

Preface

ASIACRYPT 2002 was held in Queenstown, New Zealand, December 1–5, 2002. The conference was organized by the International Association for Cryptologic Research (IACR).

The program committee received 173 submissions from around the world, from which 34 were selected for presentation. Each submission was reviewed by at least three experts in the relevant research area.

Let me first thank all the authors, including those whose submissions were not successful, for taking the time to prepare the submissions. Their dedication and efforts in advancing research in cryptography made this conference possible.

Selecting presentations from such a large number of submissions was an extremely difficult and challenging task. The program committee members, together with external referees, spent thousands of hours of their precious time reviewing the submissions. At the completion of the selection process, the program committee received 875 review reports in total. In addition, the committee received several hundred comments during the three-week period of discussions.

Taking this opportunity, I would like to thank all the program committee members for their time and dedication. Without their expertise in the state of the art in cryptography and their willingness to serve the data security community, the conference would not have had such a high-quality program. I would also like to thank the numerous external referees for their invaluable assistance in identifying the scientific and practical merits of the submissions.

The quality of the program was further enhanced by two distinguished keynote speeches delivered by Prof. Tsutomu Matsumoto from Yokohama National University in Japan, and Dr. Moti Yung from CertCo and Columbia University in the USA. On behalf of the program committee, I would like to thank both prominent pioneers in cryptography for their inspiring presentations.

Thanks also go to the general chair Hank Wolfe from the University of Otago for successfully running the conference in such a beautiful town. It was a wonderful experience for me to work with Hank.

The reviewing process benefited greatly from the advice of Bart Preneel and Wim Moreau on handling the reviewing software. I appreciated Colin Boyd's assistance in editing the proceedings. My special thanks go to Lawrence Teo who acted as my assistant during the entire period of setting up the website, accepting, reviewing submissions, and editing the final proceedings. The year-long process would not have run so smoothly without his tireless help and superb technical skills in handling the software packages.

ASIACRYPT 2002

December 1–5, 2002, Queenstown, New Zealand

Sponsored by the
International Association for Cryptologic Research (IACR)

General Chair

Henry Wolfe, University of Otago, New Zealand

Program Chair

Yuliang Zheng, University of North Carolina at Charlotte, USA

Program Committee

Feng Bao	LIT, Singapore
Ed Dawson	QUT, Australia
Giovanni DiCrescenzo	Telcordia, USA
Matthew Franklin	UC Davis, USA
Dieter Gollmann	Microsoft Research, UK
Helena Handschuh	Gemplus, France
Philip Hawkes	Qualcomm, Australia
Ari Juels	RSA Laboratories, USA
Kwangjo Kim	ICU, South Korea
Seungjoo Kim	KISA, South Korea
Chi Sung Laih	National Cheng Kung University, Taiwan
Pil Joong Lee	POSTECH, South Korea
Arjen Lenstra	Citibank, USA
Phil MacKenzie	Lucent Technologies, USA
Masahiro Mambo	Tohoku University, Japan
Wenbo Mao	HP Labs, UK
Keith Martin	Royal Holloway, University of London, UK
Alfred Menezes	University of Waterloo, Canada
Phong Nguyen	ENS, France
Dingyi Pei	Chinese Academy of Sciences, China
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Kouichi Sakurai	Kyushu University, Japan
Jessica Staddon	PARC, USA
Serge Vaudenay	EPFL, Switzerland
Sung-Ming Yen	National Central University, Taiwan
Xian-Mo Zhang	University of Wollongong, Australia
Yuliang Zheng (Chair)	UNC Charlotte, USA
Hong Zhu	Fudan University, China

Advisory Member:

