



Call for papers

ICISC 2005



The 8th Annual International Conference on Information Security and Cryptology
December 1-2, 2005, Seoul, Korea
<http://www.icisc.org/>

Original papers on all aspects of theory and applications of information security and cryptology are solicited to the 8th Annual International Conference on Information Security and Cryptology, ICISC 2005 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
- Biometrics
- Computer Security
- Cryptographic Primitives
- Distributed Systems Security
- Electronic Commerce
- Hash Function
- Internet/Intranet Security
- Malicious Codes
- Provable Security
- Public Key Infrastructure
- Threshold Scheme
- Authentication
- Block/Stream Ciphers
- Copyright Protection
- Digital Signatures
- Efficient Representations and Implementations
- Elliptic Curve Cryptosystems
- Information Hiding
- Key Management
- Mobile Security
- Public Key Cryptosystems
- Smart/Java Cards

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 icisc05@dosan.skku.ac.kr. It is strongly recommended that submissions be processed using LaTeX2e according to the instruction at <http://www.springer.de/comp/lncs/authors.html>.

Important Dates

- Submission deadline: September 8, 2005 08:00 KST (GMT + 9 hr)
- Acceptance notification: October 16, 2005
- Proceedings version due : November 6, 2005

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

- Giuseppe Ateniese
- Tuomas Aura
- Alex Biryukov
- John Black
- Liqun Chen
- Jung Hee Cheon
- Kyo-il Chung
- Jean-Sebastien Coron
- Ed Dawson
- Alexander W Dent
- Anand Desai
- Yevgeniy Dodis
- Gerhard Eschelbeck
- Serge Fehr
- Pierre-Alain Fouque
- Eiichiro Fujisaki
- The Johns Hopkins University, USA
- Microsoft Research, UK
- Katholieke Universiteit Leuven, Belgium
- University of Colorado, USA
- Hewlett-Packard Labs, UK
- Seoul National University, Korea
- ETRI, Korea
- University of Luxembourg, Luxembourg
- Queensland University of Technology, Australia
- Royal Holloway, University of London, UK
- NTT MCL, USA
- New York University, USA
- Qualys, USA
- CWI, The Netherlands
- Ecole normale superieure(ENS), France
- NTT Labs, Japan

- Juan A. Garay
 - Marc Girault
 - Philippe Golle
 - Dieter Gollmann
 - SangGeun Hahn
 - Yongfei Han
 - Goichiro Hanaoka
 - Markus Jakobsson
 - Marc Joye
 - Jonathan Katz
 - Hiroaki Kikuchi
 - Hyoung-Joong Kim
 - Kwangjo Kim
 - Kaoru Kurosawa
 - Taekyoung Kwon
 - Young-Bin Kwon
 - Chi Sung Laih
 - Kwok-Yan Lam
 - Dong Hoon Lee
 - Sang-Ho Lee

 - Arjen Lenstra
 - Yingjiu Li
 - Helger Lipmaa
 - Javier Lopez
 - Masahiro Mambo
 - Keith Martin
 - Mitsuru Matsui
 - Chris Mitchell
 - Atsuko Miyaji
 - SangJae Moon
 - Yi Mu
 - Jesper Buus Nielsen
 - DaeHun Nyang
 - Rolf Oppliger
 - Carles Padró
 - Raphael Chung-Wei Phan
 - Josef Pieprzyk
 - Vincent Rijmen
 - Rei Safavi-Naini
 - Kouichi Sakurai
 - Palash Sarkar
 - Nigel Smart
 - JungHwan Song
 - Willy Susilo
 - Tsuyoshi Takagi
 - Wen-Guey Tzeng
 - Guilin Wang
 - William Whyte
 - Michael Wiener
 - Chuan-Kun Wu
 - Shouhuai Xu
 - Sung-Ming Yen
 - Yongjin Yeom
 - Moti Yung
- Bell Laboratories, USA
 - France Telecom, France
 - Palo Alto Research Center, USA
 - TU Hamburg, Germany
 - KAIST, Korea
 - ONETS, China
 - University of Tokyo, Japan
 - Indiana University, Bloomington, USA
 - Gemplus Card International, France
 - University of Maryland, USA
 - University of Tokai, Japan
 - Kangwon National University, Korea
 - Information and Communication University, Korea
 - Ibaraki University, Japan
 - Sejong University, Korea
 - Chung-Ang University, Korea
 - National Cheng Kung University, Taiwan
 - Tsinghua University, China
 - Korea University, Korea
 - Ewha Womans University, Korea
 - Lucent Technologies' Bell Laboratories, USA, and Eindhoven University of Technology, The Netherlands
 - Singapore Management University, Singapore
 - Cybernetica AS & University of Tartu, Estonia
 - University of Malaga, Spain
 - University of Tsukuba, Japan
 - Royal Holloway, University of London, UK
 - Mitsubishi Electric Corporation, Japan
 - Royal Holloway, University of London, UK
 - JAIST, Japan
 - Kyungpook National University, Korea
 - University of Wollongong, Australia
 - Aarhus University, Denmark
 - Inha University, Korea
 - eSECURITY technologies, Switzerland
 - Technical University of Catalonia, Spain
 - Swinburne University of Technology, Malaysia
 - Macquarie University, Australia
 - Graz University of Technology, Austria
 - University of Wollongong, Australia
 - Kyushu University, Japan
 - Indian Statistical Institute, India
 - University of Bristol, UK
 - Hanyang University, Korea
 - University of Wollongong, Australia
 - Future University, Hakodate, Japan
 - National Chiao Tung University, Taiwan
 - Institute for Infocomm Research, Singapore
 - NTRU Cryptosystems, USA
 - Cryptographic Clarity, Canada
 - Chinese Academy of Sciences, China
 - The University of Texas at San Antonio, USA
 - National Central University, Taiwan
 - NSRI, Korea
 - Columbia University, USA

Program Co-Chairs

Dongho Won
 Sungkyunkwan University
 300 Cheoncheon-dong, Jangan-gu, Suwon-si,
 Gyeonggi-do 440-746, KOREA

Seungjoo Kim
 Sungkyunkwan University
 300 Cheoncheon-dong, Jangan-gu, Suwon-si,
 Gyeonggi-do 440-746, KOREA

- Chair: icisc05chair@dosan.skku.ac.kr
- E-mail submission: icisc05@dosan.skku.ac.kr
- Secretary: icisc05sec@dosan.skku.ac.kr

- Phone: +82-31-290-5695
- Fax: +82-31-290-5696