13th International Conference on Post-Quantum Cryptography

PQCrypto 2022

Virtual event, September 28–30, 2022

https://2022.pqcrypto.org/

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 20 pages, including references and excluding appendices, 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 20 pages including references and at most an additional 10 pages for 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, and 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: May 10, 2022**
- **Final submission deadline: May 24, 2022**
- **Notification of acceptance: July 13, 2022**
- **Final version: July 27, 2022**

General chair:

- Tanja Lange, Eindhoven University of Technology, Netherlands & Academia Sinica, Taiwan

Program chairs:

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

Program committee:

- Magali Bardet, U. of Rouen Normandie, France
- Daniel J. Bernstein, U. Illinois at Chicago, USA, & Ruhr U. Bochum, Germany, & Academia Sinica, Taiwan
- Olivier Blazy, École Polytechnique, France
- André Chailloux, INRIA Paris, France
- Anupam Chattopadhyay, NTU Singapore, Singapore
- Chen-Mou Cheng, Kanazawa U., Japan
- Jung Hee Cheon, Seoul National U., Korea (chair)
- Jan-Pieter D'Anvers, KU Leuven, Belgium
- Leo Ducas, CWI, Netherlands
- Scott Fluhrer, Cisco Systems, USA
- Philippe Gaborit, U. Limoges, France
- Tommaso Gagliardoni, Kudelski Security, Switzerland
- Steven Galbraith, Auckland U., New Zealand
- Qian Guo, Lund U., Sweden
- Tim Güneysu, Ruhr U. Bochum & DFKI, Germany
- Dong-Guk Han, Kookmin U., Korea
- David Jao, U. Waterloo, Canada
- Thomas Johansson, Lund U., Sweden (chair)
- Howon Kim, Pusan National U., Korea
- Jon-Lark Kim, Sogang U., Korea
- Kwangjo Kim, KAIST, Korea
- Elena Kirshanova, Kant Baltic Federal U., Russia, & TII, UAE
- Tanja Lange, Eindhoven U. Techonology, Netherlands, & Academia Sinica, Taiwan
- Changmin Lee, KIAS, Korea
- Christian Majenz, Technical U. Denmark, Denmark
- Alexander May, Ruhr U. Bochum, Germany
- Rafael Misoczki, Google, USA
- Michele Mosca, U. Waterloo & Perimeter Inst., Canada
- Ray Perlner, NIST, USA
- Christophe Petit, U. libre de Bruxelles, Belgium
- Rachel Player, Royal Holloway, U. London, UK
- Thomas Prest, PQShield Ltd., UK
- Thomas Pöppelman, Infineon, Germany
- Nicolas Sendrier, Inria, France
- Jae Hong Seo, Hanyang U., Seoul, Korea
- Benjamin Smith, INRIA, France
- Daniel Smith-Tone, U. Louisville & NIST, USA
- Yongsoo Song, Seoul National U., Korea
- Damien Stehlé, ENS Lyon, France
- Rainer Steinwandt, U. Alabama at Huntsville, USA
- Tsuyoshi Takagi, U. of Tokyo, Japan

- Jean-Pierre Tillich, Inria, France
- Keita Xagawa, NTT, Japan
- Aaram Yun, Ewha Womans U., Korea
- Zhenfei Zhang, Etherium Foundation, USA