Lecture Notes in Computer Science 3860

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Pointcheval (Ed.)

Topics in Cryptology – CT-RSA 2006

The Cryptographers' Track at the RSA Conference 2006
San Jose, CA, USA, February 13-17, 2006
Proceedings

Volume Editor

David Pointcheval
CNRS
ENS/DI
45, rue d'Ulm, 75005 Paris, France
E-mail: David.Pointcheval@ens.fr

Library of Congress Control Number: 2005937532

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-31033-9 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-31033-4 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11605805 06/3142 5 4 3 2 1 0

Preface

The RSA® Conference, with over 15,000 attendees, as well as over 225 sponsors and exhibitors, is the largest computer security event of the year. The Cryptographers' Track is one of the many parallel tracks. These proceedings contain the papers presented during the sixth edition. The tradition indeed started in 2001, and is by now well established: the Cryptographers' Track at the RSA Conference is among the major events in cryptography.

There were 72 submitted contributions, of which 22 were selected for presentation. They cover all aspects of cryptography (symmetric and asymmetric cryptography, constructions and attacks, new trends). In addition, the program includes two invited talks, by Xiaoyun Wang on "Cryptanalysis of Hash functions and Potential Dangers," and Philip MacKenzie on "Passwords Will Not Die: How Cryptography Can Help Deal with Them."

All the submissions were reviewed by at least three members of the Program Committee. I am very grateful to the 24 members for their hard and conscientious work. Many thanks to the 89 external reviewers:

Masayuki Abe
Kazumaro Aoki
Giuseppe Ateniese
Roberto Avanzi
Zuzana Beerliová
Olivier Billet
Alex Biryukov
Ian Blake
Colin Boyd
Eric Brier
Aniello Castiglione
Juyoung Cha
Aldar Chan
Liqun Chen
Kookrae Cho
Scott Contini
Paolo D'Arco
Jintai Ding
Christophe Doche
Orr Dunkelman
Matthias Fitzi
Pierre-Alain Fouque
Jacques J.A. Fournier
Kouichi Fujisaki
Eiichiro Fujisaki
Jun Furukawa
David Galindo
Shai Halevi
Helena Handschuh
Chris Heneghan
Thomas Holenstein
Fumitaka Hoshino
Yong Ho Hwang
Toshiyuki Isshiki
Ellen Jochemsz
Antoine Joux
Ari Juels
Charanjit Jutla
Aggelos Kiayias
Hiroaki Kikuchi
Tetsutarou Kobayashi
Tadayoshi Kohno
Hugo Krawczyk
Sandeep Kumar
Tanja Lange
Jung Wook Lee
Barbara Masucci
Alexander May
Miodrag Mihaljevic
Kazuhiko Minematsu
Fabian Monrose
Paul Montague
Steve Myers
David Naccache
Antonio Nicolosi
Satoshi Obana
Satomi Okazaki
Katsuyuki Okeya
Francis Olivier
Roger Oyono
Dan Page
Jung Hyung Park
Kun Peng
Krzysztof Pietrzak
Dominik Raub
Yasuyuki Sakai
Kouichi Sakurai
Werner Schindler
Jae Woo Seo
Jong Hoon Shin
Igor Shparlinski
Ron Steinfeld

Mike Szydlo
Yael Tauman Kalai
Isamu Teranishi
Toshio Tokita
Michael Tunstall
Frederik Vercauteren
Karine Villegas
Shabsi Walfish
Huaxiong Wang
Xiaofeng Wang
Bogdan Warinschi
Benne de Weger
Christopher Wolf
Alex Yampolskiy
Yeon Hyeong Yang
Yiqun Lisa Yin
Jeong Il Yoon

Note that these proceedings contain the revised versions of the selected papers. Since the revisions were not checked again before publication, the authors (and not the committee) bear full responsibility of the contents of their papers.

I also would like to thank Jacques Beigbeder for maintaining the submission and webreview servers, and Duong Hieu Phan for the fast set up of the review phase. The submission software was written by Chanathip Namprempre, and the webreview system by Wim Moreau and Joris Claessens. Many thanks to Burt Kaliski for interfacing with the RSA conference organizers, and to Alfred Hofmann at Springer for the production of this volume.

Finally, I wish to thank all the authors who submitted papers, and the authors of accepted papers for sending their final versions on time.

November 2005

David Pointcheval
Program Chair
CT-RSA 2006

Organization

RSA Conference 2006 was organized by RSA Security Inc. and its partner organizations around the world. The Cryptogaphers' Track at RSA Conference 2006 was organized by RSA Laboratories (http://www.rsasecurity.com).

