Twelfth International Conference on Post-Quantum Cryptography

PQCrypto 2021

Daejeon, Korea, July 20–22, 2021

https://pqcrypto2021.kr

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.
Please submit your paper via EasyChair.
For more detail, please refer to "instructions for authors" linked at the PQCrypt 2021 website.

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 (everywhere):
- **Submission deadline : ~~Feb 24~~ Mar 10, 2021 (at least title and abstract)**
- **Update deadline: ~~Mar 3~~ Mar 17, 2021**
- **Notification about acceptance: ~~April 21~~ May 5, 2021**
- **Final version: ~~May 5~~ May 19, 2021**

General chairs :
- Dooho Choi, ETRI (KR)
- Kwangjo Kim, KAIST (KR)

Program chairs:
- Jung Hee Cheon, Seoul National University (KR)
- Jean-Pierre Tillich, Inria (FR)

Program committee:
- Magali Bardet, University of Rouen Normandie & INRIA (FR)
- Daniel J. Bernstein, University of Illinois at Chicago (US) & Ruhr-Universität Bochum (DE)
- Olivier Blazy, Université de Limoges (FR)
- Andre Chailloux, INRIA(FR)
- Chen-Mou Cheng, Kanazawa University (JP)
- Jintai Ding, University of Cincinnati (US)
- Léo Ducas, CWI (NL)
- Scott Fluhrer, Cisco Systems (US)
- Philippe Gaborit, XLIM- Université de Limoges (FR)
- Tommaso Gagliardoni, Kudelski Security (CH)
- Steven Galbraith, University of Auckland (NZ)
- Tim Güneysu, Ruhr-Universität Bochum (DE)
- Dong-Guk Han, Kookmin University (KR)
- David Jao, University of Waterloo (US)
- Thomas Johansson, Dept. of Electrical and Information Technology, Lund University (SE)
- Howon Kim, Pusan National University (KR)
- Jon-Lark Kim, Sogang University (KR)
- Kwangjo Kim, KAIST (KR)
- Elena Kirshanova, I.Kant Baltic Federal University(RU)
- Tanja Lange, Eindhoven University of Technology (NL)
- Changmin Lee, KIAS (KR)
- Christian Majenz, QuSoft and CWI, Amsterdam(NL)
- Alexander May, Ruhr-Universität Bochum (DE)
- Rafael Misoczki, Google (US)
- Michele Mosca, University of Waterloo (US)
- Khoa Nguyen, Nanyang Technological University (SG)
- Ray Perlner, NIST (US)
- Christophe Petit, Université libre de Bruxelles (BE)
- Rachel Player, Royal Holloway, University of London (UK)
- Thomas Pöppelmann, Infineon Technologies AG(DE)
- Thomas Prest, Oxford & PQShield (UK)
- Nicolas Sendrier, INRIA (FR)
- Jae Hong Seo, Hanyang University (KR)
- Benjamin Smith, Inria, École polytechnique (FR)
- Daniel Smith-Tone, NIST (US)
- Yongsoo Song, KAIST (KR)
- Damien Stehlé, ENS Lyon (FR)
- Rainer Steinwandt, University of Alabama in Huntsville (US)
- Tsuyoshi Takagi, University of Tokyo (JP)
- Keita Xagawa, NTT (JP)
- Aaram Yun, Ewha Womans University (KR)
- Zhenfei Zhang, Algorand(US)