PKC 2005

Les Diablerets, Switzerland, January 23-26, 2005

`http://lasecwww.epfl.ch/pkc05/`

Call for Papers

Background: For the last few years the International Workshop on Practice and Theory in Public-Key Cryptography has been the main annual workshop focusing on research on all aspects of public-key cryptography. The first workshop was organized in 1998 in Japan. Other PKCs have taken place in Australia, France, Japan, South Korea, Singapore, and USA.

Since 2003, PKC is an IACR workshop. PKC has attracted papers from world-renowned scientists in the area. The proceedings of PKC'05 will be published by Springer-Verlag in the Lecture Notes in Computer Science (LNCS) series.

Topics of interest: The topics of interest are all aspects of public-key cryptography including theory, design, analysis, implementation, and applications of public-key cryptography.

Instructions for Authors: 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 achievements, and their significance to public-key cryptology. Technical details directed to the specialist should then follow. If accepted, one of the authors is expected to present the paper at the workshop.

Submission instructions: Abstracts that have been or will be submitted in parallel to other conferences and workshops that have proceedings are not eligible for submission. A sharp limit of 18 pages in total using the standard LNCS format is placed on all submissions. The submission receipt deadline is **August 26, 2004**. To submit a paper, email to **pkc05@epfl.ch** with:

1. Submission letter in ASCII text format including the title, author names, address and phone number of the corresponding author, and the abstract.
2. Source files of the paper submission as well as the final PS or PDF file. It must be a full anonymous paper following the standard LNCS author instructions which can be found at `http://www.springer.de/comp/lncs/authors.html`

Submissions not meeting these guidelines risk rejection without consideration of their merits.

Acknowledgment of submissions: An acknowledgment email will be sent to the corresponding author upon receiving each submission. The authors are advised to contact us by email **pkc05@epfl.ch** if they do not receive the acknowledgment by August 29. This is to rescue the loss of submission due to the lower and lower reliability of email.

Important Dates:

Submission Deadline	August 26, 2004
Acceptance/Rejection Notification	October 28, 2004
Camera Ready Copy	November 14, 2004

Program Committee:

Carlisle Adams	(University of Ottawa, Canada)
Feng Bao	(Institute for Infocomm Research, Singapore)
Yvo Desmedt	(University College London, United Kingdom)
Juan Garay	(Bell Labs – Lucent Technologies, USA)
Martin Hirt	(ETH Zurich, Switzerland)
Kwangjo Kim	(Information and Communications University, Korea)
Kaoru Kurosawa	(Ibaraki University, Japan)
Anna Lysyanskaya	(Brown University, USA)
Wenbo Mao	(HP Labs Bristol, United Kingdom)
David Naccache	(Gemplus, France)
Kaisa Nyberg	(Nokia, Finland)
Tatsuaki Okamoto	(NTT Labs, Japan)
Josef Pieprzyk	(Macquarie University, Australia)
David Pointcheval	(CNRS-ENS, France)
Reihaneh Safavi-Naini	(University of Wollongong, Australia)
Kazue Sako	(NEC, Japan)
Claus-Peter Schnorr	(University of Frankfurt am Main, Germany)
Berry Schoenmakers	(Technische Universiteit Eindhoven, Netherlands)
Nigel Smart	(University of Bristol, United Kingdom)
Edlyn Teske	(University of Waterloo, Canada)
Serge Vaudenay	(EPFL, Switzerland)
Moti Yung	(University of Columbia, USA)
Yuliang Zheng	(University of North Carolina at Charlotte, USA)

Program Chair:
Prof. Serge Vaudenay, EPFL, LASEC, CH-1015 Lausanne, Switzerland

General Chairs:
Prof. Serge Vaudenay, EPFL, LASEC, CH-1015 Lausanne, Switzerland
Jean Monnerat, EPFL, LASEC, CH-1015 Lausanne, Switzerland