Eighth International Conference on Post-Quantum Cryptography

PQCrypto 2017

Utrecht, The Netherlands, June 26–28, 2017

https://2017.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 the topic of cryptography in an era with large-scale quantum computers. The conference will be preceded by a summer school on June 19–23, 2017 and an executive school on June 22–23, 2017.

Original research papers on all technical aspects of cryptographic research related to post-quantum cryptography are solicited. The topics include (but are not restricted to):

- Cryptosystems that have the potential to be safe against quantum computers such as: code-based cryptosystems, hash-based signature schemes, isogeny-based cryptosystems, lattice-based cryptosystems, and multivariate cryptosystems.
- 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 will be published in Springer's LNCS series. The length of the submission must be at most 12 pages, excluding references and appendices, in a single column format, in 10pt fonts using the default llncs class without any adjustments to margins, fonts, or other. 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.

Best paper award: The Program Committee may select one outstanding paper for the best paper award.

Submission deadlines: The initial submission deadline is February 14, 2017. Papers submitted by this deadline may be in draft form but must include a title and an abstract. The final submission deadline is February 21, 2017. Authors who submitted a paper by the February 14 deadline will be permitted to revise their papers anytime before the final submission deadline.

Important dates:

- **Initial submission deadline: February 14, 2017**
- **Final submission deadline: February 21, 2017**
- **Notification deadline: April 10, 2017**
- **Final version: April 19, 2017**

Program chairs:

- Tanja Lange, TU Eindhoven, Netherlands
- Tsuyoshi Takagi, Kyushu U., Japan

Program committee:

- Martin Albrecht, Royal Holloway, U. London, UK
- Daniel J. Bernstein, U. Illinois at Chicago, USA, & TU Eindhoven, Netherlands
- Joppe Bos, NXP Semiconductors, Belgium
- Johannes Buchmann, TU Darmstadt, Germany
- Wouter Castryck, KU Leuven, Belgium
- Chen-Mou Cheng, Osaka U., Japan
- Pierre-Louis Cayrel, Jean Monnet U., France
- Claude Crépeau, McGill University, Canada
- Jintai Ding, U. Cincinnati, USA
- Philippe Gaborit, U. Limoges, France
- Steven Galbraith, Auckland U., New Zealand
- Tim Güneysu, U. of Bremen & DFKI, Germany
- Sean Hallgren, Pennsylvania State U., USA
- Yasufumi Hashimoto, U. Ryukyu, Japan
- Andreas Hülsing, TU Eindhoven, Netherlands
- David Jao, U. Waterloo, Canada
- Stacey Jeffery, CWI, Netherlands
- Thomas Johansson, Lund U., Sweden
- Tancrède Lepoint, SRI International, USA
- Yi-Kai Liu, NIST, USA
- Frédéric Magniez, CNRS, France
- Michele Mosca, U. Waterloo & Perimeter Inst., Canada
- Michael Naehrig, Microsoft Research, USA
- María Naya-Plasencia, Inria, France
- Ruben Niederhagen, Fraunhofer SIT, Germany
- Christian Rechberger, U. Graz, Austria
- Martin Rötteler, Microsoft Research, USA
- Simona Samardjiska, Ss. Cyril and Methodius U., Macedonia & Radboud U., Netherlands
- Peter Schwabe, Radboud U., Netherlands
- Nicolas Sendrier, Inria, France
- Daniel Smith-Tone, U. Louisville & NIST, USA
- Fang Song, Portland State U.
- Damien Stehlé, ENS Lyon, France
- Rainer Steinwandt, Florida Atlantic U., USA
- Krysta Svore, Microsoft Research, USA
- Jean-Pierre Tillich, Inria, France
- Ronald de Wolf, CWI & U. Amsterdam, Netherlands
- Keita Xagawa, NTT, Japan
- Bo-Yin Yang, Academia Sinica, Taiwan