

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board Members

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, Chennai, 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

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

Dongdai Lin · Kazue Sako (Eds.)

Public-Key Cryptography – PKC 2019

22nd IACR International Conference
on Practice and Theory of Public-Key Cryptography
Beijing, China, April 14–17, 2019
Proceedings, Part II

Editors

Dongdai Lin
SKLOIS, Institute of Information
Engineering
Chinese Academy of Sciences
Beijing, China

Kazuo Sako
Security Research Laboratories
NEC Corporation
Kawasaki, Japan

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-17258-9 ISBN 978-3-030-17259-6 (eBook)
<https://doi.org/10.1007/978-3-030-17259-6>

Library of Congress Control Number: 2019936577

LNCS Sublibrary: SL4 – Security and Cryptology

© International Association for Cryptologic Research 2019

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 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC 2019) was held April 14–17, 2019, in Beijing, China. 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 42 papers that were selected by the Program Committee from 173 submissions. Each submission was assigned to at least three reviewers while submissions co-authored by Program Committee members received at least five reviews. During the 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 we are 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. We thank the authors for promptly responding to the questions raised by the committee, which helped us understand the content of their submissions.

The conference program also included an invited talk by Tatsuaki Okamoto (NTT). We would like to thank the invited speaker as well as all the other speakers and the authors of all submissions for their contributions to the program and conference. Finally, we would like to thank Xiaoyun Wang, the general chair, and all the members of local Organizing Committee for organizing a great conference and all the conference attendees for making this conference a truly intellectually stimulating event through their active participation.

April 2019

Dongdai Lin
Kazue Sako

Program Committee

Erdem Alkim	Ondokuz Mayıs University, Turkey
Diego F. Aranha	Aarhus University, Denmark and University of Campinas, Brazil
Chris Brzuska	Alto University, Finland
Dario Catalano	University of Catania, Italy
Nishanth Chandran	Microsoft, India
Sanjit Chatterjee	Indian Institute of Sciences, India
Jie Chen	East China Normal University, China
Jung Hee Cheon	Seoul National University, Korea
Craig Costello	Microsoft Research, USA
Yi Deng	Chinese Academy of Sciences, China
Leo Ducas	CWI Amsterdam, The Netherlands
Nico Döttling	Cispa Helmholtz Center (i.G.), Germany
Dario Fiore	IMDEA Software Institute, Spain
Pierre-Alain Fouque	Rennes University, France
Feng Hao	University of Warwick, UK
Tibor Jäger	Paderborn University, Germany
Marc Joye	OneSpan, Belgium
Tancrede Lepoint	SRI International, USA
Benoît Libert	CNRS and ENS de Lyon, France
Helger Lipmaa	University of Tartu, Estonia
Feng-Hao Liu	Florida Atlantic University, USA
Takahiro Matsuda	AIIST, Japan
Pratyay Mukherjee	Visa Research, USA
Satoshi Obana	Hosei University, Japan
Miyako Okubo	NICT, Japan
Arpita Patra	Indian Institute of Science, India
Ludovic Perret	Sorbonne University, France
Thomas Peters	UC Louvain, Belgium
Benny Pinkas	Bar-Ilan University, Israel
Bertram Poettering	Royal Holloway, University of London, UK
Antigoni Polychriadiadou	Cornell Tech, USA
Alessandra Scafuro	NC State University, USA
Jae Hong Seo	Hanyang University, South Korea
Qiang Tang	New Jersey Institute of Technology, USA
Huaxiong Wang	Nanyang Technological University, Singapore
Yu Yu	Shanghai Jiaotong University, China

Organizing Committee

Xiaofeng Chen	Xidian University, China
Yu Chen	SKLOIS, Institute of Information Engineering, CAS, China
Shuqin Fan	State Key Laboratory of Cryptology, China

Xinyi Huang	Fujian Normal University, China
Ming Li	SKLOIS, Institute of Information Engineering, CAS, China
Zhe Liu	Nanjing University of Aeronautics and Astronautics, China
Chunming Tang	Guangzhou University, China
Anyu Wang	SKLOIS, Institute of Information Engineering, CAS, China
Jian Weng	Jinan University, China
Baofeng Wu	SKLOIS, Institute of Information Engineering, CAS, China
Fangguo Zhang	Sun Yat-sen University, China
Yunlei Zhao	Fudan University, China

