

# Preface

I would like to welcome all the participants to the 3rd International Conference on Information Security and Cryptology (ICISC 2000). It is sponsored by the Korea Institute of Information Security and Cryptology (KIISC) and is being held at Dongguk University in Seoul, Korea from December 8 to 9, 2000. This conference aims at providing a forum for the presentation of new results in research, development, and application in information security and cryptology. This is also intended to be a place where research information can be exchanged.

The Call for Papers brought 56 papers from 15 countries and 20 papers will be presented in five sessions. As was the case last year the review process was totally blind and the anonymity of each submission was maintained. The 22 TPC members finally selected 20 top-quality papers for presentation at ICISC 2000.

I am very grateful to the TPC members who devoted much effort and time to reading and selecting the papers. We also thank the experts who assisted the TPC in evaluating various papers and apologize for not including their names here. Moreover, I would like to thank all the authors who submitted papers to ICISC 2000 and the authors of accepted papers for their preparation of camera-ready manuscripts. Last but not least, I thank my student, Joonsuk Yu, who helped me during the whole process of preparation for the conference.

I look forward to your participation and hope you will find ICISC 2000 a truly rewarding experience.

December 2000

Dongho Won

# Organization

The 3rd International Conference on Information Security and Cryptology (ICISC 2000) is organized and sponsored by the Korea Institute of Information Security and Cryptology (KIISC).

## Executive Committee

Kil Hyun Nam	General Chair (President of KIISC, Korea)
Dong Ho Won	TPC chair (Sungkyunkwan University, Korea)
Jae Ho Shin	Organizing Chair (Dongguk University, Korea)

## Technical Program Committee

Dong Ho Won	Sungkyunkwan University, Korea
Zongduo Dai	Academia Sinica, P.R.C.
Ed Dawson	Queensland University of Technology, Australia
Chul Kim	Kwangwoon University, Korea
Kwang Jo Kim	Information and Communications University, Korea
Kaoru Kurosawa	Tokyo Inst. of Tech., Japan
Kwok-Yan Lam	National University of Singapore, Singapore
Kyoung Goo Lee	KISA, Korea
Pil Joong Lee	Pohang University of Sci. and Tech., Korea
Chae Hoon Lim	Future System Inc., Korea
Masahiro Mambo	Tohoku University, Japan
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	Toho University, Japan
Tatsuaki Okamoto	NTT, Japan
Choon Sik Park	ETRI, Korea
Sung Jun Park	BCQRE CO., LTD, Korea
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Heung Youl Youm	Soonchunhyang University, Korea
Moti Yung	CertCo, U.S.A.
Yuliang Zheng	Monash University, Australia

## Organizing Committee

Jae Ho Shin	Dongguk University, Korea
Chee Sun Won	Dongguk University, Korea
Sang Kyu Park	Hanyang University, Korea
Ha Bong Chung	Hongik University, Korea
Dong Hoon Lee	Korea University, Korea
Jae Jin Lee	Dongguk University, Korea
Howang Bin Ryou	Kwangwoon University, Korea
Seok Woo Kim	Hansei University, Korea
Yong Rak Choi	Taejon University, Korea
Hyun Sook Cho	ETRI, Korea
Hong Sub Lee	KISA, Korea
Seung Joo Han	Chosun University, Korea
Min Surp Rhee	Dankook University, Korea
Seog Pal Cho	Seonggul University, Korea
Kyung Seok Lee	KIET, Korea
Joo Seok Song	Yonsei University, Korea
Jong Seon No	Seoul National University, Korea
Tai Myoung Chung	Sungkyunkwan University, Korea

## Sponsoring Institutions

MIC (Ministry of Information and Communication), Korea  
IITA (Institute of Information Technology Assessment), Korea  
KISA (Korea Information Security Agency, Korea  
Dongguk University, Korea  
The Electronic Times, Korea



<http://www.springer.com/978-3-540-41782-8>

Information Security and Cryptology - ICISC 2000  
Third International Conference, Seoul, Korea, December  
8-9, 2000, Proceedings  
Won, D. (Ed.)  
2001, X, 266 p., Softcover  
ISBN: 978-3-540-41782-8