Preface

ASIACRYPT 2003 was held in Taipei, Taiwan, from Nov. 30 to Dec. 4, 2003. The 9th Annual ASIACRYPT conference was sponsored by the International Association for Cryptologic Research (IACR), this year in cooperation with the Chinese Cryptology and Information Security Association (CCISA) and National Cheng Kung University (NCKU) in Taiwan.

One hundred and eighty-eight papers from 26 countries were submitted to ASIACRYPT 2003 and 33 (of which one paper was withdrawn by the authors after notification) of these were selected for presentation. These proceedings contain revised versions of the accepted papers. We had an IACR 2003 Distinguished Lecture, by Dr. Don Coppersmith, entitled “Solving Low Degree Polynomials.” In addition, two invited talks were given at the conference. One was given by Dr. Adi Shamir. The other one was given by Dr. Hong-Sen Yan, entitled “The Secret and Beauty of Ancient Chinese Locks.” The conference program also included a rump session, chaired by Tzong Chen Wu, which featured short informal talks on recent results.

It was a pleasure for me to work with the program committee, which was composed of 27 members from 17 countries; I thank them for working very hard over several months. As a matter of fact, the review process was a challenging and time-consuming task, and it lasted about 8 weeks, followed by more than half a month for discussions among the program committee members. All submissions were anonymously reviewed by at least 3 members in the relevant areas of the program committee; in some cases, particularly for those papers submitted by a member of the program committee, they were reviewed by at least six members. We are grateful to all the program committee members who put in a lot of effort and precious time giving their expert analysis and comments on the submissions. In addition, we really appreciate the external referees who contributed with their expertise to the reviewing process; without their help, the selection process would not have gone so smoothly.

All paper submissions to ASIACRYPT 2003 were received electronically using the Web-based submission software, which was provided by Chanathip Namprempre. The review software was kindly provided by Bart Preneel, Wim Moreau, and Joris Claessens. I would like to thank Chien-Pang Kuo for his help with the installation and with solving problems we had with the software. I am also very grateful to Yi-Zhen Lin for her great help in handling ASIACRYPT 2003 affairs.

Special thanks to Yuliang Zheng, who acted as an advisory member of the committee and provided advice based on his previous experience. I would also like to thank the chair of IACR, Andy Clark, who gave me valuable advice on all kinds of problems.

For financial support of the conference, we are very grateful to this year’s sponsors, including the National Science Council, the Ministry of Education, the Directorate-General of Telecommunications, R.O.C., Chunghwa Telecom Co.,
Ltd., the Institute for Information Industry, Computer & Communications Research Labs, ITRI, etc.

Finally, we would like to thank all other people who provided any assistance, and all the authors who submitted their papers to ASIACRYPT 2003, as well as all the participants from all over the world.

September 2003

Chi Sung Laih
ASIACRYPT 2003

Nov. 30 – Dec. 4, 2003, Taipei, Taiwan

Sponsored by the
International Association for Cryptologic Research (IACR)

in cooperation with the
Chinese Cryptography and Information Security Association,
National Cheng Kung University

General Chair

Chin Chen Chang, National Chung Cheng University, No. 160, Sanshing Tsuen, Minshiung Shiang, Chiai, Taiwan 621, Taiwan

Program Chair

Chi Sung Laih, Department of Electrical Engineering, National Cheng Kung University, Tainan 701, Taiwan
Program Committee

Masayuki Abe            NTT Laboratories, Japan
Josh Benaloh             Microsoft Research, USA
Colin Boyd               QUT, Australia
Christian Cachin         IBM Zurich, Switzerland
Ivan Damgaard            University of Aarhus, Denmark
Robert H. Deng           Mui Keng Terrace, Singapore
Stefan Dziembowski       University of Warsaw, Poland
Matthias Fitzi           U.C. Davis, USA
Marc Joye                Gemplus, France
Kwangjo Kim              ICU, Korea
Pil Joong Lee            POSTECH, Korea
Chin Laung Lei           National Taiwan University, Taiwan
Arjen K. Lenstra         Citibank, USA
Tsutomu Matsumoto        Yokohama National University, Japan
Phong Q. Nguyen           ENS, France
Eiji Okamoto             University of Tsukuba, Japan
Carles Padró              Technical University of Catalonia, Spain
Sihan Qing               Chinese Academy of Sciences, China
Vincent Rijmen            KU Leuven, Belgium
Bimal Roy                Indian Statistical Institute, India
Reihaneh Safavi-Naini    University of Wollongong, Australia
Shiuh Pyng Shieh         National Chiao Tung University, Taiwan
Nigel P. Smart           University of Bristol, UK
Stefan Wolf              University of Montreal, Canada
Guozhen Xiao             Xidan University, China
Moti Yung                Columbia University, USA

