

Lecture Notes in Computer Science

Edited by G. Goos, J. Hartmanis and J. van Leeuwen

1716

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Singapore

Tokyo

Kwok Yan Lam Eiji Okamoto
Chaoping Xing (Eds.)

Advances in Cryptology – ASIACRYPT'99

International Conference on the Theory and
Application of Cryptology and Information Security
Singapore, November 14-18, 1999
Proceedings



Springer

Series Editors

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

Volume Editors

Kwok Yan Lam
National University of Singapore, School of Computing
2 Science Drive 2, Singapore 117543, Republic of Singapore
E-mail: lamky@comp.nus.edu.sg

Eiji Okamoto
School of Information Science
Japan Advanced Institute of Science and Technology
Asahidai 1-1, Tatsunokuchi, Nomi, Ishihawa, 923-1292, Japan
E-mail: okamoto@jaist.ac.jp

Chaoping Xing
Department of Mathematics, National University of Singapore
2 Science Drive 2, Singapore 117543, Republic of Singapore
E-mail: xingcp@math.nus.edu.sg

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Advances in cryptology : proceedings / ASIACRYPT '99, International Conference on the Theory and Applications of Cryptology and Information Security, Singapore, November 14 - 18, 1999. Kwok Yan Lam ... (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 1999
(Lecture notes in computer science ; Vol. 1716)
ISBN 3-540-66666-4

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

ISSN 0302-9743

ISBN 3-540-66666-4 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 Berlin Heidelberg 1999
Printed in Germany

Typesetting: Camera-ready by author
SPIN: 10704290 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

Preface

Asiacrypt'99 was held in Singapore on 14-18 November 1999. Asiacrypt is one of the major events in the cryptology research community. Asiacrypt'99, the fifth annual Asiacrypt conference, was sponsored by the Asiacrypt Steering Committee and the Centre for Systems Security of the National University of Singapore, and in cooperation with the International Association for Cryptology Research. As the Program Co-Chairs of Asiacrypt'99, we are extremely honored to organize this event, which showcases the state-of-the-art development of cryptology research at the conclusion of this millennium.

This year, a total of 96 research papers were submitted to Asiacrypt'99. The portfolio of country of origin of submissions serves as a good indicator of the international reputation of the conference. Countries from which submissions originated include: Australia, Belgium, China, Estonia, France, Germany, Greece, India, Iran, Japan, Korea, Norway, Russia, Saudi Arabia, Switzerland, Singapore, Spain, Taiwan, Thailand, The Netherlands, Turkey, Ukraine, UK, USA and Yugoslavia. Through a stringent refereeing process by the Program Committee, 31 papers of outstanding quality were accepted and are included in the conference proceedings. Accepted papers were authored by researchers from the following countries: Australia, Belgium, France, Germany, India, Japan, China, Singapore, Switzerland, Taiwan, The Netherlands, UK, and USA.

Thanks to the highly competent program committee, which was formed by a team of reputable and dedicated cryptology researchers, the refereeing process was conducted in a very professional and efficient manner. The refereeing schedule was closely adhered to by all program committee members but without compromising the quality of the refereeing work. The preparation of the Asiacrypt'99 program went smoothly as a result of the hard work of the program committee members. We would like to take this opportunity to acknowledge their professional work. The members of the program committee are: Colin Boyd, Michael Burmester, Chin-Chen Chang, Cunsheng Ding, Markus Jakobsson, Kwangjo Kim, Pil-Joong Lee, Ueli Maurer, Mitsuru Matsui, David Naccache, Harald Niederreiter, Andrew Odlyzko, Dingyi Pei, Jacques Stern, Guozhen Xiao, and Yuliang Zheng. We are also very grateful to the external referees who assisted the program committee in evaluating many papers (the list of external referees is included on a separate page).

We would like to express appreciation for the support of all researchers who submitted papers to Asiacrypt'99 and the cooperation of the authors of the accepted papers.

Last but not least, we would like to express our sincere gratitude to the organizing committee. Special thanks go to Chuk Yang Seng, Boon Chuan Tay, Huaxiong Wang, Chaoping Xing, and Huanhui Zhao.

