

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 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

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

© Springer Nature Switzerland AG 2020

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

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 to 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
Nicolas Sendrier

Sorbonne University, France
Inria, France

Program Chairs

Jintai Ding
Jean-Pierre Tillich

University of Cincinnati, USA
Inria, France

Steering Committee

Daniel J. Bernstein
Johannes Buchmann
Claude Crépeau
Jintai Ding
Philippe Gaborit
Tanja Lange
Daniele Micciancio
Michele Mosca
Nicolas Sendrier
Tsuyoshi Takagi
Bo-Yin Yang

University Illinois at Chicago, USA, and Ruhr
University Bochum, Germany
Technische Universität Darmstadt, Germany
McGill University, Canada
University of Cincinnati, USA
University of Limoges, France
Technische Universiteit Eindhoven, The Netherlands
University of California at San Diego, USA
Waterloo University and Perimeter Institute, Canada
Inria, France
University of Tokyo, Japan
Academia Sinica, Taiwan

Program Committee

Reza Azarderakhsh
Jean-Philippe Aumasson
Yoshinori Aono
Magali Bardet
Daniel J. Bernstein
Olivier Blazy
André Chailloux
Chen-Mou Cheng
Jung Hee Cheon
Tung Chou
Dung Duong

Florida Atlantic University and PQSecure
Technologies, USA
Taserakt AG, Switzerland
National Institute of Communication Technology,
Japan
University of Rouen, France
University Illinois at Chicago, USA, and Ruhr
University Bochum, Germany
University of Limoges, France
Inria, France
Osaka University and Kanazawa University, Japan
Seoul National University, South Korea
Osaka University, Japan, and Academia Sinica, Taiwan
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
Maria 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	Wouter Castryck	Benjamin Curtis
Florian Bache	Ming-Shing Chen	Bernardo David
Subhadeep Banik	Ding-Yuan Cheng	Luca De Feo
Khashayar Barooti	Ilaria Chillotti	Rafael Pablo Del Pino
Loic Bidoux	Wonhee Cho	Amit Deo
Nina Bindel	Gwangbae Choi	Hülya Evkan
Xavier Bonnetain	Alain Couvreur	Xiutao Feng

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

Organization and Sponsors

The conference was organized by Inria and Sorbonne University, with the support of the ERC Almacrypt¹.

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

Randomized Decoding of Gabidulin Codes Beyond the Unique Decoding Radius.	3
<i>Julian Renner, Thomas Jerkovits, Hannes Bartz, Sven Puchinger, Pierre Loidreau, and Antonia Wachter-Zeh</i>	
About Low DFR for QC-MDPC Decoding.	20
<i>Nicolas Sendrier and Valentin Vasseur</i>	
QC-MDPC Decoders with Several Shades of Gray	35
<i>Nir Drucker, Shay Gueron, and Dusan Kostic</i>	

Implementation

Isochronous Gaussian Sampling: From Inception to Implementation: With Applications to the Falcon Signature Scheme.	53
<i>James Howe, Thomas Prest, Thomas Ricosset, and Mélissa Rossi</i>	
Benchmarking Post-quantum Cryptography in TLS	72
<i>Christian Paquin, Douglas Stebila, and Goutam Tamvada</i>	
Efficient Key Generation for Rainbow	92
<i>Albrecht Petzoldt</i>	

Isogeny-Based Cryptography

CSIDH on the Surface.	111
<i>Wouter Castryck and Thomas Decru</i>	
LegRoast: Efficient Post-quantum Signatures from the Legendre PRF	130
<i>Ward Beullens and Cyprien Delpech de Saint Guilhem</i>	
The Supersingular Isogeny Problem in Genus 2 and Beyond	151
<i>Craig Costello and Benjamin Smith</i>	
Sashimi: Cutting up CSI-FiSh Secret Keys to Produce an Actively Secure Distributed Signing Protocol.	169
<i>Daniele Cozzo and Nigel P. Smart</i>	

Lattice-Based Cryptography

Defeating NewHope with a Single Trace	189
<i>Dorian Amiet, Andreas Curiger, Lukas Leuenberger, and Paul Zbinden</i>	
Decryption Failure Is More Likely After Success	206
<i>Nina Bindel and John M. Schanck</i>	
Compact Privacy Protocols from Post-quantum and Timed Classical Assumptions	226
<i>Jonathan Bootle, Anja Lehmann, Vadim Lyubashevsky, and Gregor Seiler</i>	
Efficient Post-quantum SNARKs for RSIS and RLWE and Their Applications to Privacy	247
<i>Cecilia Boschini, Jan Camenisch, Max Ovsiankin, and Nicholas Spooner</i>	
Short Zero-Knowledge Proof of Knowledge for Lattice-Based Commitment . . .	268
<i>Yang Tao, Xi Wang, and Rui Zhang</i>	
COSAC: COMpact and Scalable Arbitrary-Centered Discrete Gaussian Sampling over Integers	284
<i>Raymond K. Zhao, Ron Steinfeld, and Amin Sakzad</i>	

Multivariate Cryptography

Combinatorial Rank Attacks Against the Rectangular Simple Matrix Encryption Scheme	307
<i>Daniel Apon, Dustin Moody, Ray Perlner, Daniel Smith-Tone, and Javier Verbel</i>	
A Structural Attack on Block-Anti-Circulant UOV at SAC 2019.	323
<i>Hiroki Furue, Koha Kinjo, Yasuhiko Ikematsu, Yacheng Wang, and Tsuyoshi Takagi</i>	
Generalization of Isomorphism of Polynomials with Two Secrets and Its Application to Public Key Encryption	340
<i>Bagus Santoso</i>	
Practical Cryptanalysis of k -ary C^*	360
<i>Daniel Smith-Tone</i>	
A Rank Attack Against Extension Field Cancellation.	381
<i>Daniel Smith-Tone and Javier Verbel</i>	
Multivariate Encryption Schemes Based on Polynomial Equations over Real Numbers	402
<i>Takanori Yasuda, Yacheng Wang, and Tsuyoshi Takagi</i>	

Quantum Algorithms

Improved Quantum Circuits for Elliptic Curve Discrete Logarithms.	425
<i>Thomas Häner, Samuel Jaques, Michael Naehrig, Martin Roetteler, and Mathias Soeken</i>	
The Power of Few Qubits and Collisions – Subset Sum Below Grover’s Bound	445
<i>Alexander Helm and Alexander May</i>	
On Quantum Distinguishers for Type-3 Generalized Feistel Network Based on Separability	461
<i>Samir Hodžić, Lars Knudsen Ramkilde, and Andreas Brasen Kidmose</i>	

Security Proofs

Many a Mickle Makes a Muckle: A Framework for Provably Quantum-Secure Hybrid Key Exchange	483
<i>Benjamin Dowling, Torben Brandt Hansen, and Kenneth G. Paterson</i>	
A Note on the Instantiability of the Quantum Random Oracle	503
<i>Edward Eaton and Fang Song</i>	
Collapseability of Tree Hashes	524
<i>Aldo Günsing and Bart Mennink</i>	
Encryption Schemes Using Random Oracles: From Classical to Post-Quantum Security.	539
<i>Juliane Krämer and Patrick Struck</i>	
Author Index	559