Lecture Notes in Computer Science 2964

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

Springer
Berlin
Heidelberg
New York
Hong Kong
London
Milan
Paris
Tokyo

Tatsuaki Okamoto (Ed.)

Topics in Cryptology – CT-RSA 2004

The Cryptographers' Track at the RSA Conference 2004
San Francisco, CA, USA, February 23-27, 2004
Proceedings

Springer

Volume Editor

Tatsuaki Okamoto
NTT Labs
Room 612A, 1-1 Hikarinooka, Yokosuka-shi, 239-0847 Japan
E-mail: okamoto@isl.ntt.co.jp

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, G.2.1, D.4.6, K.6.5, K.4.4, F.2.1-2, C.2, J.1

ISSN 0302-9743
ISBN 3-540-20996-4 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Protago-TeX-Production GmbH
Printed on acid-free paper SPIN: 10986998 06/3142 5 4 3 2 1 0

Preface

The Cryptographers' Track (CT-RSA) is a research conference within the RSA conference, the largest, regularly staged computer security event. CT-RSA 2004 was the fourth year of the Cryptographers' Track, and it is now an established venue for presenting practical research results related to cryptography and data security.

The conference received 77 submissions, and the program committee selected 28 of these for presentation. The program committee worked very hard to evaluate the papers with respect to quality, originality, and relevance to cryptography. Each paper was reviewed by at least three program committee members. Extended abstracts of the revised versions of these papers are in these proceedings. The program also included two invited lectures by Dan Boneh and Silvio Micali.

I am extremely grateful to the program committee members for their enormous investment of time and effort in the difficult and delicate process of review and selection. Many of them attended the program committee meeting during the Crypto 2003 conference at the University of California, Santa Barbara.

I gratefully acknowledge the help of a large number of colleagues who reviewed submissions in their area of expertise: Masayuki Abe, Toru Akishita, Kazumaro Aoki, Gildas Avoine, Joonsang Baek, Harald Baier, Alex Biryukov, Dario Catalano, Xiaofeng Chen, Benoit Chevallier-Mames, J.S. Coron, Christophe De Cannière, Alex Dent, J.-F. Dhem, Matthias Fitzi, Marc Fossorier, Steven Galbraith, Pierrick Gaudry, Craig Gentry, Shai Halevi, Helena Handschuh, Javier Herranz Sotoca, Doi Hiroshi, Thomas Holenstein, Tetsu Iwata, Tetsuya Izu, Miodrag J. Mihaljevic, Jacques J.A. Fournier, Markus Jakobsson, Dominic Jost, Pascal Junod, Naoki Kanayama, Hiroki Koga, Yuichi Komano, Hugo Krawczyk, Dennis Kuegler, Noboru Kunihiro, Eyal Kushilevitz, Yi Lu, Christoph Ludwig, Philip MacKenzie, Keith Martin, Kazuto Matsuo, Jean Monnerat, Shiho Moriai, Christophe Mourtel, Sean Murphy, David Naccache, Koh-Ichi Nagao, Anderson Nascimento, Wakaha Ogata, Kenji Ohkuma, Satomi Okazaki, Elisabeth Oswald, Daniel Page, Kenny Paterson, Krzysztof Pietrzak, Zulfikar Ramzan, Renato Renner, Taiichi Saito, Ryuichi Sakai, Kouichi Sakurai, Arthur Schmidt, Katja Schmidt-Samoa, Junji Shikata, Atsushi Shimbo, Johan Sjödin, Ron Steinfeld, Makoto Sugita, Masahiko Takenaka, Jin Tamura, Bogdan Warinschi, Kai Wirt, Xun Yi, and Rui Zhang.

Electronic submissions were made possible by the Web Review system of K.U. Leuven. I would like to thank Bart Preneel for his kind support. Special thanks to Thomas Herlea, who greatly supported us by operating the Web Review system customized for CT-RSA 2004.

In addition, I would like to thank Mami Yamaguchi for her support in the review process and in editing these proceedings.

I am specially grateful to Burt Kaliski and Ari Juels of RSA Laboratories for interfacing with the RSA conference.

I wish to thank all the authors, who by submitting papers made this conference possible, and the authors of accepted papers for their cooperation.

December 2003

Tatsuaki Okamoto
Program Chair
CT-RSA 2004

RSA Cryptographers' Track 2004

February 23–27, 2004, San Francisco, CA, USA

The RSA Conference 2004 was organized by RSA Security Inc. and its partner organizations around the world. The Cryptographers' Track was organized by RSA Laboratories.

Program Chair

Tatsuaki Okamoto, NTT Labs, Japan

Program Committee

Junhui Chao ..... Chuo U., Japan
Ronald Cramer ..... Aarhus U., Denmark
Alex Dent ..... Royal Holloway, UK
Anand Desai ..... NTT MCL, USA
Rosario Gennaro ..... IBM Research, USA
Goichiro Hanaoka ..... U. of Tokyo, Japan
Martin Hirt ..... ETH Zurich, Switzerland
Kwangjo Kim ..... ICU, Korea
Mitsuru Matsui ..... Mitsubishi Electric, Japan
Phong Nguyen ..... ENS, France
Kazuo Ohta ..... UEC, Japan
Pascal Paillier ..... Gemplus, France
David Pointcheval ..... ENS, France
Bart Preneel ..... K.U. Leuven, Belgium
Jean-Jacques Quisquater ..... UCL, Belgium
Tsuyoshi Takagi ..... TU Darmstadt, Germany
Serge Vaudenay ..... EPF Lausanne, Switzerland
Chung-Huang Yang ..... NKNU, Taiwan
Moti Yung ..... Columbia U., USA
Yuliang Zheng ..... UNC Charlotte, USA

Steering Committee

Marc Joye ..... Gemplus, France
Burt Kaliski ..... RSA Lab, USA
Bart Preneel ..... K.U. Leuven, Belgium
Ron Rivest ..... MIT, USA
Moti Yung ..... Columbia U., USA

Table of Contents

Side-Channel Attacks

Hardwares

Mode of Operations

Hash and Hash Chains

Visual Cryptography

Ellictic Curve Cryptosystems