Eleventh International Conference on Post-Quantum Cryptography

PQCrypto 2020

Paris, France, April 15–17, 2020

https://pqcrypto2020.inria.fr

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):

- Cryptosystems that have the potential to be safe against quantum computers such as: code-based, hash-based, isogeny-based, lattice-based, and multivariate constructions.
- Cryptanalysis of post-quantum systems, and quantum cryptanalysis.
- 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 12 pages, excluding references and appendices in a single column format in 10pt fonts using the default llncs class without adjustments.

If the submission is accepted, the length of the final version will be at most 20 pages including 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, 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: Nov 26, 2019**
- **Final submission deadline: Dec 3, 2019**
- **Notification about acceptance: Jan 20, 2020**
- **Final version: Feb 3, 2020**

General chairs :

- Antoine Joux, Sorbonne U. (FR)
- Nicolas Sendrier, Inria (FR)

Program chairs:

- Jintai Ding, U. of Cincinnati (US)
- Jean-Pierre Tillich, Inria (FR)

Program committee:

- Reza Azarderakhsh, Florida Atlantic U. & PQSecure Technologies (US)
- Jean-Philippe Aumasson, Teserakt AG (CH)
- Yoshinori Aono, NICT (JP)
- Magali Bardet, U. of Rouen (FR)
- Daniel J. Bernstein, U. Illinois at Chicago (US) & Ruhr-U. Bochum (DE)
- Olivier Blazy, U. of Limoges (FR)
- André Chailloux, Inria (FR)
- Chen-Mou Cheng, Osaka U. & Kanazawa U. (JP)
- Jung Hee Cheon, Seoul National U. (KR)
- Tung Chou, Osaka U. (JP) & Academia Sinica (TW)
- Dung Duong, U. of Wollongong (AU)
- Scott Fluhrer, Cisco Systems (US)
- Philippe Gaborit, U. of Limoges (FR)
- Tommaso Gagliardoni, Kudelski Security (CH)
- Steven Galbraith, U. of Auckland (NZ)
- Xiao-Shan Gao, Chinese Academy of Sciences (CN)
- Tim Güneysu, Ruhr-U. of Bochum & DFKI (DE)
- David Jao, U. of Waterloo & evolutionQ (CA)
- Jiwu Jing, U. of Chinese Academy of Sciences (CN)
- Thomas Johansson, Lund U. (SE)
- Antoine Joux, Sorbonne U. (FR)
- Kwangjo Kim, KAIST (KR)
- Elena Kirshanova, I.Kant Baltic Federal U. (RU)
- Yi-Kai Liu, NIST & U. of Maryland (US)
- Prabhat Mishra, U. of Forida (US)
- Michele Mosca, Waterloo U. & Perimeter Inst. (CA)
- María Naya-Plasencia, Inria (FR)
- Khoa Nguyen, Nanyang Technological U. (SG)
- Ruben Niederhagen, Fraunhofer SIT (DE)
- Ray Perlner, NIST (DE)
- Christophe Petit, U. of Birmingham (UK)
- Rachel Player, U. of London (UK)
- Thomas Pöppelmann, Infineon Technologies (DE)
- Thomas Prest, PQShield (UK)
- Nicolas Sendrier, Inria (FR)
- Junji Shikata, Yokohama National U. (JP)
- Daniel Smith-Tone, NIST & U. of Louisville (US)
- Rainer Steinwandt, Florida Atlantic U. (US)
- Damien Stehlé, ENS de Lyon (FR)
- Tsuyoshi Takagi, U. of Tokyo (JP)
- Routo Terada, U. of São Paulo (BR)
- Serge Vaudenay, EPFL (CH)
- Keita Xagawa, NTT Secure Platform Laboratories (JP)
- Bo-Yin Yang, Academia Sinica (TW)
- Zhenfeng Zhang, Inst. of Software & Chinese Academy of Sciences (CN)