Lecture Notes in Computer Science 1716
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

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

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

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

Table of Contents

Public Key Cryptosystems

Integers and Computation

Network Security

Random Number

Key Management

Authentication