Call for Papers:

9th International Workshop on Practice and Theory in Public Key Cryptography (PKC) 2006

April 22-24, 2006

Columbia University, New York, NY, USA

http://pkc06.cs.columbia.edu

Original research papers on all technical aspects of public key cryptography are solicited for submission to PKC 2006, the 9th International Workshop on Practice and Theory in Public Key Cryptography.

Submission Deadline: November 15, 2005
Author Notification: January 20, 2006
Camera-Ready Copy: February 10, 2006

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 (January 20th, 2006) 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 **November 15, 2005 5:59pm EST**. 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://pkc06.cs.columbia.edu, about one month before the deadline. Submissions not meeting the guidelines risk rejection without consideration of their merits.

Program Committee:

Masayuki Abe, NTT Japan
Feng Bao, I^2R, Singapore
Paulo Barreto, University of Sao Paulo, Brazil
Amos Beimel, Ben Gurion University, Israel
Xavier Boyen, Voltage Technology, USA
Jean-Sebastien Coron, University of Luxembourg
Serge Fehr, CWI, The Netherlands
Pierre-Alain Fouque, ENS Paris, France
Juan Garay, Bell Labs, USA
Rosario Gennaro, IBM Research, USA
Nick Howgrave-Graham, NTRU, USA
Dong Hoon Lee, Korea University, Korea
Wenbo Mao, HP Labs, China
Alexander May, Paderborn University, Germany
David Naccache, Gemplus and U. of Paris II, France
Rafail Ostrovsky, UCLA, USA
Kenny Paterson, Royal Holloway, U. of London, UK
Giuseppe Persiano, University of Salerno, Italy
Benny Pinkas, Haifa University, Israel
Leonid Reyzin, Boston University, USA
Kazue Sako, NEC Japan
Alice Silverberg, U. C. Irvine, USA
Jessica Staddon, PARC, USA
Ron Steinfeld, Macquarie University, Australia
Edlyn Teske, University of Waterloo, Canada
Wen-Guey Tzeng, NCTU, Taiwan
Susanne Wetzel, Stevens Institute, USA
Yiqun Lisa Yin, Independent Consultant, USA
Adam Young, Mitre, USA
Moti Yung, RSA Labs and Columbia U., USA

Conference Organizing Committee:

Conference and Program Committee Chair: Moti Yung, RSA Labs and Columbia University, USA
General Chair and Local Arrangements Chair: Tal Malkin, Columbia University, USA
General Chair and Sponsorship Chair: Yevgeniy Dodis, New York University, USA
Publicity and Publication Chair: Aggelos Kiayias, University of Connecticut, USA

Contact Information:

For questions, comments, or further information, please contact pkc06@cs.columbia.edu