

Jung Hee Cheon  
Thomas Johansson (Eds.)

LNCS 13512

# Post-Quantum Cryptography

13th International Workshop, PQCrypto 2022  
Virtual Event, September 28–30, 2022  
Proceedings



 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*

Moti Yung 

*Columbia University, New York, NY, USA*


More information about this series at <https://www.springer.com/bookseries/558>

Jung Hee Cheon · Thomas Johansson (Eds.)

# Post-Quantum Cryptography

13th International Workshop, PQCrypto 2022  
Virtual Event, September 28–30, 2022  
Proceedings

*Editors*

Jung Hee Cheon   
Seoul National University  
Seoul, Korea (Republic of)

Thomas Johansson  
Lund University  
Lund, Sweden

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-031-17233-5              ISBN 978-3-031-17234-2 (eBook)  
<https://doi.org/10.1007/978-3-031-17234-2>

© The Editor(s) (if applicable) and The Author(s), under exclusive license  
to Springer Nature Switzerland AG 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

PQCrypto 2022, the 13th International Conference on Post-Quantum Cryptography, was organized fully online, during September 28–30, 2022. 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 2022 adopted a two-stage submission process in which authors registered their paper one week before the final submission deadline. The conference received 66 submissions. 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 23 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 23 contributed technical presentations, the program featured three invited talks - by Peter Schwabe on “6 years of NIST PQC, looking back and ahead”, by Andreas Hülsing on “Hash-Based Signatures: History and Challenges”, and by Ward Beullens on “Breaking Rainbow takes a weekend on a laptop”.

The Program Committee selected by voting a paper to receive the Best Paper Award: “Breaking Category 5 SPHINCS+ with SHA-256” by Ray Perlner, David Cooper, and John Kelsey.

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 2022 a success. In particular, we would like thank all members of the Program Committee and the external reviewers who were vital for compiling the technical program. Evaluating and discussing the submissions was a labor-intensive task, and we truly appreciate the work that went into this. On behalf of the community, we are indebted to Tanja Lange for organizing the meeting and managing all the technical challenges of an online event. We also thank the team at Springer for handling the publication of these conference proceedings.

August 2022

Jung Hee Cheon  
Thomas Johansson

# Organization

## General Chair

Tanja Lange  
Eindhoven University of Technology,  
The Netherlands

## Program Committee Chairs

Jung Hee Cheon  
Thomas Johansson  
Seoul National University, South Korea  
Lund University, Sweden

## Program Committee

Magali Bardet  
Daniel J. Bernstein  
University of Rouen Normandy, France  
University of Illinois at Chicago, USA, Ruhr  
University Bochum, Germany, and Academia  
Sinica, Taiwan

Olivier Blazy  
André Chailloux  
Anupam Chattopadhyay  
Chen-Mou Cheng  
Jan-Pieter D'Anvers  
Leo Ducas  
Scott Fluhrer  
Philippe Gaborit  
Tommaso Gagliardoni  
Steven Galbraith  
Qian Guo  
Tim Güneysu  
Dong-Guk Han  
David Jao  
Howon Kim  
Jon-Lark Kim  
Kwangjo Kim  
École Polytechnique, France  
Inria, France  
NTU Singapore, Singapore  
Kanazawa University, Japan  
KU Leuven, Belgium  
CWI, The Netherlands  
Cisco Systems, USA  
University of Limoges, France  
Kudelski Security, Switzerland  
University of Auckland, New Zealand  
Lund University, Sweden  
Ruhr-Universität Bochum and DFKI, Germany  
Kookmin University, South Korea  
University of Waterloo, Canada  
Pusan National University, South Korea  
Sogang University, South Korea  
Korea Advanced Institute of Science and  
Technology, South Korea

Elena Kirshanova  
Immanuel Kant Baltic Federal University, Russia,  
and TII, UAE

Tanja Lange  
Eindhoven University of Technology,  
The Netherlands, and Academia Sinica, Taiwan

Changmin Lee	KIAS, South Korea
Christian Majenz	Technical University Denmark, Denmark
Alexander May	Ruhr-Universität Bochum, Germany
Rafael Misoczki	Google, USA
Michele Mosca	University of Waterloo and Perimeter Institute, Canada
Khoa Nguyen	Nanyang Technological University, Singapore
Ray Perlner	NIST, USA
Christophe Petit	Université libre de Bruxelles, Belgium
Rachel Player	Royal Holloway, University of London, UK
Thomas Prest	PQShield Ltd., UK
Thomas Pöppelmann	Infineon, Germany
Nicolas Sendrier	Inria, France
Jae Hong Seo	Hanyang University, South Korea
Benjamin Smith	Inria, France
Daniel Smith-Tone	University of Louisville and NIST, USA
Yongsoo Song	Seoul National University, South Korea
Damien Stehlé	ENS de Lyon, France
Rainer Steinwandt	University of Alabama in Huntsville, USA
Tsuyoshi Takagi	University of Tokyo, Japan
Keita Xagawa	NTT, Japan
Aaram Yun	Ewha Womans University, South Korea
Zhenfei Zhang	Etherium Foundation, USA

