14th International Conference on Post-Quantum Cryptography

PQCrypto 2023

University of Maryland, College Park, MD, USA, August 16–18, 2023

https://pqcrypto2023.umiacs.io/

ANNOUNCEMENT AND CALL FOR PAPERS

The aim of PQCrypto is to serve as a forum for researchers to present results and exchange ideas on cryptography in an era with large-scale quantum computers. Original research papers on all technical aspects of cryptographic research related to post-quantum cryptography are solicited. Topics of interest include (but are not restricted to):

- Cryptanalysis of post-quantum systems, and quantum cryptanalysis.
- Cryptosystems that have the potential to be safe against quantum computers such as: code-based, hash-based, isogeny-based, lattice-based, and multivariate constructions.
- Implementations of, and side-channel attacks on, post-quantum cryptosystems.
- Security models for the post-quantum era.

Instructions to authors.

Accepted papers are planned to be published in Springer's LNCS series. Submissions must not exceed 30 pages, including appendices and excluding references, and must be in a single column format in 10pt fonts using the default llncs class without adjustments. Reviewers are not required to read appendices, and submissions are expected to be intelligible and complete without them.

If the submission is accepted, the length of the final version is at most 35 pages including both references and appendices, in the llncs class format. Submissions must not substantially duplicate work that any of the authors has published in a journal or a conference/workshop with proceedings, or has submitted/is planning to submit before the author notification deadline to a journal or other conferences/workshops that have proceedings. The submission should begin with a title, the authors' names and affiliations, a short abstract, and a list of key words. Its introduction should summarize the contributions of the paper at a level appropriate for a non-specialist reader. Submissions ignoring these guidelines may be rejected without further consideration.

Important dates:

- **Initial submission deadline: April 17th, 2023**
- **Final submission deadline: April 24th, 2023**
- **Notification of acceptance: June 5th, 2023**
- **Final version: June 23rd, 2023**

General chair:

- Yi-Kai Liu, NIST (USA)

Program chairs:

- Daniel Smith-Tone, NIST (USA)
- Thomas Johansson, Lund University (SE)

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
- Andreas Hülsing, Eindhoven U. Techonology, Netherlands
- David Jao, U. Waterloo, Canada
- Thomas Johansson, Lund U., Sweden (chair)
- John Kelsey, NIST, USA, KU Leuven, Belgium
- Howon Kim, Pusan National U., Korea
- Jon-Lark Kim, Sogang U., Korea
- Kwangjo Kim, KAIST, Korea
- Elena Kirshanova, Technology Innovation Inst., UAE
- Tanja Lange, Eindhoven U. Techonology, Netherlands
- Changmin Lee, KIAS, 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., 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, U. Rennes, CNRS, IRISA
- Yu Yu, Shanghai Jiao Tong U.
- Aaram Yun, Ewha Womans U., Korea