low Communication via Key-Homomorphic PRFs	554
<i>Peter Scholl</i>	

Multiparty Computation

Committed MPC: Maliciously Secure Multiparty Computation from Homomorphic Commitments	587
<i>Tore K. Frederiksen, Benny Pinkas, and Avishay Yanai</i>	
Fast Garbling of Circuits over 3-Valued Logic	620
<i>Yehuda Lindell and Avishay Yanai</i>	
Efficient Covert Two-Party Computation	644
<i>Stanislaw Jarecki</i>	
Towards Characterizing Securely Computable Two-Party Randomized Functions.	675
<i>Deepesh Data and Manoj Prabhakaran</i>	
On the Message Complexity of Secure Multiparty Computation	698
<i>Yuval Ishai, Manika Mittal, and Rafail Ostrovsky</i>	
Author Index	713

Contents – Part II

Signatures

SOFIA: \mathcal{MQ} -Based Signatures in the QROM	3
<i>Ming-Shing Chen, Andreas Hülsing, Joost Rijneveld, Simona Samardjiska, and Peter Schwabe</i>	
A Unified Framework for Trapdoor-Permutation-Based Sequential Aggregate Signatures.	34
<i>Craig Gentry, Adam O’Neill, and Leonid Reyzin</i>	
Constant-Size Group Signatures from Lattices.	58
<i>San Ling, Khoa Nguyen, Huaxiong Wang, and Yanhong Xu</i>	
Attribute-Based Signatures for Unbounded Circuits in the ROM and Efficient Instantiations from Lattices	89
<i>Ali El Kaafarani and Shuichi Katsumata</i>	

Structure-Preserving Signatures

Improved (Almost) Tightly-Secure Structure-Preserving Signatures	123
<i>Charanjit S. Jutla, Miyako Ohkubo, and Arnab Roy</i>	
Weakly Secure Equivalence-Class Signatures from Standard Assumptions . . .	153
<i>Georg Fuchsbauer and Romain Gay</i>	

Functional Encryption

Simple and Generic Constructions of Succinct Functional Encryption	187
<i>Fuyuki Kitagawa, Ryo Nishimaki, and Keisuke Tanaka</i>	
Making Public Key Functional Encryption Function Private, Distributively	218
<i>Xiong Fan and Qiang Tang</i>	
Full-Hiding (Unbounded) Multi-input Inner Product Functional Encryption from the k -Linear Assumption	245
<i>Pratish Datta, Tatsuaki Okamoto, and Junichi Tomida</i>	

Foundations

Local Non-malleable Codes in the Bounded Retrieval Model	281
<i>Dana Dachman-Soled, Mukul Kulkarni, and Aria Shahverdi</i>	

Non-malleability vs. CCA-Security: The Case of Commitments	312
<i>Brandon Broadnax, Valerie Fetzer, Jörn Müller-Quade, and Andy Rupp</i>	

Obfuscation-Based Cryptographic Constructions

Interactively Secure Groups from Obfuscation	341
<i>Thomas Agrikola and Dennis Hofheinz</i>	
Graded Encoding Schemes from Obfuscation	371
<i>Pooya Farshim, Julia Hesse, Dennis Hofheinz, and Enrique Larraia</i>	

Protocols

Hashing Solutions Instead of Generating Problems: On the Interactive Certification of RSA Moduli	403
<i>Benedikt Auerbach and Bertram Poettering</i>	
Two-Factor Authentication with End-to-End Password Security	431
<i>Stanislaw Jarecki, Hugo Krawczyk, Maliheh Shirvanian, and Nitesh Saxena</i>	

Blockchain

Bootstrapping the Blockchain, with Applications to Consensus and Fast PKI Setup	465
<i>Juan A. Garay, Aggelos Kiayias, Nikos Leonardos, and Giorgos Panagiotakos</i>	

Zero-Knowledge

Efficient Adaptively Secure Zero-Knowledge from Garbled Circuits	499
<i>Chaya Ganesh, Yashvanth Kondi, Arpita Patra, and Pratik Sarkar</i>	
Compact Zero-Knowledge Proofs of Small Hamming Weight.	530
<i>Ivan Damgård, Ji Luo, Sabine Oechsner, Peter Scholl, and Mark Simkin</i>	
Efficient Batch Zero-Knowledge Arguments for Low Degree Polynomials . . .	561
<i>Jonathan Bootle and Jens Groth</i>	
On the Security of Classic Protocols for Unique Witness Relations	589
<i>Yi Deng, Xuyang Song, Jingyue Yu, and Yu Chen</i>	

Lattices

New (and Old) Proof Systems for Lattice Problems.	619
<i>Navid Alamati, Chris Peikert, and Noah Stephens-Davidowitz</i>	
Hash Proof Systems over Lattices Revisited	644
<i>Fabrice Benhamouda, Olivier Blazy, Léo Ducas, and Willy Quach</i>	
Privately Constraining and Programming PRFs, the LWE Way.	675
<i>Chris Peikert and Sina Shiehian</i>	
Learning with Errors and Extrapolated Dihedral Cosets	702
<i>Zvika Brakerski, Elena Kirshanova, Damien Stehlé, and Weiqiang Wen</i>	
Rounded Gaussians: Fast and Secure Constant-Time Sampling for Lattice-Based Crypto	728
<i>Andreas Hülsing, Tanja Lange, and Kit Smeets</i>	
Author Index	759