

Goichiro Hanaoka
Junji Shikata
Yohei Watanabe (Eds.)

LNCS 13177

Public-Key Cryptography – PKC 2022

25th IACR International Conference
on Practice and Theory of Public-Key Cryptography
Virtual Event, March 8–11, 2022
Proceedings, Part I



Part I



 Springer

Founding Editors

Gerhard Goos

Karlsruhe Institute of Technology, Karlsruhe, Germany

Juris Hartmanis

Cornell University, Ithaca, NY, USA

Editorial Board Members

Elisa Bertino

Purdue University, West Lafayette, IN, USA

Wen Gao

Peking University, Beijing, China

Bernhard Steffen 

TU Dortmund University, Dortmund, Germany

Gerhard Woeginger 

RWTH Aachen, Aachen, Germany

Moti Yung 

Columbia University, New York, NY, USA

More information about this subseries at <https://link.springer.com/bookseries/7410>

Goichiro Hanaoka · Junji Shikata ·
Yohei Watanabe (Eds.)

Public-Key Cryptography – PKC 2022

25th IACR International Conference
on Practice and Theory of Public-Key Cryptography
Virtual Event, March 8–11, 2022
Proceedings, Part I

Editors

Goichiro Hanaoka
National Institute of Advanced Industrial
Science and Technology (AIST)
Tokyo, Japan

Junji Shikata
Yokohama National University
Yokohama, Japan

Yohei Watanabe
The University of Electro-Communications
Tokyo, Japan

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-97120-5 ISBN 978-3-030-97121-2 (eBook)
<https://doi.org/10.1007/978-3-030-97121-2>

LNCS Sublibrary: SL4 – Security and Cryptology

© International Association for Cryptologic Research 2022

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 25th IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC 2022) was held virtually during March 8–11, 2022. (Initially, the conference was scheduled to be held in Yokohama, Japan, but unfortunately, due to the prolonged global outbreak of COVID-19, it was finally decided to hold the conference virtually.) This conference is organized annually by the International Association of Cryptologic Research (IACR), and is the main IACR-sponsored conference with an explicit focus on public-key cryptography. The proceedings are comprised of two volumes and include the 39 papers that were selected by the Program Committee. (Initially, 40 papers were accepted, but one of them was later withdrawn by the authors.)

A total of 137 submissions were received for consideration for this year’s program. Submissions were assigned to at least three reviewers, while submissions by Program Committee members received at least five reviews. The review period was divided into two stage. The first stage was reserved for individual reviewing and lasted four weeks. It was followed by the second stage, which lasted about five weeks, in which the Program Committee members engaged in discussion. On a number of occasions, authors were contacted regarding reviewer questions and provided clarifications. One of the papers was conditionally accepted and received a final additional round of reviewing. The reviewing and paper selection process was a difficult task and I am deeply grateful to the members of the Program Committee for their hard and thorough work. Additionally, my deep gratitude is extended to the 145 external reviewers who assisted the Program Committee. PKC 2022 was the first PKC to use HotCRP in the peer review process. I would like to express my sincere thanks to Kevin McCurley for his support in using HotCRP.

Two invited talks were given at PKC 2022. The first invited talk, entitled “The First 25 Years of the PKC Annual Conference”, was delivered by Yuliang Zheng, who is the chair of the PKC steering committee. Since PKC 2022 was the 25th PKC, this invited talk was a review of the history of the past quarter century. The second invited talk, entitled “The Beginning of the End: The First NIST PQC Standards”, was delivered by Dustin Moody. In this invited talk, he presented the latest status of NIST Post-Quantum Cryptography Standardization. I would like to express my deepest gratitude to both invited speakers for accepting the invitation and contributing to the program this year as well as all the authors who submitted their work. I would like to also thank co-editors of these two volumes, Junji Shikata and Yohei Watanabe, who served as general co-chairs this year. I would also like to express my appreciation to the PKC 2022 local organizing committee members (Keita Emura, Ryuya Hayashi, Takahiro Matsuda, Takayuki Nagane, Yusuke Naito, Kazumasa Shinagawa, Jacob Schuldt, Naoto Yanai, and Kazuki Yoneyama) for their dedication and cooperation. Finally, I am deeply grateful to our industry sponsors, listed on the conference’s website, who provided generous financial support.

