

Preface

The 2nd International Conference on Information Security and Cryptology (ICISC) was sponsored by the Korea Institute of Information Security and Cryptology (KIISC). It took place at Korea University, Seoul, Korea, December 9-10, 1999. Jong In Lee of Korea University was responsible for the organization.

The call for papers brought 61 papers from 10 countries on four continents. As in the last year the review process was totally blind. The information about authors or their affiliation was not given to Technical Program Committee (TPC) members. Each TPC member was random-coded and did not even know who was reviewing which paper. The 23 TPC members finally selected 20 top-quality papers for presentation at ICISC 1999 together with one invited talk. Serge Vaudenay gave an invited talk on “Provable Security for Conventional Cryptography”.

Many people contributed to ICISC’99. First of all I would like to thank all the authors who submitted papers. I am grateful to the TPC members for their hard work reviewing the papers and the Organization Committee members for all the supporting activities which made ICISC’99 a success. I would like to thank the Ministry of Information and Communication of Korea (MIC) which financially sponsored ICISC’99. Special thanks go to Pil Joong Lee and Heung Youl Youm who helped me during the whole process of preparation for the conference. Last, but not least, I thank my students, KyuMan Ko, Sungkyu Chie, and Chan Yoon Jung.

December 1999

Jooseok Song

ICISC'99

December 9-10, 1999, Korea University, Seoul, Korea

The 2nd International Conference on
Information Security and Cryptology

Sponsored by
Korea Institute of Information Security and Cryptology
(KIISC)

In cooperation with
Korea Information Security Agency
(KISA)

Under the patronage of the
Ministry of Information and Communication (MIC), Korea

General Chair

Kil-Hyun Nam (President of KIISC, Korea)

Technical Program Committee

Zongduo Dai (Academica Sinica, P.R.C.)

Ed Dawson (Queensland University of Technology, Australia)

Tzonelih Hwang (National Cheng-Kung University, Taiwan, R.O.C.)

Chul Kim (Kwangwoon University, Korea)

Kwangjo Kim (Information and Communication University, Korea)

Kaoru Kurosawa (Tokyo Institute of Technology, Japan)

Kwok-Yan Lam (National University of Singapore)

Koung Goo Lee (KISA, Korea)

Pil Joong Lee (Pohang University of Science & Technology, Korea)

Chae Hoon Lim (Future Systems Incorporation, Korea)

Jong In Lim (Korea University, Korea)

Chris Mitchell (University of London, U.K.)

Sang Jae Moon (Kyungpook National University, Korea)

Kaisa Nyberg (Nokia Research Center, Finland)

Eiji Okamoto (JAIST, Japan)

Tatsuaki Okamoto (NTT, Japan)

Choon Sik Park (ETRI, Korea)

Sung Jun Park (KISA, Korea)

Bart Preneel (Katholieke Universiteit Leuven, Belgium)

Dong Ho Won (Sungkyunkwang University, Korea)

Heung Youl Youm (Soonchunhyang University, Korea)

Moti Yung (CertCo, U.S.A.)

Yuliang Zheng (Monash University, Australia)

Organizing Committee

Jong In Lim (Korea University)

Sang Kyu Park (HanYang University)

Ha Bong Chung (HongIk University)

Dong Hoon Lee (Korea University)

Sang Jin Lee (Korea University)

Howang Bin Ryou (KwangWoon University)

Seok Woo Kim (HanSei University)

Yong Rak Choi (Taejon University)

Jae Moungh Kim (ETRI)

Hong Sub Lee (KISA)

Seung Joo Han (ChoSun University)

Min Surp Rhee (DanKook University)

Seog Pal Cho (SeongGyul University)

Kyung Seok Lee (KIET)

Jong Seon No (Seoul National University)

Information Security and Cryptology - ICISC'99
Second International Conference Seoul, Korea,
December 9-10, 1999 Proceedings

Song, J. (Ed.)

2000, XII, 284 p., Softcover

ISBN: 978-3-540-67380-4