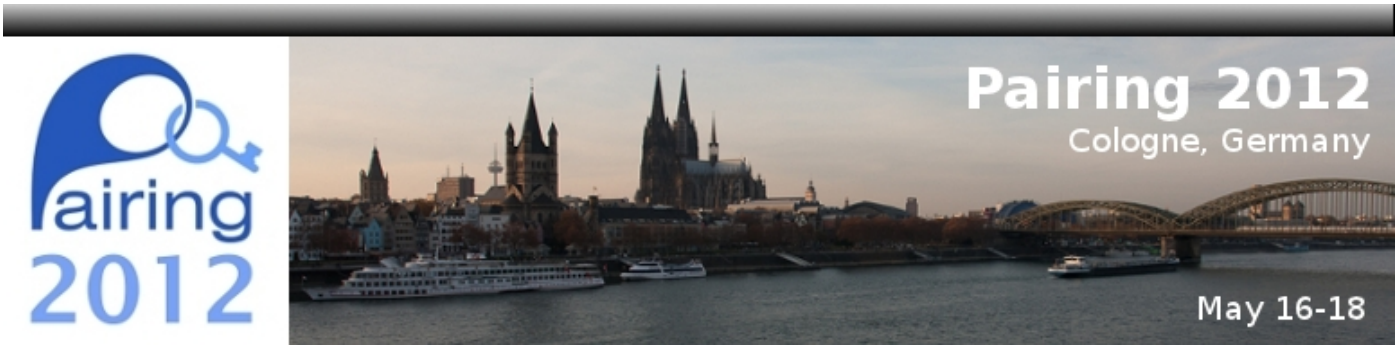

Call for Papers `www.pairing-conference.org/2012`

The 5th International Conference on Pairing-Based Cryptography (Pairing 2012) will be held in Cologne, Germany on May 16-18, 2012; these are Wednesday – Friday before PKC which is held in Darmstadt, Germany. As in previous years, the focus of Pairing 2012 is on all aspects of pairing-based cryptography, including: cryptographic primitives and protocols, mathematical foundations, software and hardware implementation, and applied security.

The first International Conference on Pairing-based Cryptography (Pairing 2007) was held in Tokyo, Japan, followed by conferences in Egham, UK in 2008, Palo Alto, USA in 2009, and Yamanaka Hot Spring, Japan in 2010.

Paper submission deadline:	**February 20, 2012, 23:59 UTC**
Modifications allowed until:	February 24, 2012
Notifications to authors:	April 02, 2012
Final version deadline:	April 20, 2012
Conference:	May 16-18, 2012

The proceedings will be published in Springer's Lecture Notes in Computer Science and will be sent to the participants after the conference.

Instructions for authors

Authors are invited to submit papers describing their original research on all aspects of pairing-based cryptography, including (but not limited to) the topics stated below. Submissions must not substantially duplicate work that any of the authors have published elsewhere or that has been submitted in parallel to any other conference or workshop. Submissions should be anonymous, with no author names, affiliations, acknowledgement or obvious references. Papers should be at most 14 pages, excluding the bibliography and appendices, using at least 11-point fonts and with reasonable margins. Committee members are not required to read appendices; the paper should be intelligible without them. Submitted papers should follow the formatting instructions of the Springer LNCS Style. Please check the Information for LNCS Authors page at Springer (http://www.springer.de/comp/lncs/) for style and formatting guidelines. The final version of accepted papers should be at most 18 pages in standards LNCS style.

At least one author of each accepted paper must register with the conference and present the paper in order to be included in the proceedings.

Topics

Area I: Novel cryptographic protocols

* ID-based and certificateless cryptosystems
* Broadcast encryption, signcryption, etc
* Short / multi / aggregate / group / ring / threshold / blind signatures
* Designed confirmer or undeniable signatures
* Identification / authentication schemes
* Key agreement
* Predicate encryption

Area II: Mathematical foundations

* Efficient pairing variants
* Security consideration of pairings
* Other pairings and applications of pairings in mathematics
* Generation of pairing-friendly curves
* Elliptic and hyperelliptic curves
* Number-theoretic algorithms
* Addition algorithms in divisor groups

Area III: SW / HW implementation

* Secure operating systems
* Efficient software implementation
* FPGA or ASIC implementation
* Smart-card implementation
* RFID security
* Middleware security
* Side-channel and fault attacks

Area IV: Applied security

* Novel security applications
* Secure ubiquitous computing
* Security management
* PKI models
* Application to network security
* Grid computing
* Internet and web security
* E-business or E-commerce security
* Cloud computing
* Mobile and wireless network security
* Application to sensor network security
* Peer-to-peer security

General Chairs

Tanja Lange, Technische Universiteit Eindhoven, Netherlands
Michael Naehrig, Technische Universiteit Eindhoven, Netherlands
Secretarial Support: Anita Klooster-Derks, Technische Universiteit Eindhoven, Netherlands

Program Chairs

Michel Abdalla, ENS Paris, France
Tanja Lange, Technische Universiteit Eindhoven, Netherlands

Program Committee

So far the following people have accepted serving on the PC of Pairing 2012.

Paulo Barreto, University of São Paulo, Brazil
Naomi Benger, University of Adelaide, Australia
Melissa Chase, Microsoft Research, USA
Jérémie Detrey, INRIA, France
Junfeng Fan, K.U.Leuven, Belgium
Dario Fiore, New York University, USA
David Mandell Freeman, Stanford University, USA
Steven Galbraith, University of Auckland, New Zealand
Juan González Nieto, Queensland University of Technology, Australia
Shai Halevi, IBM Research, USA
Antoine Joux, Université de Versailles & DGA, France
Kwangjo Kim, KAIST, Korea
Kristin Lauter, Microsoft Research, USA
Allison B. Lewko, The University of Texas at Austin, USA
Benoît Libert, Université Catholique de Louvain, Belgium
Atsuko Miyaji, Japan Advanced Institute of Science and Technology, Japan
Michael Naehrig, Technische Universiteit Eindhoven, Netherlands
Takeshi Okamoto, University of Tsukuba, Japan
Adam O'Neill, Boston University, USA
Giuseppe Persiano, Università di Salerno, Italy
Christophe Ritzenthaler, IML, France
Francisco Rodríguez-Henríquez, CINVESTAV-IPN, Mexico
Palash Sarkar, Indian Statistical Institute, Kolkata, Inida
Peter Schwabe, Academia Sinica, Taiwan
Mike Scott, Certivox Ltd, Ireland
Tsuyoshi Takagi, Kyushu University, Japan
Katsuyuki Takashima, Mitsubishi Electric, Japan
Edlyn Teske-Wilson, University of Waterloo, Canada
Damien Vergnaud, École Normale Supérieure, France
Jianying Zhou, Institute for Infocomm Research, Singapore