Organization

General Chair

Junji Shikata
Yohei Watanabe

Yokohama National University, Japan
University of Electro-Communications, Japan

Program Committee Chair

Goichiro Hanaoka

AIST, Japan

Steering Committee

Masayuki Abe
Jung Hee Cheon
Yvo Desmedt
Juan Garay
Goichiro Hanaoka
Aggelos Kiayias
Tanja Lange
David Pointcheval
Moti Yung
Yuliang Zheng (Chair)

NTT, Japan
Seoul National University, South Korea
University of Texas at Dallas, USA
Texas A&M University, USA
AIST, Japan
University of Edinburgh, UK
Eindhoven University of Technology, Netherlands
ENS, France
Google and Columbia University, USA
University of Alabama at Birmingham, USA

Program Committee

Prabhanjan Ananth
Daniel Apon
Christian Badertscher
Manuel Barbosa
Carsten Baum
Jonathan Bootle
Chris Brzuska
Liqun Chen
Ilaria Chillotti
Craig Costello
Geoffroy Couteau
Bernardo David
Nico Döttling

University of California, Santa Barbara, USA
NIST, USA
IOHK, Switzerland
University of Porto and INESC TEC, Portugal
Aarhus University, Denmark
IBM Research Zurich, Switzerland
Aalto University, Finland
University of Surrey, UK
ZAMA, France
Microsoft Research, USA
Paris Diderot University, France
IT University of Copenhagen, Denmark
CISPA, Germany

Thomas Espitau	NTT, Japan
Sebastian Faust	TU Darmstadt, Germany
Dario Fiore	IMDEA Software Institute, Spain
Pierre-Alain Fouque	ENS, France
Pierrick Gaudry	CNRS, Nancy, France
Junqing Gong	East China Normal University, China
Rishab Goyal	MIT, USA
Goichiro Hanaoka	AIST, Japan
Shuichi Katsumata	AIST, Japan
Elena Kirshanova	Immanuel Kant Baltic Federal University, Russia, and Ruhr-Universität Bochum, Germany
Fuyuki Kitagawa	NTT, Japan
Ilan Komargodski	Hebrew University of Jerusalem, Israel, and NTT Research, USA
Tanja Lange	Technische Universiteit Eindhoven, The Netherlands
Changmin Lee	KIAS, South Korea
Benoit Libert	CNRS and ENS de Lyon, France
Feng-Hao Liu	Florida Atlantic University, USA
Giulio Malavolta	Max Planck Institute for Security and Privacy, Germany
Alexander May	Ruhr-Universität Bochum, Germany
Jiaxin Pan	NTNU, Norway
Alice Pellet-Mary	CNRS and University of Bordeaux, France
Christophe Petit	Université libre de Bruxelles, Belgium
Bertram Poettering	IBM Research Zurich, Switzerland
Jacob Schuldt	AIST, Japan
Luisa Siniscalchi	Aarhus University, Denmark
Yongsoo Song	Seoul National University, South Korea
Akshayaram Srinivasan	Tata Institute of Fundamental Research, India
Igors Stepanovs	ETH Zürich, Switzerland
Atsushi Takayasu	University of Tokyo, Japan
Qiang Tang	University of Sydney, Australia
Serge Vaudenay	EPFL, Switzerland
Benjamin Wesolowski	Institut de Mathématiques de Bordeaux, France
David Wu	University of Texas at Austin, USA
Keita Xagawa	NTT, Japan
Bo-Yin Yang	Academia Sinica, Taiwan
Yu Yu	Shanghai Jiao Tong University, China
Mark Zhandry	Princeton University and NTT Research, USA

Additional Reviewers

Nuttapong Attrapadung
Subhadeep Banik
Razvan Barbulescu
James Bartusek
Andrea Basso
Balthazar Bauer
Daniel J. Bernstein
Pedro Branco
Yanlin Chen
Arka Rai Choudhuri
Sherman S. M. Chow
Daniel Collins
Sandro Coretti
Maria Corte-Real Santos
Ben Curtis
Jan Czajkowski
Poulami Das
Thomas Decru
Rafael Del Pino
Amit Deo
Jelle Don
Jesko Dujmovic
Julien Duman
Reo Eriguchi
Andreas Erwig
Daniel Escudero
Andre Esser
Hanwen Feng
Matthias Fitzl
Cody Freitag
Hiroki Furue
Rachit Garg
Romain Gay
Nicholas Genise
Lorenzo Gentile
Satrajit Ghosh
Aarushi Goel
Aditya Gulati
Keisuke Hara
Dominik Hartmann
Keitaro Hashimoto
Kathrin Hoevelmanns
Lois Hughenin-Dumittan

