PQCrypto 2024

15th International Conference on Post-Quantum Cryptography

June 12-14, 2024 – Mathematical Institute, University of Oxford, UK.

`https://www.maths.ox.ac.uk/events/conferences/pqcrypto-2024`

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:	January 19, 2024
- Final submission deadline:	January 26, 2024
- Notification of acceptance:	March 15, 2024
- Final version due:	March 29, 2024

General chairs:

- Federico Pintore (University of Trento)
- Ali El Kaafarani (PQShield and U. of Oxford)

Program chairs:

- Markku-Juhani O. Saarinen (Tampere University and PQShield)
- Daniel Smith-Tone (U. of Louisville and NIST)

Paper submission page: `https://easychair.org/conferences/?conf=pqcrypto2024`

Program Committee

Magali Bardet (University of Rouen Normandie)
Daniel J. Bernstein (UIC, RUB, and Academica Sinica)
Ward Beullens (IBM)
Olivier Blazy (Ecole Polytechnique)
Katharina Boudgoust (Aarhus University)
Daniel Cabarcas (UNAL-Sede Medellín)
Ryann Cartor (Clemson University)
Sanjit Chatterjee (Indian Institute of Science)
Anupam Chattopadhyay (Nanyang Technological University)
Chen-Mou Cheng (BTQ Technologies Corp)
Jung Hee Cheon (Seoul National University)
Thomas Decru (Katholieke Universiteit Leuven)
Martin Ekerå (KTH and Swedish NCSA)
Thibauld Feneuil (CryptoExperts)
Scott Fluhrer (Cisco Systems)
Philippe Gaborit (University of Limoges)
Tommaso Gagliardoni (Kudelski Security)
Qian Guo (Lund University)
Michael Hamburg (Rambus)
David Jao (University of Waterloo)
Thomas Johansson (Lund University)
Shuichi Katsumata (PQShield and AIST)
John Kelsey (NIST)
Jon-Lark Kim (Sogang University)
Elena Kirshanova (TII)
Dustin Moody (NIST)
Ray Perlner (NIST)
Edoardo Persichetti (FAU and Sapienza University)
Thomas Pöppelmann (Infineon)
Thomas Prest (PQShield)
Angela Robinson (NIST)
Mélissa Rossi (ANSSI)
Palash Sarkar (Indian Statistical Institute)
Nicolas Sendrier (INRIA)
Benjamin Smith (INRIA)
Damien Stehlé (ENS Lyon)
Rainer Steinwandt (UAH)
Tsuyoshi Takagi (University of Tokyo)
Atsushi Takayasu (University of Tokyo)
Jean-Pierre Tillich (INRIA)
Yu Yu (Shanghai Jiao Tong University)
Yang Yu (Univ. Rennes, CNRS, IRISA)
Aaram Yun (Ewha Womans University)
Rina Zeitoun (IDEMIA)