Preface

The origins of the Asiacrypt series of conferences can be traced back to 1990, when the first Auscrypt conference was held, although the name Asiacrypt was first used for the 1991 conference in Japan. Starting with Asiacrypt 2000, the conference is now one of three annual conferences organized by the International Association for Cryptologic Research (IACR). The continuing success of Asiacrypt is in no small part due to the efforts of the Asiacrypt Steering Committee (ASC) and the strong support of the IACR Board of Directors.

There were 153 papers submitted to Asiacrypt 2001 and 33 of these were accepted for inclusion in these proceedings. The authors of every paper, whether accepted or not, made a valued contribution to the success of the conference. Sending out rejection notifications to so many hard working authors is one of the most unpleasant tasks of the Program Chair.

The review process lasted some 10 weeks and consisted of an initial refereeing phase followed by an extensive discussion period. My heartfelt thanks go to all members of the Program Committee who put in extreme amounts of time to give their expert analysis and opinions on the submissions. All papers were reviewed by at least three committee members; in many cases, particularly for those papers submitted by committee members, additional reviews were obtained. Specialist reviews were provided by an army of external reviewers without whom our decisions would have been much more difficult. A list of their names is included overleaf; I hope this is complete, but if there are omissions please be assured this was not intentional. My thanks go to all of them.

In addition to the contributed papers, I was delighted to be able to secure two eminent and engaging speakers for the invited talks at the conference. Arjen K. Lenstra talked on “Impossible Security: Matching AES Security Using Public Key Systems” and Brendan McKay talked on “Debunking the Bible Codes”. As is traditional at all IACR conferences, a rump session was held to give the opportunity to hear latest results and work in progress on a wide variety of topics. I would like to thank Bill Caelli for agreeing to take charge of this event with his usual flair.

The smooth running of Asiacrypt 2001 was engineered by an Organizing Committee led by the General Chair, Ed Dawson, and his deputy Mark Looi. Other members of the committee were Andrew Clark, Ernest Foo, Betty Hansford, Lauren May, Christine Orme and Jason Thomas.

I received sterling advice from many experienced people at all stages of the program preparation. Members of the ASC and the IACR board were all very supportive. Special mention must go to Tatsuaki Okamoto who acted as Advisory Member of the committee and provided advice based on his considerable experience. I would also like to particularly thank previous chairs of IACR conferences, Mihir Bellare, Bart Preneel, and Joe Kilian, who got very used to being
bothered by me with requests for advice on all kinds of problems I had not encountered before and were always prepared to give their insightful opinions.

Any conference today relies heavily on technology to ease the administrative burden. All paper submissions to Asiacrypt 2001 were received electronically using the web based submission software which has been provided by Chanathip Namprempre. Papers were then seamlessly imported into the review software which was kindly provided by COSIC, Katholieke Universiteit Leuven, courtesy of Bart Preneel. The submission software was supported by COSIC’s Wim Moreau, who was extremely helpful in providing advice and bug fixes, and went to great lengths to provide extra features in the software at very short notice. Installing and maintaining the software at ISRC was Andrew Clark. Andrew worked tirelessly to ensure that the web server and review server were (almost) always available, provided several additional features to the software, and generally worked miracles to solve all the problems I came up with.

I was assisted in many different ways by numerous other ISRC members. Ed Dawson, as General Chair and also as Director of ISRC, provided his support throughout. Greg Maitland and Kapali Viswanathan came to my rescue on numerous occasions.

Having seen all the people who contributed to the process of preparing the program, it may be deduced that I did very little myself. Nevertheless all those late nights and weekends went somewhere and I would like to acknowledge the forbearance of my family $D + C^2$, and my colleagues and research students, who experienced severe denial of service at many times over the months leading up to the conference.