Yasuhiko Ikematsu
Iliia Iliashenko
Ryoma Ito
Joseph Jaeger
Aayush Jain
Sam Jaques
Yao Jiang
Fatih Kaleoglu
Harish Karthikeyan
Hamidreza Khoshakhlagh
Jiseung Kim
Duhyeong Kim
Susumu Kiyoshima
Dimitris Kolonelos
Yashvanth Kondi
Anders Konring
David Kretzler
Mikhail Kudinov
Sabrina Kunzweiler
Péter Kutas
Qiqi Lai
Changmin Lee
Jiangtao Li
Yanan Li
Xiao Liang
Mingyu Liang
Jacob Lichtinger
Damien Ligier
Xiangyu Liu
Jiahui Liu
Zhen Liu
Patrick Longa
George Lu
Yuan Lu
Ji Luo
Lin Lyu
Monosij Maitra
Takahiro Matsuda
Pierre Meyer
Carl Miller
Niklas Miller
Hart Montgomery
Pedro Moreno-Sánchez

Fabrice Mouhartem
Alexander Munch-Hansen
Michael Naehrig
Ryo Nishimaki
Anca Nitulescu
Semyon Novoselov
Julian Nowakowski
Kazuma Ohara
Jean-Baptiste Orfila
Maximilian Orlt
Pascal Paillier
Lorenz Panny
Alain Passelègue
Ray Perlner
Thomas Peters
Sihang Pu
Chen Qian
Tian Qiu
Willy Quach
Anais Querol
Divya Ravi
Michael Reichle
Siavash Riahi
Angela Robinson
Yusuke Sakai
Shingo Sato
Lars Schlieper
Yu-Ching Shen
Sina Shiehian

Tjerand Silde
Daniel Slamanig
Daniel Smith-Tone
Yongha Son
Fang Song
Nick Spooner
Shifeng Sun
Abdullah Talayhan
Bénédict Tran
Ida Tucker
Bogdan Ursu
Prashant Vasudevan
Michael Walter
Yuyu Wang
Han Wang
Zhedong Wang
Florian Weber
Charlotte Weitkaemper
Yunhua Wen
Stella Wohning
David Wu
Shota Yamada
Takashi Yamakawa
Yusuke Yoshida
Greg Zaverucha
Runzhi Zeng
Xiao Zhang
Yongjun Zhao

Contents – Part I

Cryptanalysis

Multitarget Decryption Failure Attacks and Their Application to Saber and Kyber	3
<i>Jan-Pieter D’Anvers and Senne Batsleer</i>	
Post-quantum Security of Plain OAEP Transform	34
<i>Ehsan Ebrahimi</i>	
On the Security of OSIDH	52
<i>Pierrick Dartois and Luca De Feo</i>	
Time-Memory Tradeoffs for Large-Weight Syndrome Decoding in Ternary Codes	82
<i>Pierre Karpman and Charlotte Lefevre</i>	
Syndrome Decoding Estimator	112
<i>Andre Esser and Emanuele Bellini</i>	
On the Isogeny Problem with Torsion Point Information	142
<i>Tako Boris Fouotsa, Péter Kutas, Simon-Philipp Merz, and Yan Bo Ti</i>	

MPC and Secret Sharing

Reusable Two-Round MPC from LPN	165
<i>James Bartusek, Sanjam Garg, Akshayaram Srinivasan, and Yinuo Zhang</i>	
On the Bottleneck Complexity of MPC with Correlated Randomness	194
<i>Claudio Orlandi, Divya Ravi, and Peter Scholl</i>	
Low-Communication Multiparty Triple Generation for SPDZ from Ring-LPN	221
<i>Damiano Abram and Peter Scholl</i>	
Storing and Retrieving Secrets on a Blockchain	252
<i>Vipul Goyal, Abhiram Kothapalli, Elisaweta Masserova, Bryan Parno, and Yifan Song</i>	
CNF-FSS and Its Applications	283
<i>Paul Bunn, Eyal Kushilevitz, and Rafail Ostrovsky</i>	

Cryptographic Protocols

Efficient Verifiable Partially-Decryptable Commitments from Lattices
and Applications 317
Muhammed F. Esgin, Ron Steinfeld, and Raymond K. Zhao

Making Private Function Evaluation Safer, Faster, and Simpler 349
Yi Liu, Qi Wang, and Siu-Ming Yiu

Two-Round Oblivious Linear Evaluation from Learning with Errors 379
Pedro Branco, Nico Döttling, and Paulo Mateus

