Fifth International Workshop on Post-Quantum Cryptography

PQCrypto 2013

Limoges, France, June 4–7, 2013

http://pqcrypto2013.xlim.fr/

ANNOUNCEMENT AND CALL FOR PAPERS

PQCrypto's aim is to serve as a forum for researchers to present results and exchange ideas in post-quantum cryptography.

Original research papers on all technical aspects of cryptographic research related to the future world with large quantum computers are solicited. The topics include (but are not restricted to):

- Cryptosystems that have the potential to resist possible future quantum computers such as: hash-based Merkle-type signature schemes, lattice-based cryptosystems, code-based cryptosystems, multivariate cryptosystems and quantum cryptographic schemes;
- Classical and quantum attacks including side-channel attacks on the post-quantum cryptosystems;
- Security models for the post-quantum era.

Instructions to authors.

Accepted papers will be published in the LNCS series of Springer. The paper should be at most 12 pages excluding the bibliography and appendices, and at most 20 pages total using at least 11-point font and reasonable margins. The authors are encouraged to prepare their submission in LaTeX following Springer's guidelines.

Submissions must not substantially duplicate work that any of the authors has published elsewhere or has submitted in parallel to any other conference or workshop with formally published proceedings. Accepted submissions may not appear in any other conference or workshop with 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 risk rejection without consideration of their merits.

Important dates:

- **Submission by January 25, 2013**
- **Notification by March 13, 2013**
- **Final version by March 24, 2013**

General chair:

- Thierry Berger, U. Limoges, France

Local organization:

- XLIM-University of Limoges

Invited speakers:

- to be announced

Program committee:

- Carlos Aguilar Melchor, U. Limoges, France
- Paulo Barreto, U. São Paulo, Brazil
- Daniel J. Bernstein, U. Illinois at Chicago, USA
- Xavier Boyen, QUT, Australia
- Johannes Buchmann, TU Darmstadt, Germany
- Stanislav Bulygin, TU Darmstadt, Germany
- Claude Crépeau, McGill U., Canada
- Jintai Ding, U. Cincinnati, USA
- Pierre-Alain Fouque, U. Rennes I, France
- Philippe Gaborit, U. Limoges, France (**chair**)
- Tim Guneysu, Rhur U. Bochum, Germany
- Sean Hallgren, U. Pennsylvania , USA
- Kazukuni Kobara, AIST, Japan
- Tanja Lange, TU Eindhoven, Netherlands
- Gregor Leander, Danmarks TU, Denmark
- Michele Mosca, U. Waterloo, Canada
- Bart Preneel, KU Leuven, Belgium
- Michael Schneider, TU Darmstadt, Germany
- Nicolas Sendrier, Inria, France
- Damien Stehlé, ENS Lyon, France
- Jean-Pierre Tillich, Inria, France
- Bo-Yin Yang, Academia Sinica, Taiwan