

Preface

ASIACRYPT'98, the international conference covering all aspects of theory and application of cryptology and information security, is being held at Beijing Friendship Hotel from October 18 to 22. This is the fourth of the Asiacrypt conferences. ASIACRYPT'98 is sponsored by the State Key Laboratory of Information Security (SKLOIS), University of Science and Technology of China (USTC), and the Asiacrypt Steering Committee (ASC), in cooperation with the International Association for Cryptology Research (IACR).

The 16-member Program Committee organized the scientific program and considered 118 submissions. Of these, 32 were accepted for presentation. The authors' affiliations of the 118 submissions and the 32 accepted papers range over 18 and 13 countries or regions, respectively.

The submitted version of each paper was sent to all members of the Program Committee and was extensively examined by at least three committee members and/or outside experts. The review process was rigorously blinded and the anonymity of each submission are maintained until the selection was completed. We followed the traditional policy that each member of the Program Committee could be an author of at most one accepted paper.

These proceedings contain the revised versions of the 32 contributed talks as well as a short note written by one invited speaker. Comments from the Program Committee were taken into account in the revisions. However, the authors (not the committee) bear full responsibility for the contents of their papers.

We are very grateful to the members of the Program Committee for generously spending so much of their time on the difficult task of selecting the papers. They are: Thomos A. Berson, Colin Boyd, Zongduo Dai, Marc Girault, Xuejia Lai, Tzonelih Hwang, Burt Kaliski, Kwangjo Kim, Kouichi Sakurai, Mitsuru Matsui, Andrew Odlyzko, Guozhen Xiao, Lam Kwok Yan, Yuliang Zheng. We also thank the following outside experts who assisted the Program Committee in evaluating various papers: Masayuki Abe, Kazumaro Aoki, Fabrice Boudot, Dengguo Feng, Atsushi Fujioka, Eiichiro Fujisaki, Henri Gilbert, Louis Goubin, Shaoquan Jiang, Masayuki Kanda, Shiho Moriai, Tatsuaki Okamoto, Haiwen Ou, Jacques Patarin, Philippe Toffin, Jacques Traore, Shigenori Uchiyama, Yujie Zhou, Moti Yung. We apologize for any omission in this list.

We would like to appreciate all who have submitted papers to ASIACRYPT'98 and the authors of accepted papers for their on-time preparation of camera-ready manuscripts.

We are also pleased to thank Shu Chang and Chen Lan for their help with preparation of the various tasks of the program co-chairs.

August 1998

Kazuo Ohta
Dingyi Pei

ASIACRYPT'98

Beijing, October 18-22, China

**International Conference on the Theory and
Application of Cryptology and Information Security**

Sponsored by

**The State Key Laboratory of Information Security
University of Science and Technology of China**

and

The Asiacrypt Steering Committee

In cooperation with

The International Association for Cryptologic Research

General Chair

Keqin Feng (Vice President of USTC)

Program Committee

Thomas A. Berson (Anagram Labs., USA)

Colin Boyd (Queensland Univ. of Tech., Australia)

Zongduo Dai (Chinese Academy of Sciences, China)

Marc Girault (France Telecom, France)

Xuejia Lai (R3 Security Engineering, Switzerland)

Tzonelih Hwang (National Cheng Chung Univ., Taiwan)

Burt Kaliski (RSA Labs., USA)

Kwangjo Kim (Information and Communication Univ., Korea)

Kouichi Sakurai (Kyushu Univ., Japan)

Mitsuru Matsui (Mitsubishi Electric Corp., Japan)

Andrew Odlyzko (AT&T, USA)

Kazuo Ohta (Co-chair, NTT, Japan)

Dingyi Pei (Co-chair, SKLOIS, China)

Guozhen Xiao (Xidian Univ., China)

Lam Kwok Yan (National Univ. of Singapore, Singapore)

Yuliang Zheng (Monash Univ., Australia)

Organizing Committee

Qing Chang (National Nature Science Foundation, China)

Guang Hua (Graduate School of USTC, China)

Kan Zhang (Chinese Academy of Sciences, China)

Xinkao Song (Beijing Scientific and Technical Society, China)

Zhansheng Zhao (Chairman, SKLOIS, China)