Ninth International Conference on Post-Quantum Cryptography

PQCrypto 2018

Fort Lauderdale, FL, USA, April 9–11, 2018

`http://www.math.fau.edu/pqcrypto2018/`

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 2018 will be co-located with NIST's First PQC Standardization Conference (April 12–13, 2018) in Fort Lauderdale, FL. 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 20 pages, including references and appendices in a single column format in 10pt fonts using the default llncs class without any adjustments. 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.

Best paper award. The program committee may select one outstanding paper for the best paper award.

Submission deadlines. All papers must be submitted by the initial submission deadline (Nov 18, 2017). Authors may continue to revise their submissions until the final submission deadline (Nov 25, 2017). 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 18, 2017**
- **Final submission deadline: Nov 25, 2017**
- **Notification about acceptance: Jan 10, 2018**
- **Final version: Jan 24, 2018**

Program chairs:

- Tanja Lange, Technische U. Eindhoven, NL
- Rainer Steinwandt, Florida Atlantic U., US

Program committee:

- Gorjan Alagic (U. of Maryland, US)
- Shi Bai (Florida Atlantic U., US)
- Lejla Batina (Radboud U., NL)
- Daniel J. Bernstein (U. of Illinois at Chicago, US)
- Joppe W. Bos (NXP Semiconductors, BE)
- Johannes Buchmann (TU Darmstadt, DE)
- Wouter Castryck (KU Leuven, BE)
- Pierre-Louis Cayrel (U. Jean Monnet St-Etienne, FR)
- Chen-Mou Cheng (Osaka U., JP)
- Jung Hee Cheon (Seoul National U., KR)
- Andrew Childs (U. of Maryland, US)
- Jintai Ding (U. Cincinnati, US)
- Thomas Eisenbarth (U. zu Lübeck, DE & WPI, US)
- Scott Fluhrer (Cisco Systems, US)
- Philippe Gaborit (U. Limoges, FR)
- Tommaso Gagliardoni (IBM Research, CH)
- Kris Gaj (George Mason U., US)
- Steven Galbraith (U. of Auckland, NZ)
- Tim Güneysu (Ruhr-U. Bochum & DFKI, DE)
- Sean Hallgren (Pennsylvania State U., US)
- Yasufumi Hashimoto (U. of the Ryukyus, JP)
- Andreas Hülsing (Technische U. Eindhoven, NL)
- David Jao (U. Waterloo & evolutionQ, Inc., CA)
- Stacey Jeffery (CWI, QuSoft, NL)
- Thomas Johansson (Lund U., SE)
- Kwangjo Kim (KAIST, KR)
- Stefan Kölbl (Technical U. of Denmark, DK)
- Tancrède Lepoint (SRI International, US)
- Yi-Kai Liu (NIST & U. of Maryland, US)
- Michele Mosca (U. Waterloo & Perimeter Inst., CA)
- Michael Naehrig (Microsoft Research, US)
- María Naya-Plasencia (INRIA, FR)
- Ruben Niederhagen (Fraunhofer SIT, DE)
- Edoardo Persichetti (Florida Atlantic U., US)
- Thomas Pöppelmann (Infineon Technologies, DE)
- Christian Rechberger (TU Graz, AT)
- Martin Roetteler (Microsoft Research, US)
- Alexander Russell (U. of Connecticut, US)
- Simona Samardjiska (Radboud U., NL & UKIM, MK)
- Peter Schwabe (Radboud U., NL)
- Nicolas Sendrier (INRIA, FR)
- Daniel Smith-Tone (NIST & U. of Louisville, US)
- Fang Song (Portland State U., US)
- Douglas Stebila (McMaster U., CA)
- Damien Stehlé (ENS de Lyon, FR)
- Krysta Svore (Microsoft Research, US)
- Tsuyoshi Takagi (Kyushu U. & U. of Tokyo, JP)
- Jean-Pierre Tillich (INRIA, FR)
- Christine van Vredendaal (Technische U. Eindhoven, NL)
- William Whyte (OnBoard Security, US)
- Keita Xagawa (NTT, JP)
- Bo-Yin Yang (Academia Sinica, TW)
- Zhang Zhenfeng (Chinese Academy of Sciences, CN)