



Call for papers ICISC 2004



The 7th Annual International Conference on Information Security and Cryptology
December 2-3, 2004
Novotel Ambassador Gangnam, Seoul, Korea
<http://www.icisc.org/>

Original papers on all aspects of theory and applications of information security and cryptology are solicited to the 7th Annual International Conference on Information Security and Cryptology, ICISC 2004 which is sponsored by KIISC (Korean Institute of Information Security and Cryptology) and financially supported by MIC (Ministry of Information and Communication, Korea).

Topics of Interest include, but are not limited to :

- Access Control & Audit
- Authentication
- Biometrics
- Block/Stream Ciphers
- Computer Security
- Copyright Protection
- Cryptographic Primitives
- Digital Signatures
- Distributed Systems Security
- Efficient Representations and Implementations
- Electronic Commerce
- Elliptic Curve Cryptosystems
- Hash Function
- Information Hiding
- Internet/Intranet Security
- Key Management
- Malicious Codes
- Mobile Security
- Provable Security
- Public Key Cryptosystems
- Public Key Infrastructure
- Smart/Java Cards
- Threshold Scheme

Instructions for Authors

Submission should not substantially duplicate work that any of the authors have published elsewhere or submitted in parallel to any other conference or workshop that has proceedings. The paper must start with a title, an abstract and keywords, but should be **anonymous**. The length of the submission should not exceed 12 pages excluding the bibliography and clearly marked appendices, using at least 11 point fonts and reasonable margins. Since referees are not required to read the appendices, the paper should be intelligible without them. All papers must be in PostScript (PS) or Portable Document Format (PDF), and must be submitted to icisc2004@nsri.re.kr. It is strongly recommended that submission must be processed using LaTeX2e according to the instruction at <http://www.springer.de/comp/lncs/authors.html>.

Important Dates

- Submission deadline: September 1, 2004 08:00 KST (GMT + 9 hr)
- Acceptance notification: October 16, 2004
- Proceedings version due : November 6, 2004

Conference Proceedings



The pre-proceedings will be available at the conference site and the post proceedings will be published by Springer-Verlag in the *Lecture Notes in Computer Science*.

Program Committee

- Alex Biryukov Katholieke Universiteit Leuven, Belgium
- Daniel Bleichenbacher Bell Laboratories, USA
- Kyo Il Chung ETRI, Korea
- Robert Deng Institute for Infocomm Research, Singapore
- Gene Itkis Boston University, USA
- Thomas Johansson Lund University, Sweden
- Antoine Joux DCSSI Crypto Lab, France
- Toshinobu Kaneko Tokyo University of Science, Japan
- Hyoung Joong Kim Kangwon National University, Korea
- Myung-Hwan Kim Seoul National University, Korea
- Seungjoo Kim Sungkyunkwan University, Korea
- Yongdae Kim University of Minnesota, USA
- Dong Hoon Lee Korea University, Korea
- Arjen K. Lenstra Citibank, USA & Eindhoven University of Technology, The Netherlands
- Masahiro Mambo Tohoku University, Japan
- Tsutomu Matsumoto Yokohama National University, Japan
- SangJae Moon Kyungpook National University, Korea
- David Naccache Gemplus Card International, France
- Phong Q. Nguyen CNRS/École Normale Supérieure, France
- Tatsuki Okamoto NTT Labs, Japan
- Josef Pieprzyk Macquarie University, Australia
- David Pointcheval École Normale Supérieure, France
- Vincent Rijmen Cryptomathic, Belgium & Graz University of Technology, Austria
- Matt Robshaw Royal Holloway, University of London, UK
- Jae-Cheol Ryou Chungnam National University, Korea
- Kouichi Sakurai Kyushu University, Japan
- Palash Sarkar Indian Statistical Institute, India
- William Whyte NTRU Cryptosystems, USA
- Sung-Ming Yen National Central University, Taiwan, ROC
- Moti Yung Columbia University, USA
- Yuliang Zheng University of North Carolina at Charlotte, USA

Program Committee Co-Chairs

Choonsik Park
NSRI
161 Gajeong-dong, Yuseong-gu
Daejeon, 305-350, KOREA
Phone: +82-42-860-5071
Fax: +82-42-860-5656
E-mail: csp@etri.re.kr

Seongtaek Chee
NSRI
161 Gajeong-dong, Yuseong-gu,
Daejeon, 305-350, KOREA
Phone: +82-42-860-6407
Fax: +82-42-860-5656
E-mail: chee@etri.re.kr