PKC 2004

http://www.i2r.a-star.edu.sg/pkc2004/

Singapore, March 1-4, 2004

Call for Papers

Submission Deadline: Sept 20, 2003

Background: For the last few years the International Workshop on Practice and Theory in Public Key Cryptography PKC is 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 and USA. PKC has attracted papers from famous international authors in the area.

The proceedings of PKC'04 will be published by Springer-Verlag in the Lecture Notes in Computer Science series. Submissions in all areas related to applications and theory in public key cryptography are welcome, including but not limited to the following areas:

1. Theory of public key cryptography.
2. Design of new public key cryptosystems.
3. Analysis of public key cryptosystems.
4. Efficient implementation of public key cryptographic algorithms.
5. Applications of public key cryptography and PKI.

Instructions for Authors: The paper must start with a title, an abstract and keywords, but should be **anonymous**. 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. Self citations to unpublished work should be avoided to maintain the anonymity. A limit of 12 singlespaced pages of 11pt type (not counting the appendices) is placed on all submissions. Since referees are not required to read the appendices, the paper should be intelligible without them. Submissions not meeting these guidelines risk rejection without consideration of their merits.

Submission instructions: Abstracts that have been or will be submitted in parallel to other conferences or workshops that have proceedings are not eligible for submission. One of the authors is expected to present the paper. The submission receipt deadline is **September 20, 2003**. To submit a paper, e-mail to

PKC2004@i2r.a-star.edu.sg

with:

1. Submission letter in ASCII including the title, author names, address and phone number of the corresponding author, and the abstract.
2. Paper submission in PS (or PDF) file. It must be a full **anonymous** paper.

Acknowledgment of submissions: An acknowledgment email will be sent to the corresponding author upon receiving each submission. The authors are advised to contact the PC Chair (either by email baofeng@i2r.a-star.edu.sg, or by phone +65 68748456) if they do not receive the acknowledgement by Sept 22. This is to rescue the loss of submission due to the less and less reliability of email.

Important Dates:

Submission Deadline	Sept 20, 2003
Acceptance/Rejection Notification	Nov 25, 2003
Camera Ready Copy	Dec 15, 2003

Program Committee:

Masayuki Abe	(NTT Laboratories, Japan)
Feng Bao	(Institute for Infocomm Research, Singapore)
Colin Boyd	(Queensland University of Technology, Australia)
Robert Deng	(Institute for Infocomm Research, Singapore)
Yvo Desmedt	(Florida State University, USA)
Marc Fischlin	(Fraunhofer-Institute Secure Telecooperation, Germany)
Eiichiro Fujisaki	(NTT Laboratories, Japan)
Goichiro Hanaoka	(University of Tokyo, Japan)
Marc Joye	(Gemplus, France)
Kwangjo Kim	(Information and Communications University, Korea)
Arjen Lenstra	(Citibank, USA & Tech Uni Eindhoven, Netherland)
Wenbo Mao	(Hewlett-Packard Labs, UK)
Alfred Menezes	(University of Waterloo, Canada)
Dingyi Pei	(Chinese Academy of Sciences, China)
Phong Nguyen	(CNRS/Ecole normale superieure, France)
Claus Schnorr	(Frankfurt University, Germany)
Nigel Smart	(University of Bristol, UK)
Renji Tao	(Chinese Academy of Sciences, China)
Serge Vaudenay	(Swiss Federal Institute of Technologies, Switzerland)
Sung-Ming Yen	(National Central University, Taiwan)
Moti Yung	(Columbia University, USA)
Yuliang Zheng	(University of North Carolina, USA)
Jianying Zhou	(Institute for Infocomm Research, Singapore)

General Chair:

Dr Robert Deng, deng@i2r.a-star.edu.sg, Institute for Infocomm Research, Singapore

Program Committee Chair:

Dr Feng Bao, baofeng@i2r.a-star.edu.sg, Institute for Infocomm Research, Singapore

Publication Chair:

Dr Jianying Zhou, jyzhou@i2r.a-star.edu.sg, Institute for Infocomm Research, Singapore