

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

Series Editors

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

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

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

© Springer-Verlag Berlin Heidelberg 2004
Printed in Germany

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 Warinski, 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

Symmetric Encryption

Online Encryption Schemes: New Security Notions and Constructions ...	1
<i>Alexandra Boldyreva, Nut Taesombut</i>	
Related-Key Attacks on Triple-DES and DESX Variants	15
<i>Raphael C.-W. Phan</i>	
Design of AES Based on Dual Cipher and Composite Field	25
<i>Shee-Yau Wu, Shih-Chuan Lu, Chi Sung Lai</i>	
Periodic Properties of Counter Assisted Stream Ciphers	39
<i>Ove Scavenius, Martin Boesgaard, Thomas Pedersen, Jesper Christiansen, Vincent Rijmen</i>	
A Fast Correlation Attack via Unequal Error Correcting LDPC Codes ...	54
<i>Maneli Noorkami, Faramarz Fekri</i>	

Aymmetric Encryption

k -Resilient Identity-Based Encryption in the Standard Model	67
<i>Swee-Huay Heng, Kaoru Kurosawa</i>	
A Generic Construction for Intrusion-Resilient Public-Key Encryption ...	81
<i>Yevgeniy Dodis, Matt Franklin, Jonathan Katz, Atsuko Miyaji, Moti Yung</i>	

Digital Signatures

A Certificate-Based Signature Scheme	99
<i>Bo Gyeong Kang, Je Hong Park, Sang Geun Hahn</i>	
Identity Based Undeniable Signatures	112
<i>Benoît Libert, Jean-Jacques Quisquater</i>	
Compressing Rabin Signatures	126
<i>Daniel Bleichenbacher</i>	

Protocols

A Key Recovery System as Secure as Factoring	129
<i>Adam Young, Moti Yung</i>	
Server Assisted Signatures Revisited	143
<i>Kemal Bicakci, Nazife Baykal</i>	

Cryptanalysis of a Zero-Knowledge Identification Protocol of Eurocrypt '95	157
<i>Jean-Sébastien Coron, David Naccache</i>	
Universal Re-encryption for Mixnets	163
<i>Philippe Golle, Markus Jakobsson, Ari Juels, Paul Syverson</i>	
Bit String Commitment Reductions with a Non-zero Rate	179
<i>Anderson C.A. Nascimento, Joern Mueller-Quade, Hideki Imai</i>	
Improving Robustness of PGP Keyrings by Conflict Detection	194
<i>Qinglin Jiang, Douglas S. Reeves, Peng Ning</i>	

Side-Channel Attacks

Issues of Security with the Oswald-Aigner Exponentiation Algorithm ...	208
<i>Colin D. Walter</i>	
Hardware Countermeasures against DPA – A Statistical Analysis of Their Effectiveness	222
<i>Stefan Mangard</i>	
Self-Randomized Exponentiation Algorithms	236
<i>Benoît Chevallier-Mames</i>	

Hardware

Flexible Hardware Design for RSA and Elliptic Curve Cryptosystems	250
<i>Lejla Batina, Geke Bruin-Muurling, Siddika Berna Örs</i>	
High-Speed Modular Multiplication	264
<i>Wieland Fischer, Jean-Pierre Seifert</i>	
Yet Another Sieving Device	278
<i>Willi Geiselmann, Rainer Steinwandt</i>	

Mode of Operations

A Parallelizable Enciphering Mode	292
<i>Shai Halevi, Phillip Rogaway</i>	
Padding Oracle Attacks on the ISO CBC Mode Encryption Standard ...	305
<i>Kenneth G. Paterson, Arnold Yau</i>	

Hash and Hash Chains

A 1 Gbit/s Partially Unrolled Architecture of Hash Functions SHA-1 and SHA-512	324
<i>Roar Lien, Tim Grembowski, Kris Gaj</i>	
Fast Verification of Hash Chains	339
<i>Marc Fischlin</i>	

Visual Cryptography

Almost Ideal Contrast Visual Cryptography with Reversing	353
<i>Duong Quang Viet, Kaoru Kurosawa</i>	

Ellictic Curve Cryptosystems

Weak Fields for ECC	366
<i>Alfred Menezes, Edlyn Teske, Annegret Weng</i>	

Author Index	387
---------------------------	-----