Preface

ICICS 2001, the Third International Conference on Information and Communications Security, was held in Xi'an, China, 13-16 November 2001. Among the preceding conferences, ICICS'97 was held in Beijing, China, 11-14 November 1997 and ICICS'99 in Sydney, Australia, 9-11 November 1999. The ICICS'97 and ICICS'99 proceedings were released as volumes 1334 and 1726 of Springer-Verlag's Lecture Notes in Computer Science series.

ICICS 2001 was sponsored by the Chinese Academy of Sciences (CAS), the National Natural Science Foundation of China, and the China Computer Federation. The conference was organized by the Engineering Research Center for Information Security Technology of the Chinese Academy of Sciences (ERCIST, CAS) in co-operation with the International Association for Cryptologic Research (IACR), the International Communications and Information Security Association (ICISA), and the Asiacrypt Steering Committee.

The format of ICICS 2001 was selected to cover the complete spectrum of information and communications security, and to promote participant interaction. The sessions were designed to promote interaction between the major topics of the conference: theoretical foundations of security, secret sharing, network security, authentication and identification, boolean functions and stream ciphers, security evaluation, signatures, block ciphers and public-key systems, information hiding, protocols and their analysis, and cryptanalysis.

The 29-member Program Committee considered 134 submissions from 23 different countries and regions, among them 56 papers were accepted for presentation. Each paper was carefully reviewed blindly by a minimum of three referees from the respective field. The accepted papers came from 17 different countries and areas, including some 17 papers from China, 7 from Korea, 5 each from Australia and the USA, 3 each from Germany, Japan, Singapore, and Taiwan, 2 each from the UK, and 1 each from Finland, France, India, Israel, Italy, Portugal, Spain, and Thailand. We would like to take this opportunity to thank all who submitted papers to ICICS 2001 and the authors of accepted papers for their excellent work in preparing the camera-ready manuscripts.

We wish to thank the members of the program committee and reviewers for their effort in reviewing the papers in a short time and their great contribution to the conference in variety of ways. We are also pleased to thank Prof. Xizhen Ni, Dr. Yeping He, and the other members of the organizing committee for helping with many local details. Special thanks to Dr. Jianying Zhou of Oracle who took care of most of the tough work related to the publishing affairs. Finally, we would like to thank all the ICICS 2001 participants, organizers, and contributors for their work in making the conference a successful one.

August 2001   Sihan Qing
                                                                   Tatsuaki Okamoto

ICICS 2001

Third International Conference
on Information and Communications Security

Xi'an, China
November 13-16, 2001

Sponsored by

Chinese Academy of Sciences (CAS)
National Natural Science Foundation of China
China Computer Federation

Organized by

Engineering Research Center for Information Security Technology (ERCIST)
Chinese Academy of Sciences

In co-operation with

International Association for Cryptologic Research (IACR)
International Communications and Information Security Association (ICISA)
Asiacrypt Steering Committee

Conference Chairs

Qiheng Hu, general chair	(Vice President, China Association for Science and Technology)
Yongfei Han, vice chair	(MIAN, China)
Sihan Qing, program chair	(ERCIST, CAS, China)
Tatsuaki Okamoto, program chair	(NTT, Japan)

Program Committee

Tuomas Aura	(HUT, Finland)
Thomas Berson	(Anagram, USA)
Chin-Chen Chang	(MOE, Taiwan)
Lily Chen	(Motorola, USA)
Welland Chu	(THALES, Hong Kong, China)
Edward Dawson	(QUT, Australia)
Jan Eloff	(RAU, South Africa)
Dengguo Feng	(CAS, China)
Dieter Gollmann	(MicroSoft Lab in Cambridge, UK)
Kwangjo Kim	(ICU, Korea)
Xuejia Lai	(Entrust, Switzerland)

Chi-Sung Laih	(NCKU, Taiwan)
Wenbo Mao	(Hewlett-Packard Labs, Bristol, UK)
David Naccache	(Gemplus, France)
Eiji Okamoto	(Toho Univ., Japan)
David Pointcheval	(ENS, France)
Jean-Jacques Quisquater	(UCL, Belgium)
Bimal Roy	(ISICAL, India)
Pierangela Samarati	(UNIMI, Italy)
Vijay Varadharajan	(UWS, Australia)
Yumin Wang	(Xidian Univ., China)
Susanne Gudrun Wetzel	(Bell Lab, USA)
Tara Whalen	(CRC, Canada)
Guozhen Xiao	(Xidian Univ., China)
Lisa Yiqun Yin	(NTT, USA)
Moti Yung	(Columbia, USA)
Jianying Zhou	(Oracle, USA)

Organizing Committee

Xizhen Ni, chair	(ERCIST, CAS, China)
Yeping He, vice chair	(ERCIST, CAS, China)