Improved Constructions of Anonymous Credentials
from Structure-Preserving Signatures on Equivalence Classes 409
Aisling Connolly, Pascal Lafourcade, and Octavio Perez Kempner

Traceable PRFs: Full Collusion Resistance and Active Security 439
Sarasij Maitra and David J. Wu

Tools

Radical Isogenies on Montgomery Curves 473
Hiroshi Onuki and Tomoki Moriya

Towards a Simpler Lattice Gadget Toolkit 498
Shiduo Zhang and Yang Yu

SNARKs and NIZKs

Polynomial IOPs for Linear Algebra Relations 523
Alan Szepieniec and Yuncong Zhang

A Unified Framework for Non-universal SNARKs 553
Helger Lipmaa

ECLIPSE: Enhanced Compiling Method for Pedersen-Committed
zkSNARK Engines 584
*Diego F. Aranha, Emil Madsen Bennedsen, Matteo Campanelli,
Chaya Ganesh, Claudio Orlandi, and Akira Takahashi*

Rational Modular Encoding in the DCR Setting: Non-interactive Range
Proofs and Paillier-Based Naor-Yung in the Standard Model 615
Julien Devevey, Benoît Libert, and Thomas Peters

Author Index 647

Contents – Part II

Key Exchange

Post-quantum Asynchronous Deniable Key Exchange and the Signal Handshake	3
<i>Jacqueline Brendel, Rune Fiedler, Felix Günther, Christian Janson, and Douglas Stebila</i>	
Post-quantum Anonymous One-Sided Authenticated Key Exchange Without Random Oracles	35
<i>Ren Ishibashi and Kazuki Yoneyama</i>	

Theory

Lockable Obfuscation from Circularly Insecure Fully Homomorphic Encryption	69
<i>Kamil Kluczniak</i>	
Financially Backed Covert Security	99
<i>Sebastian Faust, Carmit Hazay, David Kretzler, and Benjamin Schlosser</i>	
Lifting Standard Model Reductions to Common Setup Assumptions	130
<i>Ngoc Khanh Nguyen, Eftychios Theodorakis, and Bogdan Warinschi</i>	

Encryption

Efficient Lattice-Based Inner-Product Functional Encryption	163
<i>Jose Maria Bermudo Mera, Angshuman Karmakar, Tilen Marc, and Azam Soleimanian</i>	
The Direction of Updatable Encryption Does Matter	194
<i>Ryo Nishimaki</i>	
Leakage-Resilient IBE/ABE with Optimal Leakage Rates from Lattices	225
<i>Qiqi Lai, Feng-Hao Liu, and Zhedong Wang</i>	
Encapsulated Search Index: Public-Key, Sub-linear, Distributed, and Delegatable	256
<i>Erik Aronesty, David Cash, Yevgeniy Dodis, Daniel H. Gallancy, Christopher Higley, Harish Karthikeyan, and Oren Tysor</i>	

KDM Security for the Fujisaki-Okamoto Transformations in the QROM	286
<i>Fuyuki Kitagawa and Ryo Nishimaki</i>	
A New Security Notion for PKC in the Standard Model: Weaker, Simpler, and Still Realizing Secure Channels	316
<i>Wasilij Beskorovajnov, Roland Gröll, Jörn Müller-Quade, Astrid Ottenhues, and Rebecca Schwerdt</i>	
Signatures	
Lattice-Based Signatures with Tight Adaptive Corruptions and More	347
<i>Jiaxin Pan and Benedikt Wagner</i>	
Count Me In! Extendability for Threshold Ring Signatures	379
<i>Diego F. Aranha, Mathias Hall-Andersen, Anca Nitulescu, Elena Pagnin, and Sophia Yakoubov</i>	
A Note on the Post-quantum Security of (Ring) Signatures	407
<i>Rohit Chatterjee, Kai-Min Chung, Xiao Liang, and Giulio Malavolta</i>	
Logarithmic-Size (Linkable) Threshold Ring Signatures in the Plain Model	437
<i>Abida Haque, Stephan Krenn, Daniel Slamanig, and Christoph Striecks</i>	
On Pairing-Free Blind Signature Schemes in the Algebraic Group Model	468
<i>Julia Kastner, Julian Loss, and Jiayu Xu</i>	
Efficient Lattice-Based Blind Signatures via Gaussian One-Time Signatures . . .	498
<i>Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Maxime Plancon</i>	
Author Index	529