Seventh International Conference on Post-Quantum Cryptography

PQCrypto 2016

Fukuoka, Japan, February 24–26, 2016

https://pqcrypto2016.jp/

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 winter school on February 22–23, 2016.

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: hash-based signature schemes, lattice-based cryptosystems, code-based cryptosystems, multivariate cryptosystems and quantum cryptographic schemes;
- Classical and quantum attacks including 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 11pt fonts and with reasonable margins. 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 October 7, 2015. Papers submitted by this deadline may be in draft form but must include a title and an abstract. The final submission deadline is October 14. Authors who submitted a paper by the October 7 deadline will be permitted to revise their papers anytime before the final submission deadline.

Important dates:

- **Initial submission deadline: October 7, 2015**
- **Final submission deadline: October 14, 2015**
- **Notification deadline: November 20, 2015**
- **Final version: December 2, 2015**

General chair:

- Kouichi Sakurai, Kyushu U. & ISIT, Japan

General co-chairs:

- Takanori Yasuda, ISIT, Japan
- Kirill Morozov, Kyushu U., Japan

Program chair:

- Tsuyoshi Takagi, Kyushu U., Japan

Program committee:

- Joppe Bos, NXP Semiconductors, Belgium
- Johannes Buchmann, TU Darmstadt, Germany
- Chen-Mou Cheng, National Taiwan U., Taiwan
- Pierre-Louis Cayrel, Jean Monnet U., France
- Claude Crépeau, McGill University, Canada
- Jintai Ding, U. Cincinnati, USA
- Philippe Gaborit, U. Limoges, France
- Danilo Gligoroski, Norwegian U. Sci. Tech., Norway
- Tim Güneysu, Ruhr U. Bochum, Germany
- Sean Hallgren, Pennsylvania State U., USA
- Yasufumi Hashimoto, U. Ryukyu, Japan
- David Jao, U. Waterloo, Canada
- Tanja Lange, TU Eindhoven, Netherlands
- Yi-Kai Liu, NIST, USA
- Michele Mosca, U. Waterloo & Perimeter Inst., Canada
- Martin Rötteler, Microsoft Research, USA
- Nicolas Sendrier, Inria, France
- Daniel Smith-Tone, U. Louisville & NIST, USA
- Damien Stehlé, ENS Lyon, France
- Rainer Steinwandt, Florida Atlantic U., USA
- Jean-Pierre Tillich, Inria, France
- Keita Xagawa, NTT, Japan
- Bo-Yin Yang, Academia Sinica, Taiwan
- Zhengfeng Zhang, Chinese Academy of Sciences, China