Preface

Annually sponsored by the Korea Institute of Information Security and Cryptology (KIISC), the fourth International Conference on Information Security and Cryptology (ICISC 2001) was held at the 63 Building in Seoul, Korea, December 6–7, 2001. The 63 Building, consisting of 60 stories above the ground and 3 stories underground, stands soaring up into the sky on the island of Youido, the Manhattan of Korea, and ranks by far the tallest of all buildings in the country.

The program committee received 102 submissions from 17 countries and regions (Australia, Belgium, China, Denmark, France, Germany, India, Italy, Japan, Korea, The Netherlands, Spain, Taiwan, Thailand, Vietnam, UK, and USA), of which 32 were selected for presentation in 8 sessions. All submissions were anonymously reviewed by at least 3 experts in the relevant areas. There was one invited talk by David Pointcheval (ENS, France) on "Practical Security in Public-Key Cryptography".

We are very grateful to all the program committee members who devoted much effort and valuable time to reading and selecting the papers. These proceedings contain the final version of each paper revised after the conference. Since the revised versions were not checked by the program committee rigorously, the authors must bear full responsibility for the contents of their papers.

The program committee also requested the expert advice of their colleagues, including: Seigo Arita, Joonsang Baek, Aditya Bagcya, Colin Boyd, Denis Carabin, Donghyeon Cheon, Jung Hee Cheon, Joo Yeon Cho, Seung Bok Choi, Kilsoo Chun, Christophe Clavier, Jean-Sebastien Coron, James Edwards, Youichi Futa, Riccardo Focardi, Soichi Furuya, Steven Galbraith, Pierre Girard, Kishan Chand Gupta, Helena Handschuh, Matt Henricksen, Si-Hwan Hong, Hyo Sun Hwang, Kyubeom Hwang, Toshiya Itoh, Keiichi Iwamura, Marc Jóye, Sungwoo Kang, Chong Hee Kim, Hae Suk Kim, Jeeyeon Kim, Young-Baek Kim, Hyunjo Kwon, Dong Hoon Lee, Eonkyung Lee, Leonie Simpson, Mark Looi, Subhamoy Maitra, Wenbo Mao, Bill Millan, Shiho Moriai, Masahiko Motoyama, Yong Man No, Hanae Nozaki, Katsuyuki Okeya, Hai-Wen Ou, Pascal Paillier, Dong Jin Park, Haeryong Park, Ju Hwan Park, Ludovic Rousseau, Kazue Sako, Fumihiko Sano, Palash Sarkar, Kyungah Shim, Hideo Shimizu, K. Sikdar, Sang Gyoo Sim, Boyeon Song, Masakazu Sousya, Ron Steinfeld, Maenghee Sung, Mitsuru Tada, Tsuyoshi Takagi, Lawrence Teo, Toshio Tokita, Yasuyuki Tsukada, Christophe Tymen, Kapali Viswanathan, Ping Wang, Susanne Wetzel, Masato Yamamicya, Jun-hui Yang, Ding-feng Ye, and Dae Hyun Yum. We apologize for any omissions from this list.

Special thanks also goes to all members of IRIS (International Research center for Information Security, http://www.iris.re.kr) and C&IS (Cryptology and Information Security, http://caislab.icu.ac.kr) Lab. for their skillful and professional assistance in supporting the various tasks of the program chair. Byoungcheon Lee deserves special thanks for his help in publishing the proceedings.

We are also grateful to all the organizing committee members for their volunteer work.

Finally, we would like to thank all the authors who submitted their papers to ICISC 2001 (including those whose submissions were not successful), as well as the conference participants from around the world, for their support, which made this conference a big success.

December 2001 Kwangjo Kim

ICISC 2001

2001 International Conference on Information Security and Cryptology

63 Building, Seoul, Korea
December 6-7, 2001

Sponsored by

Korea Institute of Information Security and Cryptology (KIISC)
(www.kiisc.or.kr)

In cooperation with

Ministry of Information and Communication (MIC), Korea
Institute of Information Technology Assessment (IITA), Korea
and Korea Information Security Agency (KISA), Korea

Financially Supported by

BCQRE, SECUi.COM, and SOFTFORUM, Korea

General Chair

Sang Jae Moon	(Kyungpook National University, Korea)

Program Committee

Kwangjo Kim, Chair	(Information and Communications University, Korea)
Chae Hoon Lim, Vice Chair	(Future Systems, Korea)
Gail-Joon Ahn	(University of North Carolina at Charlotte, USA)
Zongduo Dai	(Academia Sinica, China)
Ed Dawson	(Queensland University of Technology, Australia)
Cunsheng Ding	(Hong Kong University of Science and Technology, China)
Markus Jakosson	(RSA Labs, USA)
Seungjoo Kim	(Korea Information Security Agency, Korea)
Xuejia Lai	(Secure Web & Intranet Solutions Group, Switzerland)
Chi Sung Laih	(National Cheng Kung University, Taiwan)
Kwok Yan Lam	(PrivyLink International, Singapore)
Pil Joong Lee	(POSTECH, Korea)
Jongin Lim	(Korea University, Korea)
Atsuko Miyaji	(JAIST, Japan)
David Naccache	(Gemplus Card International, France)
Tatsuaki Okamoto	(NTT, Japan)
Choonsik Park	(National Security Research Institute, Korea)
cangjoon Park	(BCQRE, Korea)
Bimal Roy	(Indian Statistical Institute, India)
Kouichi Sakurai	(Kyushu University, Japan)
Sung Won Sohn	(Electronics and Telecommunications Research Institute, Korea)
Nigel Smart	(University of Bristol, UK)
Moti Yung	(CertCo, USA)
Yuliang Zheng	(University of North Carolina at Charlotte, USA)

Organizing Committee

Youjin Song, Chair	(Dongguk University, Korea)
Kyo Il Chung	(Electronics and Telecommunications Research Institute, Korea)
Hyon-Cheol Chung	(Softforum, Korea)
Douglas Guen	(INICIS, Korea)
Jae Cheol Ha	(Korea Nazarene University, Korea)
Ki Yoong Hong	(SECUVE, Korea)
Souhwan Jung	(Soongsil University, Korea)
Moon-Soo Jang	(OULLIM Information Technology, Korea)
Ki Tae Kim	(The Korea Economic Daily, Korea)
Seok Woo Kim	(Hansei University, Korea)
Dong Hoon Lee	(Korea University, Korea)
Heon Lee	(Ministry of Information and Communication, Korea)
Hyung Woo Lee	(Cheonan University, Korea)
Im Yeong Lee	(Soonchunhyang University, Korea)
Jongin Lim	(Korea University, Korea)
Jong Sou Park	(Hankuk Aviation University, Korea)
Sung Jun Park	(BCQRE, Korea)
Gwangsoo Rhee	(Sookmyung Women's University, Korea)
Kyung Hyune Rhee	(Pukyong National University, Korea)
Dae Hyun Ryu	(Hansei University, Korea)
Jong Tae Shin	(ISR, Korea)
Jae Geol Yim	(Dongguk University, Korea)
E-Joon Yoon	(National Security Research Institute, Korea)