October 2001

Colin Boyd
ASIACRYPT 2001

December 9-13, 2001, Gold Coast, Australia

Sponsored by the
International Association for Cryptologic Research (IACR)

General Chair
Ed Dawson, Queensland University of Technology, Australia

Program Chair
Colin Boyd, Queensland University of Technology, Australia

Program Committee

Masayuki Abe .......................... NTT Laboratories, Japan
Ronald Cramer ..................... BRICS & University of Aarhus, Denmark
ZongDuo Dai ........................... Univ. of Science and Technology of China
Rosario Gennaro .................... IBM TJ Watson Research Centre, USA
Jovan Golić ............................. Gemplus, Italy
Chi-Sung Laih ....................... National Cheng Kung Univ., Taiwan
Kwok Yan Lam ........................ PrivyLink International Ltd, Singapore
Pil Joong Lee ............................ POSTECH, Korea
Arjen K Lenstra ...................... Citibank, USA; TU Eindhoven, The Netherlands
Wenbo Mao ............................. HP Laboratories, UK
pascal Paillier .......................... Gemplus, France
Vincent Rijmen ........................ Cryptomathic, Belgium
Bimal Roy .............................. Indian Statistical Institute
Rei Safavi-Naini ...................... University of Wollongong, Australia
Kouichi Sakurai ...................... Kyushu University, Japan
Nigel Smart ............................. University of Bristol, UK
Stefan Wolf ............................ University of Waterloo, Canada
Moti Yung ............................... CertCo, USA
Yuliang Zheng ....................... Monash University, Australia

Advisory Member:
Tatsuaki Okamoto (Asiacrypt 2000 Program Chair) NTT Laboratories, Japan
VIII Organization

External Reviewers

Joonsang Baek
Li Bao
Rana Barua
Alexandre Benoît
Simon Blackburn
Ian Blake
Daniel Bleichenbacher
Wieb Bosma
Eric Brier
Jan Camenisch
Ran Canetti
Denis Carabin
Sandeepan Choudhury
Andrew Clark
Christophe Clavier
Jean-Sebastien Coron
Robert Coulter
Ed Dawson
Jean-Francois Dhem
Ye Ding Feng
Matthias Fitzi
Matt Franklin
Atushi Fujioka
Eiichiro Fujisaki
Steven Galbraith
Shuhong Gao
Juan Garay
Pierrick Gaudry
Dieter Gollmann
Juannna González Nieto
Kishan C. Gupta
Stuart Haber
Ou Haiwen

Shai Halevi
Marie Henderson
Florian Hess
Nick Howgrave-Graham
D.J. Guan
Markus Jakobsson
Thomas Johansson
Marc Joyce
Ari Juels
Meng Chow Kang
Jonathan Katz
Kazukuni Kobara
Reto Kohlas
Hartono Kurino
Pierre-Louis Gaudry
Yehuda Lindell
Christoph Ludwig
Anna Lysyanskaya
Greg Maitland
Subhamoy Maitra
Alfred Menezes
Bernd Meyer
Bill Millan
Shingo Miyazaki
Sean Murphy
David Naccache
Phong Nguyen
Jesper Buus Nielsen
Wakaha Ogata
Katsu Okeya
Sarbani Palit
Kenny Paterson
Beatrice Peirani
Fabien Petitcolas
Wang Ping
Florence Ques
Alon Rosen
Atri Rudra
Yasu Sakai
Palash Sarkar
Claus Schnorr
Gadiel Seroussi
Nickolas Sheppard
Igor Shparlinski
Leonie Simpson
David Soldera
Martijn Stam
Ron Steinfeld
Hung-Min Sun
Willy Susilo
Koutarou Suzuki
S.C. Tai
Tsuyoshi Takagi
Chik How Tan
Christophe Tymen
Wen-Guey Tseng
Shigenori Uchiyama
Salil Vadhan
Eric Verheul
Kapali Viswanathan
Huaxiong Wang
Yejing Wang
Michael Wiener
Yi Xun
Jeff Jianxin Yan
Advances in Cryptology — ASIACRYPT 2001
7th International Conference on the Theory and
Application of Cryptology and Information Security Gold
Boyd, C. (Ed.)
2001, XI, 601 p. 22 illus., Softcover
ISBN: 978-3-540-42987-6