Preface

ASIACRYPT 2000 was the sixth annual ASIACRYPT conference. It was sponsored by the International Association for Cryptologic Research (IACR) in cooperation with the Institute of Electronics, Information, and Communication Engineers (IEICE).

The first conference with the name ASIACRYPT took place in 1991, and the series of ASIACRYPT conferences were held in 1994, 1996, 1998, and 1999, in cooperation with IACR. ASIACRYPT 2000 was the first conference in the series to be sponsored by IACR.

The conference received 140 submissions (1 submission was withdrawn by the authors later), and the program committee selected 45 of these for presentation. Extended abstracts of the revised versions of these papers are included in these proceedings. The program also included two invited lectures by Thomas Berson (Cryptography Everywhere: IACR Distinguished Lecture) and Hideki Imai (CRYPTREC Project – Cryptographic Evaluation Project for the Japanese Electronic Government). Abstracts of these talks are included in these proceedings.

The conference program also included its traditional "rump session" of short, informal or impromptu presentations, kindly chaired by Moti Yung. Those presentations are not reflected in these proceedings.

The selection of the program was a challenging task as many high quality submissions were received. The program committee worked very hard to evaluate the papers with respect to quality, originality, and relevance to cryptography.

I am extremely grateful to the program committee members for their enormous investment of time and effort in the difficult and delicate process of review and selection.

I gratefully acknowledge the help of a large member of colleagues who reviewed submissions in their area of expertise: Masayuki Abe, Harald Baier, Olivier Baudron, Mihir Bellare, John Black, Michelle Boivin, Seong-Taek Chee, Ronald Cramer, Claude Crepeau, Pierre-Alain Fouque, Louis Granboulan, Safuat Hamdy, Goichiro Hanaoka, Birgit Henhapl, Mike Jacobson, Masayuki Kanda, Jonathan Katz, Dennis Kuegler, Dong-Hoon Lee, Markus Maurer, Bodo Moeller, Phong Nguyen, Satoshi Obana, Thomas Pfahler, John O. Pliam, David Pointch, Guillaume Poupard, Junji Shikata, Holger Vogt, Ullrich Vollmer, Yuji Watanabe, Annegret Weng, and Seiji Yoshimoto.

An electronic submission process was available and recommended. I would like to thank Kazumaro Aoki, who did an excellent job in running the electronic submission system of the ACM SIGACT group and in making a support system for the review process of the PC members. Special thanks to many people who supported him: Seiichiro Hangai and Christian Cachin for their web page supports, Joe Kilian for giving him a MIME parser, Steve Tate for supporting the SIGACT package, Wim Moreau for consulting their electronic review system,

and Masayuki Abe for scanning non-electronic submissions. Special thanks go to Mami Yamaguchi and Junko Taneda for their support in arranging review reports and editing these proceedings.

I would like to thank Tsutomu Matsumoto, general chair, and the members of organizing committee: Seiichiro Hangai, Shouichi Hirose, Daisuke Inoue, Keiichi Iwamura, Masayuki Kanda, Toshinobu Kaneko, Shinichi Kawamura, Michiharu Kudo, Hidenori Kuwakado, Masahiro Mambo, Mitsuru Matsui, Natsume Matsuzaki, Atsuko Miyaji, Shiho Moriai, Eiji Okamoto, Kouichi Sakurai, Fumihiko Sano, Atsushi Shimbo, Takeshi Shimoyama, Hiroki Shizuya, Nobuhiro Tagashira, Kazuo Takaragi, Makoto Tatebayashi, Toshio Tokita, Naoya Torii. We are especially grateful to Shigeo Tsujii and Hideki Imai for their great support of the organizing committee.

The organizing committee gratefully acknowledges the financial contributions of the two organizations, Initiatives in Research of Information Security (IRIS) and the Telecommunications Advancement Organization (TAF), as well as many companies.

I wish to thank all the authors who by submitting papers made this conference possible, and the authors of accepted papers for their cooperation.

Finally, I would like to dedicate these proceedings to the memory of Kenji Koyama, who passed away in March 2000. He was 50 years old. He was one of the main organizers of the first ASIACRYPT conference held in Japan in 1991, and devoted himself to make IACR the sponsor of ASIACRYPT. He was looking forward to ASIACRYPT 2000 very much, since it was the first of the ASIACRYPT conference series sponsored by IACR. May he rest in peace.

September 2000 Tatsuaki Okamoto

ASIACRYPT 2000

3–7 December 2000, Kyoto, Japan

Sponsored by the
International Association for Cryptologic Research (IACR)
in cooperation with the
Institute of Electronics, Information and Communication Engineers (IEICE)

General Chair
Tsutomu Matusmoto, Yokohama National University, Japan

Program Chair
Tatsuaki Okamoto, NTT Labs, Japan

Program Committee

Ross Anderson ..... Cambridge University, UK
Dan Boneh ..... Stanford University, USA
Johannes Buchmann ..... Technical University of Darmstadt, Germany
Ivan Damgård ..... Århus University, Denmark
Yvo Desmedt ..... Florida State University, USA
Yongfei Han ..... SecurEworld, Singapore
Ueli Maurer ..... ETH Zurich, Switzerland
Alfred Menezes ..... University of Waterloo, Canada
Moni Naor ..... Weizmann Institute, Israel
Choonsik Park ..... ETRI, Korea
Dingyi Pei ..... Chinese Academy of Science, China
Phillip Rogaway ..... University of California at Davis, USA
Kazue Sako ..... NEC, Japan
Kouichi Sakurai ..... Kyushu University, Japan
Jacques Stern ..... ENS, France
Serge Vaudenay ..... EPF Lausanne, Switzerland
Chung-Huang Yang ..... National Kaohsiung First University, Taiwan
Moti Yung ..... CertCo, USA
Yuliang Zheng ..... Monash University, Australia

Advisory Members

Kazumaro Aoki (Electronic submissions) ..... NTT Labs, Japan
Eiji Okamoto (ASIACRYPT'99 program co-chair) University of Wisconsin, USA