# PQCrypto 2023

## The 14th International Conference on Post-Quantum Cryptography

August 16-18, 2023
College Park, MD, USA

**INDUSTRY SPONSORS:**

**SILVER**

Amazon Web Services

**BRONZE**

## Conference Proceedings

Since 2006, PQCrypto has served as a forum for researchers to present results and exchange ideas on the topic of cryptography in an era with large-scale quantum computers.

The proceedings of PQCrypto 2023 are being published by Springer in the LNCS Series. They can be accessed for free until September 11, 2023, by following the link from the PQCrypto conference web site at https://pqcrypto2023.umiacs.io/

The proceedings contain 25 papers, which were carefully reviewed and selected from 51 submissions. They are categorized in the following topical sections: code-based cryptography; group-action-based cryptography; isogeny-based cryptography; lattice-based cryptography; multivariate cryptography; quantum algorithms, cryptanalysis and models; post-quantum protocols; and side channel cryptanalysis and countermeasures.

## Program Chairs

- Thomas Johansson, Lund University, Sweden
- Daniel Smith-Tone, University of Louisville, and National Institute of Standards and Technology, USA

## Program Committee

- Magali Bardet, U. of Rouen Normandie, France
- Daniel J. Bernstein, U. Illinois at Chicago, USA, & Ruhr U. Bochum, Germany
- Olivier Blazy, Ecole Polytechnique, France
- Daniel Cabarcas, U. Nacional de Colombia, Colombia
- Ryann Cartor, Clemson U., USA
- André Chailloux, INRIA Paris, France
- Anupam Chattopadhyay, NTU Singapore, Singapore
- Chen-Mou Cheng, BTQ, Taiwan
- Jung Hee Cheon, Seoul National U., Korea
- Jan-Pieter D'Anvers, KU Leuven, Belgium
- Jintai Ding, Tsinghua U., China
- Scott Fluhrer, Cisco Systems, USA
- Philippe Gaborit, U. Limoges, France
- Tommaso Gagliardoni, Kudelski Security, Switzerland
- Qian Guo, Lund U., Sweden
- Tim Güneysu, Ruhr U. Bochum & DFKI, Germany

**Hosted by:**



- Andreas Hülsing, Eindhoven U. Technology, Netherlands
- David Jao, U. Waterloo, Canada
- Thomas Johansson, Lund U., Sweden (chair)
- John Kelsey, NIST, USA & KU Leuven, Belgium
- Howon Kim, Pusan National U., South Korea
- Jon-Lark Kim, Sogang U., South Korea
- Kwangjo Kim, KAIST, South Korea
- Elena Kirshanova, Technology Innovation Inst., UAE
- Tanja Lange, Eindhoven U. Technology, Netherlands
- Changmin Lee, KIAS, South Korea
- Christian Majenz, Technical U. Denmark, Denmark
- Dustin Moody, NIST, USA
- Michele Mosca, U. Waterloo & Perimeter Inst., Canada
- Ray Perlner, NIST, USA
- Thomas Pöppelman, Infineon, Germany
- Thomas Prest, PQShield Ltd., UK
- Angela Robinson, NIST, USA
- Palash Sarkar, ISI, India
- Nicolas Sendrier, INRIA, France
- Jae Hong Seo, Hanyang U., Seoul, Korea
- Benjamin Smith, INRIA, France
- Daniel Smith-Tone, U. Louisville & NIST, USA (chair)
- Yongsoo Song, Seoul National U., South Korea
- Damien Stehlé, CryptoLab, France
- Rainer Steinwandt, U. Alabama at Huntsville, USA
- Tsuyoshi Takagi, U. of Tokyo, Japan
- Atsushi Takayasu, U. of Tokyo, Japan
- Jean-Pierre Tillich, INRIA, France
- Keita Xagawa, NTT, Japan
- Bo-Yin Yang, Academia Sinica, Taiwan
- Yang Yu, Tsinghua U., China
- Yu Yu, Shanghai Jiao Tong U., China
- Aaram Yun, Ewha Womans U., South Korea

## General Chair

- Yi-Kai Liu, NIST and University of Maryland

## Local Organizers

- Gorjan Alagic, University of Maryland and NIST
- Andrew Childs, University of Maryland
- Dustin Moody, NIST
- Rene Peralta, NIST
- Angela Robinson, NIST

With the support of QuICS, the Joint Center for Quantum Information and Computer Science, UMIACS, the University of Maryland Institute for Advanced Computer Studies, and Conference and Visitor Services at the University of Maryland.

# PQCrypto 2023 Program

## Wednesday, August 16th

8:30-8:55
**Registration**

8:55-9:00
**Welcoming Remarks**

### Invited Presentation
9:00-10:00 **Chair: Dustin Moody**

*Isogeny-based cryptography after The Snap*
**Benjamin Wesolowski**

10:00-10:30
**Break**

### Session I: Digital Signatures
10:30-12:10 **Chair: Ryann Cartor**

10:30-10:55
*A Tightly Secure Identity-based Signature Scheme from Isogenies*
**Jiawei Chen, Hyungrok Jo, Shingo Sato and Junji Shikata**

10:55-11:20
*SPDH-Sign: towards Efficient, Post-quantum, Group-based Signatures*
**Christopher Battarbee, Delaram Kahrobaei, Ludovic Perret and Siamak F. Shahandashti**

