PKC 2003

Miami, Florida, January 6-8, 2003

Call for Papers

Submission Deadline: August 9, 2002

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 and South Korea.

PKC 2003 will be for the first time an IACR workshop. PKC has attracted papers from famous international authors in the area. The proceedings will be published by Springer Verlag in the Lecture Notes in Computer Science series.

Topics of interest The topics of interest are all aspects of public-key cryptography including:

- Certification and Time-stamping
- Computational Complexity Aspects
- Cryptanalysis
- Discrete Logarithm
- Electronic Cash/Payment
- Elliptic Curve Cryptography
- Encryption Schemes
- Fast Implementations
- Integer Factorization
- International Standards
- Lattice Reduction
- Provable Security
- Public Key Infrastructure
- Secure Electronic Commerce
- Signature Schemes

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 Self citations to unpublished work should be avoided to maintain the anonymity.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 11 singlespaced pages of 11pt type (not counting the bibliography and clearly marked appendices) is placed on all submissions. The total paper must not exceed 18 pages. 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 August 9, 2002 23:59 Hawaii time (i.e. GMT: August 10 at 9:59). To submit a paper, e-mail to pkc-submit@cs.fsu.edu an e-mail with the following two attachments:

- in ASCII the title, authors names, address of corresponding author, and the abstract,
- in PS (or PDF) file the full **anonymous** paper (i.e. title, abstract, keywords, etc.). The paper should be submitted as a Postscript or PDF (e.g. using PDFLaTeX) paper also readable on non-Windows platforms. For Unix users of LaTeX using ps2pdf one should use:
  - dvips -Ppdf -G0
    or dvips -Pcmz -G0
  - ps2pdf -dMaxSubsetPct=100 -dCompatibilityLevel=1.2 -dSubsetFonts=true -dEmbedAllFonts=true

Important dates	Submission Deadline:	August 9, 2002
	Authors Informed:	September 27, 2002
	Accepted papers need to arrive:	October 25, 2002.

Program Committee

Masayuki Abe (NTT Laboratories, Japan)
Feng Bao (Lab. for Information Technology, Singapore)
Yvo Desmedt (Florida State University, US)
Giovanni Di Crescenzo (Telcordia, US)
Marc Joye (Gemplus, France)
Kaoru Kurosawa (Ibaraki University, Japan)
Arjen Lenstra (Citicorp, US)
Tal Malkin (AT&T Research, US)
Ueli Maurer (ETH, Zurich, Switzerland)
Moni Naor (Weizmann Institute of Science, Israel)
Tatsuaki Okamoto (NTT Laboratories, Japan)
Jacques Patarin (Universite de Versailles, France)
Tal Rabin (IBM Research Lab., US)
Kazue Sako (NEC, Japan)
Jacques Stern (Ecole Normale Superieure, France)
Serge Vaudenay (ETH, Lausanne, Switzerland)
Yongge Wang (Karthika Technologies, Canada)
Michael Wiener (Canada)
Moti Yung (Certco, US)
Yuliang Zheng (University of North Carolina, US)

Sponsors For information about sponsoring, contact general chair M. Burmester at burmester@cs.fsu.edu

Program Chair: Dr. Yvo G. Desmedt
desmedt@cs.fsu.edu
206 Love Building
Florida State University
Tallahassee, FL 32306-4530

General Chair: Dr. Mike Burmester
burmester@cs.fsu.edu
206 Love Building
Florida State University
Tallahassee, FL 32306-4530