Kwok-Yan Lam and Eiji Okamoto
Co-Chairs
Asiacrypt'99 Program Committee

Asiacrypt'99

November 14-18, Singapore

International Conference on the Theory and Applications
of Cryptology and Information Security

Sponsored by
The Asiacrypt Steering Committee

and
Centre for Systems Security
National University of Singapore

in cooperation with
The International Association for Cryptologic Research

Program Committee

Colin Boyd (Queensland University of Technology, Australia)
Michael Burmester (University of London, UK)
Chin-Chen Chang (National Chung Cheng University, Taiwan)
Cunsheng Ding (National University of Singapore, Singapore)
Markus Jakobsson (Bell Labs, USA)
Kwangjo Kim (Information and Communications University, Korea)
Kwok Yan Lam (Co-Chair, National University of Singapore, Singapore)
Pil-Joong Lee (Postech, Korea)
Ueli Maurer (ETH, Zurich)
Mitsuru Matsui (Mitsubishi Electronic Corp., Japan)
David Naccache (Gemplus, France)
Harald Niederreiter (Austrian Academy of Sciences, Austria)
Andrew Odlyzko (AT&T Research Lab, USA)
Eiji Okamoto (Co-Chair, JAIST, Japan)
Dingyi Pei (Chinese Academy of Science, China)
Jacques Stern (ENS, France)
Guozhen Xiao (Xidian University, China)
Yuliang Zheng (Monash University, Australia)

Organizing Committee

Chuk Yang Seng (National University of Singapore)
Boon Chuan Tay (National University of Singapore)
Huaxiong Wang (National University of Singapore)
Chaoping Xing (Chair, National University of Singapore)
Huanhui Zhao (National University of Singapore)

External Referees

| | | |
|-----------------------|-------------------|-------------------------|
| Giuseppe Ateniese | Kenji Koyama | Yasuyuki Sakai |
| Christophe Bidan | Kaoru Kurosawa | Kazue Sako |
| Simon R Blackburn | Mehdi-Laurent | Louis Salvail |
| Daniel Bleichenbacher | Phil MacKenzie | Hiroki Shizuya |
| Ning Cai | Natsume Matsuzaki | Natsume Tohru Sorimachi |
| Takeshi Chikazawa | Markus Michels | Julien Stern |
| Sebastien Coron | C. J. Mitchell | Makoto Sugita |
| Ronald Cramer | Atsuko Miyaji | Tada |
| Serge Fehr | David M'Raihi | Katsuyuki Takashima |
| Eiichiro Fujisaki | Junko Nakajima | Izu Tetsuya |
| Steven Galbraith | Pascal Paillier | Serge Vaudenay |
| Joachim Giesen | Choonsik Park | Huaxiong Wang |
| Pierre Girard | Sangjoon Park | Chao Ping Xing |
| Helena Handschuh | Sangwoo Park | Horosuke Yamamoto |
| Toshio Hasegawa | David Pointcheval | Bulent Yener |
| Toshiya Itoh | Mike Reiter | Huanhui Zhao |
| Tetsutaro Kobayashi | Ludovic Rousseau | |

Table of Contents

Invited Talk

| | |
|---|---|
| Modulus Search for Elliptic Curve Cryptosystems | 1 |
| <i>K. Koyama, Y. Tsuruoka, N. Kunihiro</i> | |

Asymmetric Key Cryptosystems

| | |
|---|----|
| On the Lai-Massey Scheme | 8 |
| <i>S. Vaudenay</i> | |
| On Cryptographically Secure Vectorial Boolean Functions | 20 |
| <i>T. Satoh, T. Iwata, K. Kurosawa</i> | |

Analysis

| | |
|---|----|
| Equivalent Keys of HPC | 29 |
| <i>C. D'Halluin, G. Bjnens, B. Preneel, V. Rijmen</i> | |
| Cryptanalysis of Five Rounds of CRYPTON Using Impossible Differentials | 43 |
| <i>H. Seki, T. Kaneko</i> | |
| Cryptanalysis of Two Cryptosystems Based on Group Actions | 52 |
| <i>S. R. Blackburn, S. D. Galbraith</i> | |
| Probabilistic Higher Order Differential Attack and Higher Order Bent Functions | 62 |
| <i>T. Iwata, K. Kurosawa</i> | |