## **Additional Reviewers**

Ward Beullens	Markus Krausz
Xavier Bonnetain	Mikhail Kudinov
Cecilia Boschini	Sabrina Kunzweiler
Pierre Briaud	Georg Land
Jan Richter-Brockmann	Matthieu Lequesne
Maxime Bros	Ekaterina Malygina
Benjamin Curtis	Charles Meyer-Hilfinger
Thomas Debris-Alazard	Prasanna Ravi
Jelle Don	Lars Schlieper
Yu-Hsuan Huang	Tjerand Silde
Loïs Huguenin-Dumittan	Patrick Struck
Alexander Karenin	Valentin Vasseur



# Contents

## Code-Based Cryptography

Hybrid Decoding – Classical-Quantum Trade-Offs for Information Set Decoding .....	3
<i>Andre Esser, Sergi Ramos-Calderer, Emanuele Bellini, José I. Latorre, and Marc Manzano</i>	
How to Backdoor (Classic) McEliece and How to Guard Against Backdoors ...	24
<i>Tobias Hemmert, Alexander May, Johannes Mittmann, and Carl Richard Theodor Schneider</i>	
LRPC Codes with Multiple Syndromes: Near Ideal-Size KEMs Without Ideals .....	45
<i>Carlos Aguilar-Melchor, Nicolas Aragon, Victor Dyseryn, Philippe Gaborit, and Gilles Zémor</i>	
Interleaved Prange: A New Generic Decoder for Interleaved Codes .....	69
<i>Anmoal Porwal, Lukas Holzbaur, Hedongliang Liu, Julian Renner, Antonia Wachter-Zeh, and Violetta Weger</i>	
A Study of Error Floor Behavior in QC-MDPC Codes .....	89
<i>Sarah Arpin, Tyler Raven Billingsley, Daniel Rayor Hast, Jun Bo Lau, Ray Perlner, and Angela Robinson</i>	

## Multivariate Cryptography and the MinRank Problem

Improvement of Algebraic Attacks for Solving Superdetermined MinRank Instances .....	107
<i>Magali Bardet and Manon Bertin</i>	
A New Fault Attack on UOV Multivariate Signature Scheme .....	124
<i>Hiroki Furue, Yutaro Kiyomura, Tatsuya Nagasawa, and Tsuyoshi Takagi</i>	
MR-DSS – Smaller MinRank-Based (Ring-)Signatures .....	144
<i>Emanuele Bellini, Andre Esser, Carlo Sanna, and Javier Verbel</i>	
IPRainbow .....	170
<i>Ryann Cartor, Max Cartor, Mark Lewis, and Daniel Smith-Tone</i>	

2F - A New Method for Constructing Efficient Multivariate Encryption Schemes ..... 185  
*Daniel Smith-Tone*

**Quantum Algorithms, Attacks and Models**

Quantum Attacks on Lai-Massey Structure ..... 205  
*Shuping Mao, Tingting Guo, Peng Wang, and Lei Hu*

Sponge-Based Authenticated Encryption: Security Against Quantum Attackers ..... 230  
*Christian Janson and Patrick Struck*

Post-quantum Plaintext-Awareness ..... 260  
*Ehsan Ebrahimi and Jeroen van Wier*

On Quantum Ciphertext Indistinguishability, Recoverability, and OAEP ..... 286  
*Juliane Krämer and Patrick Struck*

**Implementation and Side Channel Attacks**

Efficiently Masking Polynomial Inversion at Arbitrary Order ..... 309  
*Markus Krausz, Georg Land, Jan Richter-Brockmann, and Tim Güneysu*

A Power Side-Channel Attack on the Reed-Muller Reed-Solomon Version of the HQC Cryptosystem ..... 327  
*Thomas Schamberger, Lukas Holzbaur, Julian Renner, Antonia Wachter-Zeh, and Georg Sigl*

A New Key Recovery Side-Channel Attack on HQC with Chosen Ciphertext ..... 353  
*Guillaume Goy, Antoine Loiseau, and Philippe Gaborit*

**Isogeny**

On Actively Secure Fine-Grained Access Structures from Isogeny Assumptions ..... 375  
*Fabio Campos and Philipp Muth*

Attack on SHeals and HealS: The Second Wave of GPST ..... 399  
*Steven D. Galbraith and Yi-Fu Lai*

Post-Quantum Signal Key Agreement from SIDH ..... 422  
*Samuel Dobson and Steven D. Galbraith*

**Lattice-Based Cryptography**

Forward-Secure Revocable Secret Handshakes from Lattices ..... 453  
*Zhiyuan An, Jing Pan, Yamin Wen, and Fangguo Zhang*

Estimating the Hidden Overheads in the BDGL Lattice Sieving Algorithm ..... 480  
*Léo Ducas*

**Cryptanalysis**

Breaking Category Five SPHINCS<sup>+</sup> with SHA-256 ..... 501  
*Ray Perlner, John Kelsey, and David Cooper*

**Author Index** ..... 523