11:20-11:45
*DME: a full encryption, signature and KEM multivariate public key cryptosystem*
**Ignacio Luengo, Martín Avendaño and Pilar Coscojuela**

11:45-12:10
*Wave Parameter Selection*
**Nicolas Sendrier:**

12:10-13:45
**Lunch Break**

## Session II: Theory

13:45-15:25 **Chair: Jintai Ding**

13:45-14:10
*Fast Enumeration Algorithm For Multivariate Polynomials Over General Finite Fields*
**Hiroki Furue and Tsuyoshi Takagi**

14:10-14:35
*On the Hardness of Scheme-Switching Between SIMD FHE Schemes*
**Karim Eldefrawy, Nicholas Genise and Nathan Manohar**

14:35-15:00
*NTRU in Quaternion Algebras of Bounded Discriminant*
**Cong Ling and Andrew Mendelsohn**

15:00-15:25
*NTWE: A Natural Combination of NTRU and LWE*
**Joel Gärtner**

15:25-15:55
**Break**

## Session III: Quantum I

15:55-17:10 **Chair: Rainer Steinwandt**

15:55-16:20
*Classical and quantum 3 and 4-sieves to solve SVP with low memory*
**André Chailloux and Johanna Loyer**

16:20-16:45
*Time and Query Complexity Tradeoffs for the Dihedral Coset Problem*
**Maxime Remaud, André Schrottenloher and Jean-Pierre Tillich**

16:45-17:10
*Non-Observable Quantum Random Oracle Model*
**Navid Alamati, Varun Maram and Daniel Masny**

17:10—
**Evening activities organized by attendees**

# Thursday, August 17th

8:30-9:00
**Registration**

## Invited Presentation
9:00-10:00 **Chair: Maxime Bros**

*Post-Quantum Signatures from Multiparty Computation: Recent Advances*
**Thibauld Feneuil**

10:00-10:30
**Break**

## Session IV: Quantum II
10:30-11:45 **Chair: Daniel Apon**

10:30-10:55
*Breaking the Quadratic Barrier: Quantum Cryptanalysis of Milenage, Telecommunications' Cryptographic Backbone*
**Vincent Quentin Ulitzsch and Jean-Pierre Seifert**

10:55-11:20
*Characterizing the qIND-qCPA (In)security of the CBC, CFB, OFB and CTR Modes of Operation*
**Tristan Nemoz, Zoé Amblard and Aurélien Dupin**

11:20-11:45
*On the Quantum Security of HAWK*
**Serge Fehr and Yu-Hsuan Huang**

11:45-13:30
**Lunch Break**

## Invited Presentation
13:30-14:30 **Chair: Ray Perlner**

*PQC at Google*
**Sophie Schmieg**

## Session V: Post-Quantum Protocols

14:30-15:45 **Chair: Scott Fluhrer**

14:30-14:55
*Post-Quantum Signatures in DNSSEC via Request-Based Fragmentation*
**Jason Goertzen and Douglas Stebila**

14:55-15:20
*Hash-based Direct Anonymous Attestation*
**Liqun Chen, Changyu Dong, Nada El Kassem, Christopher J.P. Newton and Yalan Wang**

15:20-15:45
*Muckle+: End-to-End Hybrid Authenticated Key Exchanges*
**Sonja Bruckner, Sebastian Ramacher and Christoph Striecks**

15:45-16:15
**Break**

## Session VI: Cryptanalysis

16:15-17:55 **Chair: Nicolas Sendrier**

16:15-16:40
*An extension of Overbeck's attack with an application to cryptanalysis of Twisted Gabidulin-based schemes*
**Alain Couvreur and Ilaria Zappatore**

16:40-17:05
*Cryptanalysis of rank-metric schemes based on distorted Gabidulin codes*
**Pierre Briaud and Pierre Loidreau**

17:05-17:30
*Do not bound to a single position: near-optimal multi-positional mismatch attacks against Syber and Saber*
**Qian Guo and Erik Mårtensson**

17:30-17:55
*New NTRU Records with Improved Lattice Bases*
**Elena Kirshanova, Alexander May and Julian Nowakowski**

18:00—
**Conference Banquet and Rump Session**

# Friday, August 18th

## Invited Presentation

9:00-10:00 **Chair: Thomas Johansson**

*New algebraic attacks on the McEliece cryptosystem*
**Jean-Pierre Tillich**

10:00-10:30
**Break**

## Hardware and Side Channels

10:30-12:10 **Chair: Dustin Moody**

10:30-10:55
*A High-Performance Hardware Implementation of the LESS Digital Signature Scheme*
**Luke Beckwith, Robert Wallace, Kamyar Mohajerani and Kris Gaj**

10:55-11:20
*WrapQ: Side-Channel Secure Key Management for Post-Quantum Cryptography*
**Markku-Juhani O. Saarinen**

11:20-11:45
*Breaking and Protecting the Crystal: Side-Channel Analysis of Dilithium in Hardware*
**Hauke Steffen, Georg Land, Lucie Kogelheide and Tim Güneysu**

11:45-12:10
*Faulting Winternitz One-Time Signatures to forge LMS, XMSS, or SPHINCS+ signatures*
**Alexander Wagner, Vera Wesselkamp, Felix Oberhansl, Marc Schink and Emanuele Strieder**

12:10-12:15
**Closing Remarks**