

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Marc Fischlin (Ed.)

Topics in Cryptology – CT-RSA 2009

The Cryptographers' Track at the RSA Conference 2009
San Francisco, CA, USA, April 20-24, 2009
Proceedings

Volume Editor

Marc Fischlin
TU Darmstadt, Theoretical Computer Science
Hochschulstrasse 10, 64289, Darmstadt, Germany
E-mail: marc.fischlin@gmail.com

Library of Congress Control Number: Applied for

CR Subject Classification (1998): E.3, D.4.6, K.6.5, C.2, K.4.4

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN	0302-9743
ISBN-10	3-642-00861-5 Springer Berlin Heidelberg New York
ISBN-13	978-3-642-00861-0 Springer 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. Violations are liable to prosecution under the German Copyright Law.

springer.com

© Springer-Verlag Berlin Heidelberg 2009
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12637942 06/3180 5 4 3 2 1 0

Preface

The 2009 RSA conference was held in San Francisco, USA, during April 20-24. The conference is devoted to security-related topics and, as part of this, hosts a distinguished track for cryptographic research. Since 2001 the proceedings of this Cryptographers' Track (CT-RSA) have been published in the series *Lecture Notes in Computer Science* of Springer.

The proceedings of CT-RSA 2009 contain 31 papers selected from 93 submissions, covering a wide variety of cryptographic areas. Each submission was anonymized for the reviewing process and was assigned to at least three of the 25 Program Committee members. Submissions co-authored by committee members were assigned to at least five members. After carefully considering more than 15,000 lines (more than 100,000 words) of reviews and online discussions, the committee selected 31 submissions for acceptance. The program also included an invited talk by Kenny Paterson entitled "Cryptography and Secure Channels."

I would like to thank all the authors who submitted papers. I am also indebted to the Program Committee members and all external reviewers for their voluntary work. The committee's work was tremendously simplified by Shai Halevi's submission software and his support. I would also like to thank the CT-RSA Steering Committee for electing me as Chair, and all the people from the RSA conference team for their support, especially Bree LaBollita.

