Preface

The PKC'99 conference, held in the ancient capital of Kamakura, Japan, March 1-3, 1999, represents the second conference in the international workshop series dedicated to the practice and theory in public key cryptography.

The program committee of the conference received 61 submissions from 12 countries and regions (Australia, Canada, Finland, France, Japan, Saudi Arabia, Singapore, Spain, Taiwan, UK, USA, and Yugoslavia), of which 25 were selected for presentation. All submissions were reviewed by experts in the relevant areas.

The program committee consisted of Chin-Chen Chang of the National Chung Cheng University, Taiwan, Yvo Desmedt of the University of Wisconsin-Milwaukee, USA, Hideki Imai (Co-Chair) of the University of Tokyo, Japan, Markus Jakobsson of Bell Labs, USA, Kwangjo Kim of Information and Communications University, Korea, Arjen Lenstra of Citibank, USA, Tsutomu Matsumoto of Yokohama National University, Japan, Eiji Okamoto of JAIST, Japan, Tatsuaki Okamoto of NTT, Japan, Nigel Smart of HP Labs Bristol, UK, and Yuliang Zheng (Co-Chair) of Monash University, Australia. Members of the committee spent numerous hours in reviewing the submissions and providing advice and comments on the selection of papers. We would like to take this opportunity to thank all the members for their invaluable help in producing such a high quality technical program.

The program committee also asked expert advice of many of their colleagues, including: Masayuki Abe, Kazumaro Aoki, Daniel Bleichenbacher, Atsushi Fujioka, Eiichiro Fujisaki, Chandana Gamage, Brian King, Kunio Kobayashi, Tetsutaro Kobayashi, Phil MacKenzie, Hidemi Moribatake, Kazuo Ohta, Amin Shokrollahi, Shigenori Uchiyama, and Yongge Wang. We thank them all for their help.

The conference would not have been successful without the skillful assistance of the members of the organizing committee. Our special thanks go to Takashi Mano of IPA, Japan, Kanta Matsuura and Hidenori Shida, both of University of Tokyo, Japan.

Last, but not least, we would like to thank all the people who submitted their papers to the conference (including those whose submissions were not successful), as well as the workshop participants from around the world, for their support which made this conference possible.

March 1999
University of Tokyo, Japan   Hideki Imai
Monash University, Melbourne, Australia   Yuliang Zheng

PKC'99

1999 International Workshop
on Practice and Theory
in Public Key Cryptography

Kamakura Prince Hotel, Kamakura, Japan
March 1-3, 1999

In cooperation with
The Technical Group on Information Security, the Institute of
Electronics, Information and Communication Engineers (IEICE)

Organizing Committee

Hideki Imai, Chair	(University of Tokyo, Japan)
Takashi Mano	(IPA, Japan)
Kanta Matsuura	(University of Tokyo, Japan)
Hidenori Shida	(University of Tokyo, Japan)
Yuliang Zheng	(Monash University, Australia)

Program Committee

Hideki Imai, Co-Chair	(University of Tokyo, Japan)
Yuliang Zheng, Co-Chair	(Monash University, Australia)
Chin-Chen Chang	(National Chung Cheng University, Taiwan)
Yvo Desmedt	(University of Wisconsin-Milwaukee, USA)
Kwangjo Kim	(Information and Communications University, Korea)
Markus Jakobsson	(Bell Labs, USA)
Arjen Lenstra	(Citibank, USA)
Tsutomu Matsumoto	(Yokohama National University, Japan)
Eiji Okamoto	(JAIST, Japan)
Tatsuaki Okamoto	(NTT, Japan)
Nigel Smart	(HP Labs Bristol, UK)