Lecture Notes in Computer Science 11505

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

Jintai Ding · Rainer Steinwandt (Eds.)

Post-Quantum Cryptography

10th International Conference, PQCrypto 2019
Chongqing, China, May 8–10, 2019
Revised Selected Papers

Springer

Editors
Jintai Ding
University of Cincinnati
Cincinnati, OH, USA

Rainer Steinwandt
Department of Mathematical Sciences
Florida Atlantic University
Boca Raton, FL, USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-25509-1 ISBN 978-3-030-25510-7 (eBook)
https://doi.org/10.1007/978-3-030-25510-7

LNCS Sublibrary: SL4 – Security and Cryptology

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

PQCrypto 2019, the 10th International Workshop on Post-Quantum Cryptography, was held in Chongqing, China, during May 8–10, 2019.

The aim of the PQCrypto conference series is to serve as a forum for researchers to present and discuss their work on cryptography in an era with large-scale quantum computers.

Following the same model as its predecessor, PQCrypto 2019 adopted a two-stage submission process in which authors registered their paper(s) one week before the final submission deadline.

The conference received 76 submissions with authors from about 30 countries. Each paper (that had not been withdrawn by the authors) was reviewed in private by at least three Program Committee members. The private review phase was followed by an intensive discussion phase, conducted online. At the end of this process, the Program Committee selected 22 papers for inclusion in the technical program and publication in these proceedings. In some cases, a shepherding phase was imposed to ensure that necessary changes were incorporated by the submitting authors, before the paper was accepted for inclusion in the program and these proceedings. The accepted papers cover a broad spectrum of research within the conference's scope, including both the design and the analysis of cryptographic systems.

In addition to the 22 contributed technical presentations, the program featured outstanding invited talks and a presentation on NIST's ongoing post-quantum cryptography standardization process.

Organizing and running this year's edition of the PQCrypto conference series was a team effort, and we are indebted to everyone who helped make PQCrypto 2019 a success. In particular, we would like to thank all members of the Program Committee and the external reviewers who were a vital part of compiling the technical program. Evaluating and discussing the submissions was a labor-intense task, and we truly appreciate the work that went into this. We also owe a big thank you to Professor Hong Xiang from Chongqing University, who made sure that all local arrangements fell into place as needed.

May 2019

Jintai Ding
Rainer Steinwandt

PQCrypto 2019

The 10th International Conference on Post-Quantum Cryptography

Chongqing, China
May 8–10, 2019

Program Chairs

Jintai Ding	University of Cincinnati, USA
Rainer Steinwandt	Florida Atlantic University, USA

Steering Committee

Daniel J. Bernstein	University of Illinois at Chicago, USA
Johannes Buchmann	Technische Universität Darmstadt, Germany
Claude Crépeau	McGill University, Canada
Jintai Ding	University of Cincinnati, USA
Philippe Gaborit	University of Limoges, France
Tanja Lange	Technische Universiteit Eindhoven, The Netherlands
Daniele Micciancio	University of California at San Diego, USA
Michele Mosca	University of Waterloo, Canada
Nicolas Sendrier	Inria, France
Rainer Steinwandt	Florida Atlantic University, USA
Tsuyoshi Takagi	Kyushu University and University of Tokyo, Japan
Bo-Yin Yang	Academia Sinica, Taiwan

Program Committee

Gorjan Alagic	University of Maryland, USA
Martin R. Albrecht	University of London, UK
Yoshinori Aono	National Institute of Communication Technology, Japan
John B. Baena	University Nacional de Colombia, Colombia
Shi Bai	Florida Atlantic University, USA
Lejla Batina	Radboud University, The Netherlands
Daniel J. Bernstein	University of Illinois at Chicago, USA
Johannes Buchmann	Technische Universität Darmstadt, Germany
Chen-Mou Cheng	Osaka University, Japan
Jung Hee Cheon	Seoul National University, Republic of Korea

Thomas Eisenbarth	Universität zu Lübeck, Germany, and Worcester Polytechnic Institute, USA
Ali El Kaafarani	University of Oxford, UK
Scott Fluhrer	Cisco Systems, USA
Philippe Gaborit	Université Limoges, France
Tommaso Gagliardoni	IBM Research, Switzerland
Kris Gaj	George Mason University, USA
María I. González Vasco	University Rey Juan Carlos, Spain
Tim Güneysu	Ruhr-Universität Bochum, DFKI, Germany
Sean Hallgren	Pennsylvania State University, USA
David Jao	University of Waterloo, evolutionQ Inc., Canada
Jiwu Jing	Chinese Academy of Sciences, China
Thomas Johansson	Lund University, Sweden
Antoine Joux	Institut de Mathematique de Jussieu, France
Kwangjo Kim	KAIST, Republic of Korea
Stefan Kölbl	Technical University of Denmark, Denmark
Brad Lackey	University of Maryland, USA
Kristin Lauter	Microsoft Research, USA
Yi-Kai Liu	NIST, USA
Vadim Lubachevsky	IBM Research, USA
Michele Mosca	University of Waterloo, Perimeter Inst., Canada
María Naya-Plasencia	Inria, France
Ruben Niederhagen	Fraunhofer SIT, Germany
Ray Perlner	NIST, USA
Ludovic Perret	Post-Quantum Advanced Technologies, Sorbonne University, France
Edoardo Persichetti	Florida Atlantic University, USA
Albrecht Petzoldt	University of Versailles, France
Thomas Pöppelmann	Infineon Technologies, Germany
Martin Roetteler	Microsoft Research, USA
Alexander Russell	University of Connecticut, USA
Nicolas Sendrier	Inria, France
Junji Shikata	Yokohama National University, Japan
Daniel Smith-Tone	NIST, University of Louisville, USA
Fang Song	Portland State University, USA
Jakub Szefer	Yale University, USA
Damien Stehlé	ENS de Lyon, France
Tsuyoshi Takagi	Kyushu University and University of Tokyo, Japan
Katsuyuki Takashima	Mitsubishi Electric, Japan
Jean-Pierre Tillich	Inria, France
Keita Xagawa	NTT, Japan
Bo-Yin Yang	Academia Sinica, Taiwan
Shengyu Zhang	Tencent, The Chinese University of Hong Kong, SAR China
Zhang Zhenfeng	Chinese Academy of Sciences, China

External Reviewers

Roberto Araujo
Florian Bache
Ward Beullens
Nina Bindel
Denis Butin
Daniel Cabarcas
Ryann Cartor
Crystal Clough
Edward Eaton
Daniel Escudero
Thomas Espitau
Tim Fritzmann
Qian Guo
Javier Herranz
James Howe
Lei Hu
Shih-Han Hung
Shuichi Katsumata
Natasha Kharchenko
Markus Krausz
Aaron Lye
Pedro Maat Massolino
Khoa Nguyen
Tobias Oder
Angel L. Perez Del Pozo
Federico Pintore
Rachel Player
Eamonn Postlethwaite
Thomas Prest
Youming Qiao
Joost Renes
Angela Robinson
Peter Schwabe
Alan Szepieniec
Rotem Tsabary
Javier Verbel
Weiqiang Wen
Yang Yu
Pavol Zajac

Contents

Lattice-Based Cryptography

Learning with Errors

Cryptanalysis

Key Establishment

Isogeny-Based Cryptography

Hash-Based Cryptography

Code-Based Cryptography