Third International Workshop on Post-Quantum Cryptography

PQCrypto 2010

Darmstadt, Germany, May 25–28, 2010

http://pqc2010.cased.de/

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):

- (public key) 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 November 22, 2009**
- **Notification by February 1st, 2010**
- **Final version by February 28, 2010**

General chairs:

- Johannes Buchmann, TU Darmstadt, Germany
- Markus Rückert, TU Darmstadt, Germany

Local organization:

- Center for Advanced Security Research Darmstadt (CASED)

Invited speakers:

- Renato Renner, ETHZ, Switzerland
- Oded Regev, Tel Aviv U., Israel

Program committee:

- Nicolas Sendrier, INRIA, France (**chair**)
- Daniel Augot, INRIA, France
- Paulo Barreto, U. São Paulo, Brazil
- Daniel J. Bernstein, U. Illinois at Chicago, USA
- Gilles Brassard, U. Montréal, Canada
- Claude Crépeau, McGill U., Canada
- Erik Dahmen, TU Darmstadt, Germany
- Jintai Ding, U. Cincinnati, USA
- Matthieu Finiasz, ENSTA, France
- Philippe Gaborit, U. Limoges, France
- Gert-Martin Greuel, U. Kaiserslautern, Germany
- Tanja Lange, TU Eindhoven, Netherlands
- Pierre Loidreau, CELAR, France
- Vadim Lyubashevsky, Tel Aviv U., Israel
- Christof Paar, Ruhr-U. Bochum, Germany
- Chris Peikert, Georgia Tech, USA
- Gerhard Schabhüser, BSI, Germany
- Graeme Smith, IBM, USA
- Damien Stehlé, CNRS/U. Sydney/Macquarie U., Australia
- Michael Szydlo, Akamai, USA
- Shigeo Tsujii, Chuo U., Japan
- Ralf-Philipp Weinmann, U. Luxembourg
- Bo-Yin Yang, Academia Sinica, Taiwan