Tenth International Conference on Post-Quantum Cryptography

PQCrypto 2019

Chongqing, China, May 8–10, 2019

pqcrypto2019.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. PQCrypto 2019 will be preceded by a Summer School (May 6–7, 2019) at Chongqing University. Original 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.
- Implementations of, and side-channel attacks on, post-quantum cryptosystems.
- Security models for the post-quantum era.

Instructions for authors. Accepted papers will 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. Final versions of accepted papers will be limited to 20 pages. 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. Submissions should begin with a title, the authors' names and affiliations, a short abstract, and a list of keywords. Submissions ignoring these guidelines may be rejected without further consideration.

Submission deadlines. All papers must be registered with title and abstract at the initial submission deadline (Nov 24, 2018). Authors may continue to revise their submissions until the final submission deadline (Dec 1, 2018). Between the deadlines, PC members will have access to the title and abstract of the papers, but not to the PDF files. The abstract should summarize the contributions of the paper at a level appropriate for a non-specialist reader.

Important dates:

- **Initial submission deadline: Nov 24, 2018**
- **Final submission deadline: Dec 1, 2018**
- **Notification of acceptance: Jan 12, 2019**
- **Final version: Jan 26, 2019**

General chair:

- Xiang Hong (Chongqing U.)

Program chairs:

- Jintai Ding (U. Cincinnati)
- Rainer Steinwandt (Florida Atlantic U.)

Program committee:

- Gorjan Alagic (U. of Maryland & NIST)
- Martin R. Albrecht (U. of London)
- Yoshinori Aono (NICT)
- John B. Baena (U. Nacional de Colombia)
- Shi Bai (Florida Atlantic U.)
- Lejla Batina (Radboud U.)
- Daniel J. Bernstein (U. of Illinois at Chicago)
- Johannes Buchmann (TU Darmstadt)
- Chen-Mou Cheng (Osaka U.)
- Jung Hee Cheon (Seoul National U.)
- Thomas Eisenbarth (U. zu Lübeck & WPI)
- Ali El Kaafarani (U. of Oxford)
- Scott Fluhrer (Cisco Systems)
- Philippe Gaborit (U. Limoges)
- Tommaso Gagliardoni (IBM Research)
- Kris Gaj (George Mason U.)
- María I. González Vasco (U. Rey Juan Carlos)
- Tim Güneysu (Ruhr-U. Bochum & DFKI)
- Sean Hallgren (Pennsylvania State U.)
- David Jao (U. Waterloo & evolutionQ, Inc.)
- Jiwu Jing (Chinese Academy of Sciences)
- Thomas Johansson (Lund U.)
- Antoine Joux (Institut de Mathématique de Jussieu)
- Kwangjo Kim (KAIST)
- Stefan Kölbl (Cybercrypt)
- Brad Lackey (U. of Maryland)
- Kristin Lauter (Microsoft Research)
- Yi-Kai Liu (NIST & U. of Maryland)
- Vadim Lyubashevsky (IBM Research – Zürich)
- Michele Mosca (U. Waterloo & Perimeter Inst.)
- María Naya-Plasencia (Inria)
- Ruben Niederhagen (Fraunhofer SIT)
- Ray Perlner (NIST)
- Ludovic Perret (Post-Quantum Advanced Technologies & Sorbonne U.)
- Edoardo Persichetti (Florida Atlantic U.)
- Albrecht Petzoldt (U. of Versailles)
- Thomas Pöppelmann (Infineon Technologies)
- Martin Roetteler (Microsoft Research)
- Alexander Russell (U. of Connecticut)
- Nicolas Sendrier (Inria)
- Junji Shikata (Yokohama National U.)
- Daniel Smith-Tone (NIST & U. of Louisville)
- Fang Song (Portland State U.)
- Jakub Szefer (Yale)
- Damien Stehlé (ENS de Lyon)
- Tsuyoshi Takagi (U. of Tokyo)
- Katsuyuki Takashima (Mitsubishi Electric)
- Jean-Pierre Tillich (Inria)
- Keita Xagawa (NTT)
- Bo-Yin Yang (Academia Sinica)
- Shengyu Zhang (Tencent & The Chinese U. of Hong Kong)
- Zhenfeng Zhang (Chinese Academy of Sciences)