Colin Boyd (Asiacrypt 2001 Program Chair) QUT, Australia

External Reviewers

Masayuki Abe
Giuseppe Ateniese
Gildas Avoine
Joonsang Baek
Dirk Balfanz
Mark Bauer
Peter Beelen
Alex Biryukov
Simon Blackburn
Daniel Bleichenbacher
Alexandra Boldyreva
Dan Boneh
Colin Boyd
Emmanuel Bresson
Eric Brier
Linda Burnett
Brice Canvel
Dario Catalano
Stefania Cavallar
Geng Hau Chang
Chien-ning Chen
Chien Yuan Chen
Liqun Chen
Jung Hee Cheon
J.H. Chiu
YoungJu Choie
Andrew Clark
Scott Contini
Jean-Sébastien Coron
Nicolas Courtois
Christophe De Cannière
Alex Dent
Anand Desai
Markus Dichtl
Hiroshi Doi
Glenn Durfee
Chun I Fan
Marc Fischlin
Yair Frankel
Martin Gagne
Steven Galbraith
Juan Garay
Katharina Geissler
Rosario Gennaro
Craig Gentry
David Goldberg
Juan Manuel Gonzalez-Nieto
Louis Goubin
Louis Granboulan
Richard Graveman
Dan Greene
D.J. Guan
Jae-Cheol Ha
Stuart Haber
Satoshi Hada
Goichiro Hanaoka
Darrel Hankerson
Matthew Henricksen
Florian Hess
Shoichi Hirose
Dennis Hofheinz
Herbie Hopkins
Min-Shiang Hwang
Yong Ho Hwang
Hisashi Inoue
Toshiya Itoh
Tetsu Iwata
Markus Jakobsson
Jinn-Ke Jan
Rob Johnson
Marc Joye
Wen-Shenq Juang
Pascal Junod
Burt Kaliski
Masayuki Kanda
Jonathan Katz
Alexander Kholosha
Aggelos Kiayias
Hiroaki Kikuchi
Chong Hee Kim
Neal Koblitz
Takeshi Koshihara
Kaoru Kurosawa
Hidenori Kuwakado
Tanja Lange
Dong-Hoon Lee
Narn-Yih Lee
Sangjin Lee

Y.C. Lee
Hsi-Chung Lin
Chi-Jen Lu
Chun-Shien Lu
Christoph Ludwig
David M'Raihi
Mike Malkin
Tal Malkin
John Malone-Lee
Takashi Mano
James McKee
Bill Millan
Sara Miner
Takaaki Mizuki
Jean Monnerat
Shiho Moriai
Siguna Muller
Bill Munro
David Naccache
Koh-ichi Nagao
Toru Nakanishi
Kazuo Ohta
Kazuomi Oishi
Satomi Okazaki
Rafail Ostrovsky
Akira Otsuka
Pascal Paillier
Dong Jin Park
Ji-Hwan Park
Kenny Paterson
Giuseppe Persiano
John Proos
Michael Quisquater
Arash Reyhani-Masoleh
Vincent Rijmen
Matt Robshaw
Peter de Rooij
Greg Rose
Ludovic Rousseau
Taiichi Saito
Ryuichi Sakai
Jasper Scholten
Chaofeng Sha

Junji Shikata
Atsushi Shimbo
Igor Shparlinski
Francesco Sica
Alice Silverberg
Joe Silverman
Sang Gyoo Sim
Leonie Simpson
Nigel Smart
Diana Smetters
David Soldera
Martijn Stam
Makoto Sugita
Hung-Min Sun
Koutarou Suzuki
Mike Szydlo
Mitsuru Tada
Tsuyoshi Takagi
Katsuyuki Takashima
Edlyn Teske
Yiannis Tsiounis
Christophe Tymen
Wen-Guey Tzeng
Masashi Une
Frederik Vercauteren
Eric Verheul
Kapali Viswanathan
Jose Vivas
Huaxiong Wang
Peter Wild
Hao-Chi Wong
Tzong-Chen Wu
Masato Yamamichi
Akihiro Yamamura
Jeff Yan
Ching-Nung Yang
Yi-Shiung Yeh
Yiqun Lisa Yin
Maki Yoshida
Dae Hyun Yum
Fanguo Zhang
Yiqiang Zuo



<http://www.springer.com/978-3-540-00171-3>

Advances in Cryptology - ASIACRYPT 2002
8th International Conference on the Theory and
Application of Cryptology and Information Security,
Queenstown, New Zealand, December 1-5, 2002,
Proceedings
Zheng, Y. (Ed.)
2002, XIV, 582 p., Softcover
ISBN: 978-3-540-00171-3