ASIACRYPT 2004

December 5-9, 2004
Jeju Island, Korea
http://www.iris.re.kr/ac04/

Call For Papers

Original papers on all technical aspects of cryptology are solicited for submission to ASIACRYPT2004, the annual International Conference on the Theory and Application of Cryptology and Information Security. The conference is organized by the International Association for Cryptologic Research (IACR) in cooperation with KIISC (Korean Institute of Information Security and Cryptology) and IRIS (International Research center for Information Security) at ICU (Information and Communications Univ.) and financially supported by MIC (Ministry of Information and Communication), Korea.

Important Dates

- **Submission: May 21, 2004**
- **Acceptance: Aug 2, 2004**
- **Proceedings version: Sep 1, 2004**

Instruction for Authors

Submissions must not substantially duplicate work that any of the authors has published elsewhere or has submitted in parallel to any other journal, conference or workshop that has proceedings. Authors of an accepted paper must guarantee that at least one of the authors will attend the conference and present their paper.

Submission Format

The paper must be anonymous, with no author names, affiliations, acknowledgments, or obvious references. It should begin with a title, a short abstract, and a list of keywords. The length of the paper should not exceed at most 12 pages excluding bibliography and appendices, and at most 20 pages total using at least 11-point fonts and with reasonable margins. The introduction should summarize the contributions of the paper at a level appropriate for a non-specialist reader. Committee members are not required to read appendices; the paper should be intelligible without them. Submissions not meeting these guidelines risk rejection without consideration of their merits.

Electronic Submission

A detailed description of the electronic submission procedure will appear by **March 14, 2004** on the Asiacrypt 2004 web pages (http://islab.postech.ac.kr/ac04/). Electronic submissions must conform to this procedure and be received by **May 21 2004, 09:00 GMT**. Other means of submission will not be honored.

Conference Proceedings

Proceedings will be published in Springer-Verlag's Lecture Notes in Computer Science and will be available at the conference. Clear instructions about the preparation of a final proceedings version will be sent to the authors of accepted papers.

Stipends

A limited number of stipends are available to those unable to obtain funding to attend the conference. Students whose papers are accepted and who will present the paper themselves are encouraged to apply if such assistance is needed. Requests for stipends should be addressed to the General Chair.

Program Committee Chair

Professor Pil Joong Lee
Department of Electronic & Electrical Engineering,
Pohang Univ. of Science & Technology (POSTECH)
(on leave at KT Research Center, Room 5601
Woomyeon-dong, Seocho-gu, Seoul 137-792,
Korea)
Tel : +82-2-526-5585, Fax : +82-2-526-6903
E-mail: pjl@postech.ac.kr, HP: +82-16-533-3232

General Chair

Professor Kwangjo Kim
School of Engineering,
Information & Communications University (ICU)
103-6 Munji-dong, Yusong-ku, Daejeon 305-714,
Korea
Tel: +82-42-866-6118, Fax: +82-42-866-6273
E-mail: kkj@icu.ac.kr, HP: +82-11-9414-1386

Program Committee

Jee Hea An	SoftMax, *USA*
Michael Backes	IBM Zurich Research Lab., *Switzerland*
Feng Bao	Institute for Infocomm Research, *Singapore*
Colin Boyd	Queensland Univ. of Tech., *Australia*
Liqun Chen	Hewlett-Packard Labs, *UK*
Don Coppersmith	IBM T.J. Watson Research Center, *USA*
Marc Joye	Gemplus, *France*
Jonathan Katz	Univ. of Maryland, *USA*
Yongdae Kim	Univ. of Minnesota, *USA*
Dong Hoon Lee	Korea Univ., *Korea*
Jaeil Lee	KISA, *Korea*
Arjen K. Lenstra	Citibank, *USA*, & Eindhoven Univ. of Tech., *The Netherlands*
Atsuko Miyaji	JAIST, *Japan*
Jesper Buus Nielsen	ETH Zurich, *Switzerland*
Choonsik Park	NSRI, *Korea*
Dingyi Pei	Chinese Academy of Sciences, *China*
Erez Petrank	Technion, *Israel*
David Pointcheval	CNRS-ENS, Paris, *France*
Bart Preneel	Katholieke Universiteit Leuven, *Belgium*
Vincent Rijmen	Graz University of Technology, *Austria*
Bimal Roy	Indian Statistical Institute, *India*
Rei Safavi-Naini	Univ. of Wollongong, *Australia*
Kazue Sako	NEC Corporation, *Japan*
Kouichi Sakurai	Kyushu University, *Japan*
Nigel Smart	University of Bristol, *UK*
Serge Vaudenay	EPFL, *Switzerland*
Sung-Ming Yen	National Central Univ., *Taiwan*
Yiqun Lisa Yin	Princeton Univ., *USA*
Moti Yung	Columbia Univ., *USA*
Yuliang Zheng	Univ. of North Carolina at Charlotte, *USA*

Secretarial support for Program Committee

Yong Ho Hwang & Yeon Hyeong Yang
Information Security Lab., Dept. of EEE, POSTECH
San 31, Hyoja-dong, Nam-gu, Pohang 790-784, Korea
Tel: +82-54-279-5650 & -5029, Fax: +82-54-279-2903,
E-mail: ac04@oberon.postech.ac.kr