Jung Hee Cheon
Thomas Johansson (Eds.)

LNCS 13512

Post-Quantum Cryptography

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

Springer

Lecture Notes in Computer Science 13512

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

Springer

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 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 Each paper (that had not been withdrawn by the authors) was reviewed in private by at least three Program Committee members.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-intense 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	Seoul National University, South Korea
Thomas Johansson	Lund University, Sweden

Program Committee

Magali Bardet	University of Rouen Normandy, France
Daniel J. Bernstein	University of Illinois at Chicago, USA, Ruhr University Bochum, Germany, and Academia Sinica, Taiwan
Olivier Blazy	École Polytechnique, France
André Chailloux	Inria, France
Anupam Chattopadhyay	NTU Singapore, Singapore
Chen-Mou Cheng	Kanazawa University, Japan
Jan-Pieter D'Anvers	KU Leuven, Belgium
Leo Ducas	CWI, The Netherlands
Scott Fluhrer	Cisco Systems, USA
Philippe Gaborit	University of Limoges, France
Tommaso Gagliardoni	Kudelski Security, Switzerland
Steven Galbraith	University of Auckland, New Zealand
Qian Guo	Lund University, Sweden
Tim Güneysu	Ruhr-Universität Bochum and DFKI, Germany
Dong-Guk Han	Kookmin University, South Korea
David Jao	University of Waterloo, Canada
Howon Kim	Pusan National University, South Korea
Jon-Lark Kim	Sogang University, South Korea
Kwangjo Kim	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
Xavier Bonnetain
Cecilia Boschini
Pierre Briaud
Jan Richter-Brockmann
Maxime Bros
Benjamin Curtis
Thomas Debris-Alazard
Jelle Don
Yu-Hsuan Huang
Loïs Huguenin-Dumittan
Alexander Karenin
Markus Krausz
Mikhail Kudinov
Sabrina Kunzweiler
Georg Land
Matthieu Lequesne
Ekaterina Malygina
Charles Meyer-Hilfiger
Prasanna Ravi
Lars Schlieper
Tjerand Silde
Patrick Struck
Valentin Vasseur

Contents

Code-Based Cryptography

Multivariate Cryptography and the MinRank Problem

Quantum Algorithms, Attacks and Models

Implementation and Side Channel Attacks

Isogeny

Lattice-Based Cryptography

Cryptanalysis