Additional Reviewers

Benjamin Dowling	Ashish Choudhury
Behzad Abdolmaleki	Peter Chvojka
Masayuki Abe	Sadro Coretti
Martin R. Albrecht	Geoffroy Couteau
Pedro G. M. R. Alves	Edouard Cuvelier
Gilad Asharov	Prem Laxman Das
Nuttapong Attrapadung	Bernardo David
Karim Bagheri	Amit Deo
Shi Bai	Apoorva Deshpande
Marshall Ball	Julien Devigne
Manuel Barbosa	Ning Ding
Hridam Basu	Lucas Enloe
Carsten Baum	Jieun Eom
Pascal Bemmann	Naomi Ephraim
Fabrice Benhamouda	Xiong Fan
Pauline Bert	Antonio Faonio
Francesco Berti	Luca De Feo
Ward Beullens	Daniele Friolo
Sauvik Bhattacharya	Georg Fuchsbauer
Olivier Blazy	Ben Fuller
Katharina Boudgoust	Tommaso Gagliardoni
Florian Bourse	Steven Galbraith
Xavier Bultel	Tatiana Galibus
Olive Chakraborty	Chaya Ganesh
Biniy Chen	Romain Gay
Long Chen	Peter Gazi
Rongmao Chen	Kai Gellert
Yu Chen	Nicholas Genise
Wonhee Cho	Satrajit Ghosh

Irene Giacomelli
Junqing Gong
Alonso Gonzalez
Jens Groth
Fabrice Ben Hammouda
Kyoohyung Han
Abida Haque
Javier Herranz
Clemens Heuberger
Minki Hhan
Hyunsook Hong
Seungwan Hong
Jingwei Hu
Qiong Huang
Xinyi Huang
Huisu Jang
Christian Janson
Jinhyuck Jeong
Yun-Seong Ji
Shaoquan Jiang
Zhang Jiang
Charanjit Jutla
R. Kabaleeshwaran
Saqib A. Kakvi
Koray Karabina
Shuichi Katsumata
Yutaka Kawai
Hamidreza Khoshakhlagh
Dongwoo Kim
Duhyeong Kim
Jaeyun Kim
Jiseung Kim
Minkyu Kim
Fuyuki Kitagawa
Susumu Kiyoshima
Kamil Kluczniak
François Koeune
Yashvanth Kondi
Toomas Krips
Shravan Kumar
Rafael Kurek
Fabien Laguillaumie
Junzuo Lai
Qiqi Lai
Hyung Tae Lee
Joohee Lee
Kiwoo Lee
Jiangtao Li
Jie Li
Changlu Lin
Fuchun Lin
Qipeng Liu
Shengli Liu
Zhe Liu
Zhen Liu
Patrick Longa
Steve Lu
Yuan Lu
Lin Lyu
Shunli Ma
Varun Madathil
Monosij Maitra
Giulio Malavolta
Mark Manulis
Chloe Martindale
Daniel Masny
Peihan Miao
Rafael Misoczki
Payman Mohassel
Fabrice Mouhartem
Yi Mu
Sayantan Mukherjee
Pierrick Méaux
Michael Naehrig
Kartik Nayak
Khoa Nguyen
David Niehues
Ryo Nishimaki
Luca Nizzardo
Ariel Nof
Koji Nuida
Sai Lakshmi Bhavana Obbattu
Cristina Onete
Emmanuella Orsini
Jiaxin Pan
Tapas Pandit
Lorenz Panny
Jong Hwan Park
Alain Passelègue
Sikhar Patranabis
Alice Pellet–Mary
Geovandro Pereira

Olivier Pereira
Rachel Player
S. Puria
Erick Purwanto
Baodong Qin
Chen Qian
Mario Di Raimondo
Somindu C. Ramanna
Divya Ravi
Joost Renes
Amanda Cristina Davi Resende
Melissa Rossi
Arnab Roy
Paul Rösler
Mohamed Sabt
Yusuke Sakai
Jonas Schneider
Peter Scholl
Jacob Schuldt
Sven Schäge
Adam Sealfon
Sruthi Sekar
Minhye Seo
Akash Shah
Kazumasa Shinagawa
Adam Shull
Janno Siim
Luisa Siniscalchi
Benjamin Smith
Azam Soleimani
Yongha Son
Katerina Sotiraki
Shifeng Sun
Willy Susilo
Koutarou Suzuki
Benjamin Hong Meng Tan
Radu Titiu
Junichi Tomida
Rotem Tsabary
Daniel Tschudi

