

Springer

Berlin

Heidelberg

New York

Hong Kong

London

Milan

Paris

Tokyo

Chi Sung Laih (Ed.)

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



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editor

Chi Sung Laih
National Cheng Kung University
Department of Electrical Engineering
1 University Road, Tainan, Taiwan, R.O.C.
E-mail: laihs@eembox.ncku.edu.tw

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie;
detailed bibliographic data is available in the Internet at <<http://dnb.ddb.de>>.

CR Subject Classification (1998): E.3, D.4.6, K.6.5, F.2.1-2, C.2, J.1, G.2.2

ISSN 0302-9743

ISBN 3-540-20592-6 Springer-Verlag Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag is a part of Springer Science+Business Media

springeronline.com

© International Association for Cryptologic Research 2003
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik
Printed on acid-free paper SPIN: 10973370 06/3142 5 4 3 2 1 0

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

Table of Contents

Public Key Cryptography I

Chosen-Ciphertext Security without Redundancy	1
<i>Duong Hieu Phan and David Pointcheval</i>	
Some RSA-Based Encryption Schemes with Tight Security Reduction	19
<i>Kaoru Kurosawa and Tsuyoshi Takagi</i>	
A Simple Public-Key Cryptosystem with a Double Trapdoor Decryption Mechanism and Its Applications	37
<i>Emmanuel Bresson, Dario Catalano, and David Pointcheval</i>	

Number Theory I

Factoring Estimates for a 1024-Bit RSA Modulus	55
<i>Arjen Lenstra, Eran Tromer, Adi Shamir, Wil Kortsmit, Bruce Dodson, James Hughes, and Paul Leyland</i>	
Index Calculus Attack for Hyperelliptic Curves of Small Genus	75
<i>Nicolas Thériault</i>	

Efficient Implementations

Parallelizing Explicit Formula for Arithmetic in the Jacobian of Hyperelliptic Curves	93
<i>Pradeep Kumar Mishra and Palash Sarkar</i>	
Tate Pairing Implementation for Hyperelliptic Curves $y^2 = x^p - x + d$	111
<i>Iwan Duursma and Hyang-Sook Lee</i>	
The AGM- $X_0(N)$ Heegner Point Lifting Algorithm and Elliptic Curve Point Counting	124
<i>David R. Kohel</i>	

Key Management and Protocols

Key Management Schemes for Stateless Receivers Based on Time Varying Heterogeneous Logical Key Hierarchy	137
<i>Miodrag J. Mihaljević</i>	
Leakage-Resilient Authenticated Key Establishment Protocols	155
<i>SeongHan Shin, Kazukuni Kobara, and Hideki Imai</i>	
Untraceable Fair Network Payment Protocols with Off-Line TTP	173
<i>Chih-Hung Wang</i>	

Hash Functions

Incremental Multiset Hash Functions and Their Application
to Memory Integrity Checking 188
*Dwaine Clarke, Srinivas Devadas, Marten van Dijk, Blaise Gassend,
and G. Edward Suh*

New Parallel Domain Extenders for UOWHF 208
*Wonil Lee, Donghoon Chang, Sangjin Lee, Soohak Sung,
and Mridul Nandi*

Cryptanalysis of 3-Pass HAVAL 228
Bart Van Rompay, Alex Biryukov, Bart Preneel, and Joos Vandewalle

Group Signatures

Efficient Group Signatures without Trapdoors 246
Giuseppe Ateniese and Breno de Medeiros

Accumulating Composites and Improved Group Signing 269
Gene Tsudik and Shouhuai Xu

Almost Uniform Density of Power Residues
and the Provable Security of ESIGN 287
Tatsuaki Okamoto and Jacques Stern

Number Theory II

Rotations and Translations of Number Field Sieve Polynomials 302
Jason E. Gower

On Class Group Computations Using the Number Field Sieve 311
Mark L. Bauer and Safuat Hamdy

Invited Talk

The Secret and Beauty of Ancient Chinese Padlocks 326
Hong-Sen Yan and Hsing-Hui Huang

Block Ciphers

A Traceable Block Cipher 331
Olivier Billet and Henri Gilbert

A New Attack against Khazad 347
Frédéric Muller

Broadcast and Multicast

An Efficient Public Key Trace and Revoke Scheme Secure
against Adaptive Chosen Ciphertext Attack 359
Chong Hee Kim, Yong Ho Hwang, and Pil Joong Lee

Sequential Key Derivation Patterns for Broadcast Encryption and Key Predistribution Schemes	374
<i>Nuttapong Attrapadung, Kazukuni Kobara, and Hideki Imai</i>	

Foundations and Complexity Theory

Boneh <i>et al.</i> 's k -Element Aggregate Extraction Assumption Is Equivalent to the Diffie-Hellman Assumption	392
<i>Jean-Sebastien Coron and David Naccache</i>	
On Diophantine Complexity and Statistical Zero-Knowledge Arguments ..	398
<i>Helger Lipmaa</i>	
Verifiable Homomorphic Oblivious Transfer and Private Equality Test	416
<i>Helger Lipmaa</i>	

Public Key Cryptography II

Generalized Powering Functions and Their Application to Digital Signatures	434
<i>Hisayoshi Sato, Tsuyoshi Takagi, Satoru Tezuka, and Kazuo Takaragi</i>	
Certificateless Public Key Cryptography	452
<i>Sattam S. Al-Riyami and Kenneth G. Paterson</i>	
A Complete and Explicit Security Reduction Algorithm for RSA-Based Cryptosystems	474
<i>Kaoru Kurosawa, Katja Schmidt-Samoa, and Tsuyoshi Takagi</i>	
The Insecurity of Esign in Practical Implementations	492
<i>Pierre-Alain Fouque, Nick Howgrave-Graham, Gwenaëlle Martinet, and Guillaume Poupard</i>	

Digital Signature

Efficient One-Time Proxy Signatures	507
<i>Huaxiong Wang and Josef Pieprzyk</i>	
Universal Designated-Verifier Signatures	523
<i>Ron Steinfeld, Laurence Bull, Huaxiong Wang, and Josef Pieprzyk</i>	

Author Index	543
--------------------	-----