Lecture Notes in Computer Science 12100

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

Jintai Ding · Jean-Pierre Tillich (Eds.)

Post-Quantum Cryptography

11th International Conference, PQCrypto 2020
Paris, France, April 15–17, 2020
Proceedings

Springer

Editors

Jintai Ding
University of Cincinnati
Cincinnati, OH, USA

Jean-Pierre Tillich
Inria
Paris, France

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-44222-4 ISBN 978-3-030-44223-1 (eBook)
https://doi.org/10.1007/978-3-030-44223-1

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

PQCrypto 2020, the 11th International Conference on Post-Quantum Cryptography, was held in Paris, France, during April 15–17, 2020. The aim of the PQCrypto conference series is to serve as a forum for researchers to present results and exchange ideas on cryptography in an era with large-scale quantum computers. Following the same model as its predecessors, PQCrypto 2020 adopted a two-stage submission process in which authors registered their paper one week before the final submission deadline. The conference received 91 submissions with authors from 25 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 Each paper (that had not been withdrawn by the authors) was reviewed in private by at least three Program Committee members.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 29 papers for inclusion in the technical program and publication in these proceedings. The accepted papers cover a broad spectrum of research within the conference's scope, including code-, hash-, isogeny-, and lattice-based cryptography, multivariate cryptography, and quantum cryptanalysis. Along with the 29 contributed technical presentations, the program featured outstanding invited talks and a presentation on NIST's post-quantum cryptography standardization. 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 2020 a success. In particular, we would like thank all members of the Program Committee and the external reviewers who were vital in compiling the technical program. Evaluating and discussing the submissions was a labor-intensive task and we truly appreciate the work that went into this. In the name of the community, let us say that we are all indebted to Antoine Joux from Sorbonne University and Nicolas Sendrier from Inria for organizing this meeting.

February 2020

Jintai Ding
Jean-Pierre Tillich

Organization

General Chairs

Antoine Joux	Sorbonne University, France
Nicolas Sendrier	Inria, France

Program Chairs

Jintai Ding	University of Cincinnati, USA
Jean-Pierre Tillich	Inria, France

Steering Committee

Daniel J. Bernstein	University Illinois at Chicago, USA, and Ruhr University Bochum, Germany
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	Waterloo University and Perimeter Institute, Canada
Nicolas Sendrier	Inria, France
Tsuyoshi Takagi	University of Tokyo, Japan
Bo-Yin Yang	Academia Sinica, Taiwan

Program Committee

Reza Azarderakhsh	Florida Atlantic University and PQSecure Technologies, USA
Jean-Philippe Aumasson	Teserakt AG, Switzerland
Yoshinori Aono	National Institute of Communication Technology, Japan
Magali Bardet	University of Rouen, France
Daniel J. Bernstein	University Illinois at Chicago, USA, and Ruhr University Bochum, Germany
Olivier Blazy	University of Limoges, France
André Chailloux	Inria, France
Chen-Mou Cheng	Osaka University and Kanazawa University, Japan
Jung Hee Cheon	Seoul National University, South Korea
Tung Chou	Osaka University, Japan, and Academia Sinica, Taiwan
Dung Duong	University of Wollongong, Australia

Scott Fluhrer	Cisco Systems, USA
Philippe Gaborit	University of Limoges, France
Tommaso Gagliardoni	Kudelski Security, Switzerland
Steven Galbraith	The University of Auckland, New Zealand
Xiao-Shan Gao	Chinese Academy of Sciences, China
Tim Güneysu	Ruhr University Bochum and DFKI, Germany
David Jao	University of Waterloo and evolutionQ, Canada
Jiwu Jing	Chinese Academy of Sciences, China
Thomas Johansson	Lund University, Sweden
Antoine Joux	Sorbonne University, France
Kwangjo Kim	KAIST, South Korea
Elena Kirshanova	I. Kant Baltic Federal University, Russia
Yi-Kai Liu	NIST and University of Maryland, USA
Prabhat Mishra	University of Florida, USA
Michele Mosca	Waterloo University and Perimeter Institute, Canada
María Naya-Plasencia	Inria, France
Khoa Nguyen	Nanyang Technological University, Singapore
Ruben Niederhagen	Fraunhofer SIT, Germany
Ray Perlner	NIST, USA
Christophe Petit	University of Birmingham, UK
Rachel Player	University of London, UK
Thomas Pöppelmann	Infineon Technologies, Germany
Thomas Prest	PQShield, UK
Nicolas Sendrier	Inria, France
Junji Shikata	Yokohama National University, Japan
Daniel Smith-Tone	NIST and University of Louisville, USA
Rainer Steinwandt	Florida Atlantic University, USA
Damien Stehlé	ENS de Lyon, France
Tsuyoshi Takagi	University of Tokyo, Japan
Routo Terada	University of São Paulo, Brasil
Serge Vaudenay	EPFL, Switzerland
Keita Xagawa	NTT Secure Platform Laboratories, Japan
Bo-Yin Yang	Academia Sinica, Taiwan
Zhenfeng Zhang	Institute of Software, Chinese Academy of Sciences, China

Additional Reviewers

Nicolas Aragon
Florian Bache
Subhadeep Banik
Khashayar Barooti
Loic Bidoux
Nina Bindel
Xavier Bonnetain
Wouter Castryck
Ming-Shing Chen
Ding-Yuan Cheng
Ilaria Chillotti
Wonhee Cho
Gwangbae Choi
Alain Couvreur
Benjamin Curtis
Bernardo David
Luca De Feo
Rafael Pablo Del Pino
Amit Deo
Hülya Evkan
Xiutao Feng

Tim Fritzmann
Leon Groot Bruinderink
Qian Guo
Yasufumi Hashimoto
Minki Hhan
Seungwan Hong
James Howe
Zhenyu Huang
Loïs Huguenin-Dumittan
Aaron Hutchinson
Yasuhiko Ikematsu
Mitsugu Iwamoto
Saqib A. Kakvi
Elif Bilge Kavun
Duhyeong Kim
Brian Koziel
Peter Kutas
Norman Lahr
Georg Land
Keewoo Lee
Seungbeom Lee
Matthieu Lequesne
Sarah McCarthy
Romy Minko
Erik Mårtensson
Alexander Nilsson
Richard Petri
Ben Pring
Renato Renner
Jan Richter-Brockmann
Yolan Romailler
Miruna Rosca
Rei Safavi-Naini
Amin Sakzad
John Schanck
André Schrottenloher
Hwajeong Seo
Arnaud Sipasseuth
Yongha Son
Junichi Tomida
David Urbanik
Valentin Vasseur
Javier Verbel
Reynaldo Villena
Fernando Virdia
Daniel Volya
Yacheng Wang
Yuntao Wang
Yohei Watanabe
Julian Wälde
Haiyang Xue
Masaya Yasuda
Greg Zaverucha

Organization and Sponsors

The conference was organized by Inria and Sorbonne University, with the support of the ERC Almacrypt[1].
The organizers thank the following companies and institutions for their generous financial support:

Amazon Web Services, USA
Cisco Systems, USA
Infineon Technologies, Germany
PQShield, UK
Worldline, France

[1] European Union's H2020 Program under grant agreement number ERC-669891.

Contents

Code-Based Cryptography

Implementation

Isogeny-Based Cryptography

Lattice-Based Cryptography

Multivariate Cryptography

Quantum Algorithms

Security Proofs