Anselme Tueno
Dominque Unruh
Muthuramakrishnan Venkatasubramaniam
Daniele Venturi
Sameer Wagh
Michael Walter
Hailong Wang
Liping Wang
Luping Wang
Yu-chen Wang
Yuyu Wang
Zhedong Wang
Weiqiang Wen
Joanne Woodage
Shota Yamada
Takashi Yamakawa
Avishay Yanay
Guomin Yang
Kang Yang
Rupeng Yang
Xu Yanhong
Donggeon Yhee
Jingyue Yu
Yang Yu
Zuoxia Yu
Aaram Yun
Michal Zajac
Ming Zeng
Cong Zhang
Jiang Zhang
Juanyang Zhang
Kai Zhang
Liang Feng Zhang
Mingwu Zhang
Rui Zhang
Xiaojun Zhang
Qian Zhao
Yunlei Zhao
Linfeng Zhou
Giorgos Zirdelis

Contents – Part II

Public Key Encryptions

Collusion Resistant Broadcast and Trace from Positional Witness Encryption	3
<i>Rishab Goyal, Satyanarayana Vusirikala, and Brent Waters</i>	
Break-glass Encryption	34
<i>Alessandra Scafuro</i>	
Registration-Based Encryption from Standard Assumptions	63
<i>Sanjam Garg, Mohammad Hajiabadi, Mohammad Mahmoody, Ahmadreza Rahimi, and Sruthi Sekar</i>	

Functional Encryption

FE for Inner Products and Its Application to Decentralized ABE.	97
<i>Zhedong Wang, Xiong Fan, and Feng-Hao Liu</i>	
Decentralizing Inner-Product Functional Encryption.	128
<i>Michel Abdalla, Fabrice Benhamouda, Markulf Kohlweiss, and Hendrik Waldner</i>	
Non-zero Inner Product Encryption Schemes from Various Assumptions: LWE, DDH and DCR	158
<i>Shuichi Katsumata and Shota Yamada</i>	
Function Private Predicate Encryption for Low Min-Entropy Predicates	189
<i>Sikhar Patranabis, Debdeep Mukhopadhyay, and Somindu C. Ramanna</i>	

Obfuscation Based Cryptography

Adaptively Single-Key Secure Constrained PRFs for NC^1	223
<i>Nuttapong Attrapadung, Takahiro Matsuda, Ryo Nishimaki, Shota Yamada, and Takashi Yamakawa</i>	
Obfuscating Simple Functionalities from Knowledge Assumptions	254
<i>Ward Beullens and Hoeteck Wee</i>	

Re-encryption Schemes

What About Bob? The Inadequacy of CPA Security
for Proxy Reencryption 287
Aloni Cohen

Adaptively Secure Proxy Re-encryption 317
*Georg Fuchsbauer, Chethan Kamath, Karen Klein,
and Krzysztof Pietrzak*

Fundamental Primitives (II)

Generic Constructions of Robustly Reusable Fuzzy Extractor 349
Yunhua Wen, Shengli Liu, and Dawu Gu

Safety in Numbers: On the Need for Robust Diffie-Hellman
Parameter Validation 379
Steven Galbraith, Jake Massimo, and Kenneth G. Paterson

Hunting and Gathering – Verifiable Random Functions from Standard
Assumptions with Short Proofs 408
Lisa Kohl

Post Quantum Cryptography

Lattice-Based Revocable (Hierarchical) IBE with Decryption Key
Exposure Resistance 441
Shuichi Katsumata, Takahiro Matsuda, and Atsushi Takayasu

Towards Non-Interactive Zero-Knowledge for NP from LWE 472
Ron D. Rothblum, Adam Sealfon, and Katerina Sotiraki

More Efficient Algorithms for the NTRU Key Generation Using
the Field Norm 504
Thomas Pornin and Thomas Prest

Efficiently Masking Binomial Sampling at Arbitrary Orders
for Lattice-Based Crypto 534
Tobias Schneider, Clara Paglialonga, Tobias Oder, and Tim Güneysu

Decryption Failure Attacks on IND-CCA Secure Lattice-Based Schemes 565
*Jan-Pieter D’Anvers, Qian Guo, Thomas Johansson, Alexander Nilsson,
Frederik Vercauteren, and Ingrid Verbauwhede*

