16th IACR International Conference on Practice and Theory in Public Key Cryptography (PKC 2013)

February 26 – March 1, 2013

Nara, Japan

IMPORTANT DATES (Tentative)

Submission	**September 10, 2012, 8:00 UTC (17:00 JST)**
Author notification	November 23, 2012
Camera-ready copy	December 14, 2012

(TCC 2013 will be held in Tokyo, March 3-6.)

GENERAL INFORMATION

Original research papers on all technical aspects of public key cryptography are solicited for submission to PKC 2013, the 16th International Conference on Practice and Theory in Public Key Cryptography.

Papers suggesting novel paradigms, original directions, or non-traditional perspectives are especially welcome.

INSTRUCTIONS FOR AUTHORS

The submission should be at most 12 pages excluding the bibliography and appendices, using reasonable margins and 11pt fonts. The submitted paper should be self-contained and intelligible without appendices, as committee members are not required to read them. Authors are encouraged to prepare their submission following Springer's guidelines.

Submissions must be fully anonymous, with no author names, affiliations, acknowledgments, or obvious references. The submission should begin with a title, a short abstract, and a list of keywords, and the 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. If accepted, one of the authors is expected to present the paper at the conference.

Submissions must not substantially duplicate work that any of the authors has published elsewhere, or has submitted in parallel to any journal or any other conference/workshop with proceedings. Accepted submissions may not appear in any other conference or workshop with proceedings. Submissions violating these rules will be rejected and may entail further consequences. IACR reserves the right to share information about submissions with other program committees to detect parallel submissions and the IACR policy on irregular submissions will be strictly enforced.

VENUE

PKC 2013 will be held at the new public prefectural hall in Nara, Japan. Nara was the capital of Japan in the 8th century. UNESCO listed the historic monuments of ancient Nara as World Heritage in 1998, which encompasses five Buddhist temples, one Shinto shrine, one Palace and one primeval forest. In particular, famous tourist attractions such as Todaiji Temple, Kofukuji Temple and Kasuga Shrine are within walking distance from the venue which is located in the center of Nara National Park. For more information, see

http://en.wikipedia.org/wiki/Historic_Monuments_of_Ancient_Nara
http://www.infomapjapan.com/sight_Nara.phtml

CONFERENCE CHAIRS

Program Chair	
Kaoru Kurosawa	Ibaraki University, Japan
General Chair	
Goichiro Hanaoka	AIST, Japan
Local Organizing co-Chairs	
Takeshi Chikazawa	IPA, Japan
Ryo Nojima	NICT, Japan

PROGRAM COMMITTEE

Nuttapong Attrapadung	AIST, Japan
David Cash	University of California, San Diego, USA
Jean-Sébastien Coron	University of Luxembourg, Luxembourg
Jintai Ding	University of Cincinnati, USA
Stefan Dziembowski	Uniwersytet Warszawski, Poland Università di Roma "La Sapienza", Italy
Marc Fischlin	Technische Universität Darmstadt, Germany
Pierre-Alain Fouque	ENS, France
Steven Galbraith	Auckland University, New Zealand
Rosario Gennaro	City College of New York, USA
Dov Gordon	Applied Communication Sciences, USA
Shai Halevi	IBM Research, USA
Carmit Hazay	Bar-Ilan University, Israel
Tibor Jager	Karlsruhe Institute of Technology, Germany
Antoine Joux	DGA and Université de Versailles Saint-Quentin-en-Yvelines, France
Eike Kiltz	Ruhr-Universität Bochum, Germany
Noboru Kunihiro	The University of Tokyo, Japan
Kaoru Kurosawa (chair)	Ibaraki University, Japan
Allison Lewko	University of Texas, Austin, USA Microsoft Research, USA
Benoît Libert	Technicolor, France
Alexander May	Ruhr-Universität Bochum, Germany
David Naccache	ENS, France
Tatsuaki Okamoto	NTT Labs, Japan
Claudio Orlandi	Aarhus Universitet, Denmark
Chris Peikert	Georgia Institute of Technology, USA
Ludovic Perret	UPMC/INRIA, France
Nigel Smart	University of Bristol, UK
Tsuyoshi Takagi	Kyushu University, Japan
Katsuyuki Takashima	Mitsubishi Electric, Japan
Vinod Vaikuntanathan	Microsoft Research, USA & University of Toronto, Canada
Hoeteck Wee	George Washington University, USA

PKC 2013

The 16th International Conference on Practice and Theory in Public-Key Cryptography