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

Springer

Lecture Notes in Computer Science 13177

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

Springer

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

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 (Initially, 40 papers were accepted, but one of them was later withdrawn by the authors.)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.

March 2022 Goichiro Hanaoka

Organization

General Chair

Junji Shikata	Yokohama National University, Japan
Yohei Watanabe	University of Electro-Communications, Japan

Program Committee Chair

Goichiro Hanaoka	AIST, Japan

Steering Committee

Masayuki Abe	NTT, Japan
Jung Hee Cheon	Seoul National University, South Korea
Yvo Desmedt	University of Texas at Dallas, USA
Juan Garay	Texas A&M University, USA
Goichiro Hanaoka	AIST, Japan
Aggelos Kiayias	University of Edinburgh, UK
Tanja Lange	Eindhoven University of Technology, Netherlands
David Pointcheval	ENS, France
Moti Yung	Google and Columbia University, USA
Yuliang Zheng (Chair)	University of Alabama at Birmingham, USA

Program Committee

Prabhanjan Ananth	University of California, Santa Barbara, USA
Daniel Apon	NIST, USA
Christian Badertscher	IOHK, Switzerland
Manuel Barbosa	University of Porto and INESC TEC, Portugal
Carsten Baum	Aarhus University, Denmark
Jonathan Bootle	IBM Research Zurich, Switzerland
Chris Brzuska	Aalto University, Finland
Liqun Chen	University of Surrey, UK
Ilaria Chillotti	ZAMA, France
Craig Costello	Microsoft Research, USA
Geoffroy Couteau	Paris Diderot University, France
Bernardo David	IT University of Copenhagen, Denmark
Nico Döttling	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 Fitzi
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
Loïs Hughenin-Dumittan
Yasuhiko Ikematsu
Ilia 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
Bénédikt 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

Cryptographic Protocols

Tools

SNARKs and NIZKs

Contents – Part II