Program Chair

David Pointcheval	CNRS/ENS, France

Program Committee

Eli Biham	Technion, Israel
Xavier Boyen	Voltage, USA
Benoît Chevallier-Mames	Gemplus, France
Anand Desai	NTT MCL, USA
Yvo Desmedt	University College London, UK
Yevgeniy Dodis	New York Univ., USA
Steven Galbraith	Royal Holloway University of London, UK
Rosario Gennaro	IBM T.J. Watson Research Center, USA
Henri Gilbert	France Telecom R&D, France
Martin Hirt	ETH Zurich, Switzerland
Nick Howgrave-Graham	NTRU Cryptosystems, USA
Markus Jakobsson	Indiana Univ., USA
Jonathan Katz	Univ. of Maryland, USA
Kwangjo Kim	ICU, Korea
Pil Joong Lee	POSTECH, Korea
Arjen Lenstra	Lucent Technologies, USA & TU Eindhoven, The Netherlands
Javier Lopez	Univ. of Malaga, Spain
Tatsuaki Okamoto	NTT, Japan
Josef Pieprzyk	Macquarie Univ., Australia
Guillaume Poupard	DCSSI Crypto Lab, France
Bart Preneel	K.U. Leuven, Belgium
Kazue Sako	NEC, Japan
Ivan Visconti	Univ. di Salerno, Italy
Moti Yung	RSA Labs & Columbia Univ., USA

Table of Contents

Attacks on AES

Cache Attacks and Countermeasures: The Case of AES
Dag Arne Osvik, Adi Shamir, Eran Tromer 1

Related-Key Impossible Differential Attacks on 8-Round AES-192
Eli Biham, Orr Dunkelman, Nathan Keller 21

Identification

Session Corruption Attack and Improvements on Encryption Based MT-Authenticators
Xiaojian Tian, Duncan S. Wong 34

Fair Identification
Omkant Pandey, Julien Cathalo, Jean-Jacques Quisquater 52

Algebra

Efficient Doubling on Genus 3 Curves over Binary Fields
Xinxin Fan, Thomas Wollinger, Yumin Wang 64

Another Look at Small RSA Exponents
M. Jason Hinek 82

Integrity

Collision-Resistant Usage of MD5 and SHA-1 Via Message Preprocessing
Michael Szydlo, Yiqun Lisa Yin 99

RFID-Tags for Anti-counterfeiting
Pim Tuyls, Lejla Batina 115

Public Key Encryption

A "Medium-Field" Multivariate Public-Key Encryption Scheme
Lih-Chung Wang, Bo-Yin Yang, Yuh-Hua Hu, Feipei Lai 132

A New Security Proof for Damgård's ElGamal
Kristian Gjøsteen 150

Signatures

Stand-Alone and Setup-Free Verifiably Committed Signatures
Huafei Zhu, Feng Bao 159

Toward the Fair Anonymous Signatures: Deniable Ring Signatures
Yuichi Komano, Kazuo Ohta, Atsushi Shimbo, Shinichi Kawamura 174

Side-Channel Attacks

Practical Second-Order DPA Attacks for Masked Smart Card Implementations of Block Ciphers
Elisabeth Oswald, Stefan Mangard, Christoph Herbst, Stefan Tillich 192

Higher Order Masking of the AES
Kai Schramm, Christof Paar 208

CCA Encryption

Chosen Ciphertext Secure Public Key Threshold Encryption Without Random Oracles
Dan Boneh, Xavier Boyen, Shai Halevi 226

How to Construct Multicast Cryptosystems Provably Secure Against Adaptive Chosen Ciphertext Attack
Yitao Duan, John Canny 244

Message Authentication

On the (Im)possibility of Blind Message Authentication Codes
Michel Abdalla, Chanathip Namprempre, Gregory Neven 262

An Optimal Non-interactive Message Authentication Protocol
Sylvain Pasini, Serge Vaudenay 280

Block Ciphers

A New Criterion for Nonlinearity of Block Ciphers
Orr Dunkelman, Nathan Keller 295

Block Ciphers Sensitive to Gröbner Basis Attacks
Johannes Buchmann, Andrei Pyshkin, Ralf-Philipp Weinmann 313

Multi-party Computation

Universally Composable Oblivious Transfer in the Multi-party Setting
Marc Fischlin 332

A Round and Communication Efficient Secure Ranking Protocol
Shaoquan Jiang, Guang Gong 350

Author Index 365