Reducing the Key Size of McEliece Cryptosystem
from Automorphism-induced Goppa Codes via Permutations 599
Zhe Li, Chaoping Xing, and Sze Ling Yeo

<p>Key Encapsulation Mechanism with Explicit Rejection in the Quantum Random Oracle Model.</p> <p style="padding-left: 2em;"><i>Haodong Jiang, Zhenfeng Zhang, and Zhi Ma</i></p>	<p>618</p>
<p>Factoring Products of Braids via Garside Normal Form</p> <p style="padding-left: 2em;"><i>Simon-Philipp Merz and Christophe Petit</i></p>	<p>646</p>
<p>Author Index</p>	<p>679</p>

Contents – Part I

Cryptographic Protocols

Sub-logarithmic Distributed Oblivious RAM with Small Block Size	3
<i>Eyal Kushilevitz and Tamer Mour</i>	
Lossy Algebraic Filters with Short Tags.	34
<i>Benoît Libert and Chen Qian</i>	
Non-interactive Keyed-Verification Anonymous Credentials	66
<i>Geoffroy Couteau and Michael Reichle</i>	

Digital Signatures

Shorter Ring Signatures from Standard Assumptions	99
<i>Alonso González</i>	
Efficient Attribute-Based Signatures for Unbounded Arithmetic Branching Programs	127
<i>Pratish Datta, Tatsuki Okamoto, and Katsuyuki Takashima</i>	
Efficient Invisible and Unlinkable Sanitizable Signatures	159
<i>Xavier Bultel, Pascal Lafourcade, Russell W. F. Lai, Giulio Malavolta, Dominique Schröder, and Sri Aravinda Krishnan Thyagarajan</i>	
Group Signatures with Selective Linkability	190
<i>Lydia Garms and Anja Lehmann</i>	
Let a Non-barking Watchdog Bite: Cliptographic Signatures with an Offline Watchdog	221
<i>Sherman S. M. Chow, Alexander Russell, Qiang Tang, Moti Yung, Yongjun Zhao, and Hong-Sheng Zhou</i>	

Zero-Knowledge

Zero-Knowledge Elementary Databases with More Expressive Queries	255
<i>Benoît Libert, Khoa Nguyen, Benjamin Hong Meng Tan, and Huaxiong Wang</i>	
Efficient Non-Interactive Zero-Knowledge Proofs in Cross-Domains Without Trusted Setup.	286
<i>Michael Backes, Lucjan Hanzlik, Amir Herzberg, Aniket Kate, and Ivan Pryvalov</i>	

Shorter Quadratic QA-NIZK Proofs.	314
<i>Vanessa Daza, Alonso González, Zaira Pindado, Carla Ràfols, and Javier Silva</i>	
Short Discrete Log Proofs for FHE and Ring-LWE Ciphertexts	344
<i>Rafael del Pino, Vadim Lyubashevsky, and Gregor Seiler</i>	
Publicly Verifiable Proofs from Blockchains.	374
<i>Alessandra Scafuro, Luisa Siniscalchi, and Ivan Visconti</i>	
Identity-Based Encryption	
Identity-Based Broadcast Encryption with Efficient Revocation.	405
<i>Aijun Ge and Puwen Wei</i>	
Tightly Secure Hierarchical Identity-Based Encryption.	436
<i>Roman Langrehr and Jiaxin Pan</i>	
Leakage-Resilient Identity-Based Encryption in Bounded Retrieval Model with Nearly Optimal Leakage-Ratio.	466
<i>Ryo Nishimaki and Takashi Yamakawa</i>	
Additively Homomorphic IBE from Higher Residuosity.	496
<i>Michael Clear and Ciaran McGoldrick</i>	
Fundamental Primitives (I)	
Upper and Lower Bounds for Continuous Non-Malleable Codes.	519
<i>Dana Dachman-Soled and Mukul Kulkarni</i>	
Improved Security Evaluation Techniques for Imperfect Randomness from Arbitrary Distributions	549
<i>Takahiro Matsuda, Kenta Takahashi, Takao Murakami, and Goichiro Hanaoka</i>	
On Tightly Secure Primitives in the Multi-instance Setting.	581
<i>Dennis Hofheinz and Ngoc Khanh Nguyen</i>	
Author Index	613