Local Organizing Committee

Jinn-Ke Jan            Hsiang-Ling Chen
Wen-Guey Tzeng        Hui-Wen Du
Shiuh-Jeng Wang       Chien-Pang Kuo
Tzong-Chen Wu         Yi-Zhen Lin

Sponsors

National Science Council, Taiwan
Ministry of Education, Taiwan
Directorate General of Telecommunications,
     Ministry of Transportation and Communications, Taiwan
Chunghwa Telecom Co., Ltd.
Institute for Information Industry
Computer & Communications Research Labs, ITRI
External Referees

Kazumaro Aoki
Feng Bao
Steve Babbage
Michael Backes
Paulo Barreto
Alexandre Benoit
Eli Biham
Eric Brier
Jan Camenisch
Dario Catalano
Sanjit Chatterjee
Jiun-Ming Chen
Xiaofeng Chen
Sanjeevan Chowdhury
Jean-Sébastien Coron
Coron Claude Crepeau
Paolo D’Arco
Simon Pierre Desrosiers
Yvo Desmedt
Jean-François Dhem
Jeroen Doumen
Dang Nguyen Duc
Orr Dunkelman
Ratna Dutta
Chun-I Fan
Serge Fehr
Jacques J.A. Fournier
Pierre-Alain Fouque
David Galindo
Steven Galbraith
Sugata Gangopadhyay
Juan Gonzalez
Louis Granboulan
D.J. Guan
Kishan Chand Gupta
Goichiro Hanaoka
Helena Handschuh
Sang Yun Han
Keith Harrison
Florian Hess
Javier Herranz
Martin Hirt
Yvonne Hitchcock
Fumitaka Hoshino
Thomas Holenstein
Min-Shiang Hwang
Ren-Junn Hwang
Shin-Jia Hwang
Yong Ho Hwang
Albert Jeng
Ji Hyun Jeong
Jorge Jim
Qingguang Ji
Jiménez Urroz Jorge
Wen-Shenq Juang
Naoki Kanayama
Rajeeva L. Karandikar
Chong Hee Kim
Ki Hyun Kim
Tetsutaro Kobayashi
Hartonu Kurnio
Tanja Lange
John Malone-Lee
C.H. Lin
Kai-Yung Lin
Chi-Jen Lu
E.H. Lu
Anna Lysyanskaya
Gwenaelle Martinet
Kazuto Matsuo
Wenbo Mao
Joydip Mitra
Sebastià Martín-Molleví
Yi Mu
Sourav Mukopadhyay
Mridul Nandi
Khanh Nguyen
Miyako Ohkubo
Daniel Page
Pascal Paillard
Dong Jin Park
Jae Hwan Park
In Kook Park
Joon Hah Park
Jacques Patarin
Duong Hieu Phan
Angela Piper
Krzysztof Pietrzak
Renato Renner
Kouichi Sakurai
Louis Salvail
Taiichi Saitoh
Palash Sarkar
Takakazu Satoh
Berry Schoenmakers
Jong Hoon Shin
Mahoro Shimura
Sang Gyou Sim
Leonie Simpson
Martijn Stam
Doug Stinson
Hung-Min Sun
Koutarou Suzuki
Willy Susilo
Alexei Tchoulkine
Dong To
Eran Tromer
Wen-Guey Tzeng
Shigenori Uchiyama
Frederik Vercauteren
Jorge Luis Villar
Samuel S. Wagstaff
Shiuh-Jeng Wang
Benne de Weger
Christopher Wolf
Hongjun Wu
Tzong-Chen Wu
Wen-ling Wu
Ching-Nung Yang
K. Yang
Yeon Hyeong Yang
Hsu-Chun Yen
Sung-Ming Yen
Her-Tyan Yeh
Yi-Shiung Yeh
Sung Ho Yoo
Young Tae Youn
Dae Hyun Yum
Fangguo Zhang
Wentao Zhang
Yuliang Zhen
Huafei Zhu
YongBin Zhou
Advances in Cryptology - ASIACRYPT 2003
9th International Conference on the Theory and
Application of Cryptology and Information Security,
Taipei, Taiwan, November 30 - December 4, 2003,
Proceedings
Laih, C.S. (Ed.)
2003, XIV, 550 p., Softcover
ISBN: 978-3-540-20592-0