Call for Papers

11th International Workshop on Practice and Theory in Public Key Cryptography (PKC) 2008

March 9-12, 2008

Barcelona, Spain

Important dates:
Submission Deadline: September 7, 2007
Author Notification: November 21, 2007
Camera-Ready Copy: December 14, 2007

Original research papers on all technical aspects of public key cryptography are solicited for submission to PKC 2008, the 11th International Workshop on Practice and Theory in Public Key Cryptography.

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 (November 21, 2007) to other conferences/workshops that have proceedings. Parallel submissions will be rejected from all places they have been submitted to, and further actions may be taken!

A sharp limit of **15 pages**, not including references and appendices, in **standard LNCS format** is placed on all submissions. The paper should be intelligible and self contained without appendices, as committee members are not required to read appendices. The submission receipt deadline is **Friday, September 7, 2007 5:59pm CEST**. The paper must be fully anonymous, with no author names, affiliations, acknowledgments, or obvious references. The paper must start with a title, an abstract, and keywords. It should be followed by a succinct statement appropriate for a non-specialist reader, specifying the subject addressed, its background, the main results, and their significance. Technical details directed to the specialist should then follow. If accepted, one of the authors is expected to present the paper at the workshop. Further submission instructions will be posted on the conference home page, `http://www.iacr.org/workshops/pkc2008/`, about one month before the deadline. Submissions not meeting the guidelines risk rejection without consideration of their merits.

Conference General Chair: Carles Padró, UPC Barcelona.

Program Committee Chair: Ronald Cramer, CWI Amsterdam and Leiden University.

Program Committee:

Michel Abdalla, ENS, France
Masayuki Abe, NTT, Japan
Alexandra Boldyreva, Georgia Tech, USA
Jung Hee Cheon, Seoul National U, South Korea
Ronald Cramer, CWI and Leiden U, The Netherlands
Matthias Fitzi, ETH, Switzerland
Matthew Franklin, UC Davis, USA
Steven Galbraith, Royal Holloway, UK
Juan Garay, Bell Labs, USA
Rosario Gennaro, IBM Research, USA
Craig Gentry, Stanford U, USA
Kristian Gjøsteen, NTNU, Norway
María I. González Vasco, U Rey Juan Carlos, Spain
Jens Groth, UCLA, USA
Yuval Ishai, Technion, Israel
Eike Kiltz, CWI, The Netherlands
Kaoru Kurosawa, Ibaraki U, Japan
Wenbo Mao, HP Labs, China
Alexander May, TU Darmstadt, Germany
Jesper Buus Nielsen, Aarhus U, Denmark
Berry Schoenmakers, TU Eindhoven, The Netherlands
abhi shelat, IBM Research, Switzerland
Victor Shoup, New York U, USA
Martijn Stam, EPFL, Switzerland
Rainer Steinwandt, Florida Atlantic U, USA
Tsuyoshi Takagi, Future U Hakodate, Japan
Edlyn Teske, U Waterloo, Canada
Ramarathnam Venkatesan, Microsoft, USA & India
Jorge Villar, UPC, Spain
Moti Yung, Columbia U & RSA Labs, USA

Proceedings: Proceedings are published in Springer-Verlag's Lecture Notes in Computer Science Series and will be available at the conference.