Preface

The 4th Workshop on Information Security Applications (WISA 2003) was sponsored by the following Korean organizations and government bodies: the Korea Institute of Information Security and Cryptology (KIISC), the Electronics and Telecommunications Research Institute (ETRI), and the Ministry of Information and Communication (MIC). The workshop was held in Jeju Island, Korea during August 25–27, 2003. This international workshop provided ample technical sessions covering a large spectrum of information security applications. Subjects covered included network/mobile security, electronic commerce security, digital rights management, intrusion detection, secure systems and applications, biometrics and human interfaces, public key cryptography, and applied cryptography.

The program committee received 200 papers from 23 countries (representing most geographic areas where security and applied cryptography research is conducted throughout the world). Each submitted paper was peer-reviewed by three program committee members. This year, we had two tracks: long and short presentation tracks. We selected 36 papers for the long presentation track and 34 papers for the short presentation tracks. This volume contains revised versions of papers accepted for the long presentation track. We would like to note that getting accepted to both tracks was an achievement to be proud of, given the competitive nature of WISA this year. Papers in the short presentation track were only published in the WISA preproceedings as preliminary notes; extended versions of these notes may be published by future conferences or workshops.

Many people worked very hard to produce a successful WISA 2003 workshop and its technical program. We are grateful to the organizing committee, the steering committee and the workshop general chairs for their support. We thank Springer-Verlag editors for their careful scrutiny and guidance in preparing the workshop proceedings. We are extremely thankful to the program committee members for spending their time on and devoting their efforts to reviewing the submitted papers and selecting the technical program. We also acknowledge the help of the external reviewers: Ahto Buldas and Markku-Juhani Saarinenl. We note that the program committee had members from numerous areas of research relevant to the workshop's subject and from many geographic areas, a fact that assured the breadth and the international nature of WISA. Finally, we would like to express our sincere thanks to all the authors of all the submitted papers, without whom this workshop would not have been possible.

October 2003

Kijoon Chae
Moti Yung

Organization

Advisory Committee

Man Young Rhee, Seoul National Univ., Korea
Hideki Imai, Tokyo Univ., Japan
Bart Preneel, Katholieke Universiteit Leuven, Belgium
Thomas A. Berson, Anagram Laboratories, USA
Gil Rok Oh, ETRI, Korea

General Co-chairs

Sehun Kim, KAIST, Korea
Chee Hang Park, ETRI, Korea

Steering Committee

Kil-Hyun Nam, Korea National Defense Univ., Korea
Sang Jae Moon, Kyungpook National Univ., Korea
Dong Ho Won, Sungkyunkwan Univ., Korea
Hyun Sook Cho, ETRI, Korea
Sung Won Sohn, ETRI, Korea

Organization Committee Chair

Jae Kwang Lee, Hannam Univ., Korea

Organization Committee

Finance	Kyo Il Chung, ETRI, Korea Hong Geun Kim, Korea Information Security Agency, Korea
Publication	Gwangsoo Rhee, Sookmyung Women's Univ., Korea Ji Young Lim, Korean Bible Univ., Korea
Publicity	Hyung Woo Lee, Hanshin Univ., Korea Dong Chun Lee, Howon Univ., Korea
Registration	Jae Cheol Ha, Korea Nazarene Univ., Korea
Treasurer	Jae Hoon Nah, ETRI, Korea
Local Arrangements	Byoung Joon Min, Incheon Univ., Korea Wang-Cheol Song, Cheju National Univ., Korea

Program Co-chairs

Kijoon Chae, Ewha Womans Univ., Korea
Moti Yung, Columbia Univ., USA

Program Committee

William Arbaugh, Univ. of Maryland, USA
Feng Bao, Institute for Infocomm Research, Singapore
Chin-Chen Chang, National Chungcheng Univ., Taiwan
Jean Sebastien Coron, Gemplus, France
Ed Dawson, QUT, Australia
Carl Ellison, Intel, USA
Marc Fischlin, Fraunhofer Gesellschaft SIT, Germany
Pierre-Alain Fouque, DCSSI, France
James Hughes, StorageTek, USA
Jong Soo Jang, ETRI, Korea
Aggelos Kiayias, Univ. of Connecticut, USA
Kwangjo Kim, ICU, Korea
Seungjoo Kim, KISA, Korea
Yongdae Kim, Univ. of Minnesota, USA
Kazukuni Kobara, Tokyo Univ., Japan
Pil Joong Lee, POSTECH, Korea
Dongdai Lin, SKLOIS, China
Helger Lipmaa, Helsinki Univ. of Technology, Finland
Fabian Monrose, Johns Hopkins Univ., USA
Shiho Moriai, Sony Computer Entertainment, Japan
Giuseppe Persiano, Univ. of Salerno, Italy
Bart Preneel, Katholieke Universiteit Leuven, Belgium
Pankaj Rohatgi, IBM, USA
Jae-Cheol Ryou, Chungnam National Univ., Korea
Kouichi Sakurai, Kyushu Univ., Japan
Tomas Sander, HP, USA
Serge Vaudenay, Federal Institute of Technology, Switzerland
Sung-Ming Yen, National Central Univ., Taiwan
Okyeon Yi, Kookmin Univ., Korea