Elliptic Curve Cryptosystems

| | |
|--|-----|
| Fast Algorithms for Elliptic Curve Cryptosystems over Binary Finite Field | 75 |
| <i>Y. F. Han, P.-C. Leong, P.-C. Tan, J. Zhang</i> | |
| Optimizing the Menezes-Okamoto-Vanstone (MOV) Algorithm for Non-supersingular Elliptic Curves | 86 |
| <i>J. Shikata, Y. Zheng, J. Suzuki, H. Imai</i> | |
| Speeding up the Discrete Log Computation on Curves with Automorphisms | 103 |
| <i>I. Duursma, P. Gaudry, F. Morain</i> | |
| ECC: Do We Need to Count? | 122 |
| <i>J.-S. Coron, H. Handschuh, D. Naccache</i> | |
| Elliptic Scalar Multiplication Using Point Halving | 135 |
| <i>E. W. Knudsen</i> | |

Public Key Cryptosystems

On the Design of RSA with Short Secret Exponent 150
H.-M. Sun, W.-C. Yang, C.-S. Laih

Efficient Public-Key Cryptosystems Provably Secure Against Active
 Adversaries 165
P. Paillier, D. Pointcheval

Adaptively-Secure Optimal-Resilience Proactive RSA 180
Y. Frankel, P. MacKenzie, M. Yung

Integers and Computation

Factorization of RSA-140 Using the Number Field Sieve 195
*S. Cavallar, B. Dodson, A. Lenstra, P. Leyland, W. Lioen,
 P. L. Montgomery, B. Murphy, H. te Riele, P. Zimmermann*

How to Prove that a Committed Number Is Prime 208
T. V. Le, K. Q. Nguyen, V. Varadharajan

Reducing Logarithms in Totally Non-maximal Imaginary Quadratic
 Orders to Logarithms in Finite Fields 219
D. Hühnlein, T. Takagi

General Adversaries in Unconditional Multi-party Computation 232
M. Fitzzi, M. Hirt, U. Maurer

Network Security

Approximation Hardness and Secure Communication in Broadcast
 Channels 247
Y. Desmedt, Y. Wang

Mix-Networks on Permutation Networks 258
M. Abe

Secure Communication in an Unknown Network Using Certificates 274
M. Burmester, Y. Desmedt

Random Number

Linear Complexity versus Pseudorandomness: On Beth and Dai’s Result . 288
Y. Wang

A Class of Explicit Perfect Multi-sequences 299
C. P. Xing, K. Y. Lam, Z. H. Wei

Cryptanalysis of LFSR-Encrypted Codes with Unknown Combining
 Function 306
S. Palit, B. K. Roy

Key Management

| | |
|--|-----|
| Doing More with Fewer Bits | 321 |
| <i>A. E. Brouwer, R. Pellikaan, E. R. Verheul</i> | |
| A Quick Group Key Distribution Scheme with “Entity Revocation” | 333 |
| <i>J. Anzai, N. Matsuzaki, T. Matsumoto</i> | |
| An Efficient Hierarchical Identity-Based Key-Sharing Method Resistant Against Collusion-Attacks | 348 |
| <i>G. Hanaoka, T. Nishioaka, Y. Zheng, H. Imai</i> | |
| Periodical Multi-secret Threshold Cryptosystems | 363 |
| <i>M. Numao</i> | |

Authentication

| | |
|---|-----|
| A Signature Scheme with Message Recovery as Secure as Discrete Logarithm | 378 |
| <i>M. Abe, T. Okamoto</i> | |
| A^3 -codes Under Collusion Attacks | 390 |
| <i>Y. J. Wang, R. Safavi-Naini</i> | |
| Broadcast Authentication in Group Communication | 399 |
| <i>R. Safavi-Naini, H. X. Wang</i> | |

| | |
|---------------------------|-----|
| Author Index | 413 |
|---------------------------|-----|