January 2009

Marc Fischlin

CT-RSA 2009

RSA Conference 2009, Cryptographers' Track

Moscone Center, San Francisco, CA, USA

April 20–24, 2009

Program Chair

Marc Fischlin

Darmstadt University of Technology, Germany

Program Committee

Michel Abdalla

ENS & CNRS, France

Zuzana Beerliova-Trubiniowa

ETH Zurich, Switzerland

Alex Biryukov

University of Luxembourg, Luxembourg

Melissa Chase

Microsoft Research, USA

Alex Dent

Royal Holloway, UK

Nelly Fazio

City University of New York, USA

Juan Garay

AT&T Labs - Research, USA

Amir Herzberg

Bar-Ilan University, Israel

Dennis Hofheinz

CWI, The Netherlands

Nick Howgrave-Graham

NTRU Cryptosystems, USA

Stanislaw Jarecki

UC Irvine, USA

Marc Joye

Thomson, France

Alexander May

Bochum University, Germany

Jesper Buus Nielsen

University of Aarhus, Denmark

Giuseppe Persiano

University of Salerno, Italy

Josef Pieprzyk

Macquarie University, Australia

Vincent Rijmen

K.U. Leuven, Belgium, and Graz University of
Technology, Austria

Kazue Sako

NEC, Japan

Christian Schaffner

CWI, The Netherlands

Berry Schoenmakers

TU Eindhoven, The Netherlands

Willy Susilo

University of Wollongong, Australia

Pim Tuyls

Philips, The Netherlands

Jorge Villar

UPC Barcelona, Spain

Bogdan Warinschi

University of Bristol, UK

External Reviewers

Divesh Aggarwal	Dmitry Khovratovich	Thomas Popp
Toshinori Araki	Eike Kiltz	Dominik Raub
Giuseppe Ateniese	Ilya Kizhvatov	Thomas Ristenpart
Man Ho Au	Sandeep Kumar	Matt Robshaw
Roberto Avanzi	Alptekin Kupcu	Pankaj Rohatgi
Rikke Bendlin	Gregor Leander	Dries Schellekens
Johannes Blömer	Anja Lehmann	Martin Schlaeffer
Colin Boyd	Helger Lipmaa	Jacob Scholdt
Christoph de Canniere	Xiaomin Liu	Gautham Sekar
Srdjan Capkun	Jiqiang Lu	Haya Shulman
Rafik Chaabouni	Christoph Lucas	Nigel Smart
Donghoon Chang	Roel Maes	Martijn Stam
Sherman Chow	Mark Manulis	Ron Steinfeld
Christophe Clavier	Krystian Matusiewicz	Marc Stevens
Erik Dahmen	Sigurd Torkel Meldgaard	Bjoern Tackmann
Jean-François Dhem	Florian Mendel	Christophe Tartary
Orr Dunkelman	Nele Mentens	Tamir Tassa
Serge Fehr	Kazuhiko Mihematsu	Isamu Teranishi
Jun Feng	Gert Lassoe Mikkelsen	Stefano Tessaro
Pierre-Alain Fouque	Paul Morrissey	Elmar Tischhauser
Jakob Funder	Nicky Mouha	Nikos Triandopoulos
Steven Galbraith	Elke De Mulder	Michael Tunstall
Martin Geisler	Tomislav Nad	Mike Tunstall
Rosario Gennaro	Gregory Neven	Osman Ugus
Benedikt Gierlichs	Long Nguyen	Frederic Vercauteren
Aline Gouget	Phong Nguyen	Damien Vergnaud
Tim Gueneysu	Antonio Nicolosi	Peishun Wang
Carmiy Hazay	Ivica Nikolic	Benne de Weger
Martin Hirt	Svetla Nikova	Ralf-Philipp Weinmann
Qiong Huang	Satoshi Obana	Enav Weinreb
Xinyi Huang	Francis Olivier	Christopher Wolf
Sebastiaan Indesteege	Claudio Orlandi	Oliver Wuebbolt
Vicenzo Iovino	Elisabeth Oswald	Ng Ching Yu
Vincenzo Iovino	Dan Page	Tsz Hon Yuen
Toshiyuki Isshiki	Kenny Paterson	Hong-Sheng Zhou
Gene Itkis	Giuseppe Persiano	Vassilis Zikas
Emilia Kasper	Krzysztof Pietrzak	

Table of Contents

Identity-Based Encryption

Adaptive-ID Secure Revocable Identity-Based Encryption	1
<i>Benoît Libert and Damien Vergnaud</i>	
An Efficient Encapsulation Scheme from Near Collision Resistant Pseudorandom Generators and Its Application to IBE-to-PKE Transformations	16
<i>Takahiro Matsuda, Goichiro Hanaoka, Kanta Matsuura, and Hideki Imai</i>	
Universally Anonymous IBE Based on the Quadratic Residuosity Assumption	32
<i>Giuseppe Ateniese and Paolo Gasti</i>	

Protocol Analysis

Attacks on the DECT Authentication Mechanisms	48
<i>Stefan Lucks, Andreas Schuler, Erik Tews, Ralf-Philipp Weinmann, and Matthias Wenzel</i>	
Comparison-Based Key Exchange and the Security of the Numeric Comparison Mode in Bluetooth v2.1	66
<i>Andrew Y. Lindell</i>	

Two-Party Protocols

Key Insulation and Intrusion Resilience over a Public Channel	84
<i>Mihir Bellare, Shanshan Duan, and Adriana Palacio</i>	
Statistically Hiding Sets	100
<i>Manoj Prabhakaran and Rui Xue</i>	
Adaptively Secure Two-Party Computation with Erasures	117
<i>Andrew Y. Lindell</i>	

More Than Signatures

Short Redactable Signatures Using Random Trees	133
<i>Ee-Chien Chang, Chee Liang Lim, and Jia Xu</i>	
Divisible On-Line/Off-Line Signatures	148
<i>Chong-zhi Gao, Baodian Wei, Dongqing Xie, and Chunming Tang</i>	

Collisions for Hash Functions

Speeding up Collision Search for Byte-Oriented Hash Functions	164
<i>Dmitry Khovratovich, Alex Biryukov, and Ivica Nikolic</i>	
Hard and Easy Components of Collision Search in the Zémor-Tillich Hash Function: New Attacks and Reduced Variants with Equivalent Security	182
<i>Christophe Petit, Jean-Jacques Quisquater, Jean-Pierre Tillich, and Gilles Zémor</i>	

Cryptanalysis

A Statistical Saturation Attack against the Block Cipher PRESENT . . .	195
<i>B. Collard and F.-X. Standaert</i>	
Practical Attacks on Masked Hardware	211
<i>Thomas Popp, Mario Kirschbaum, and Stefan Mangard</i>	
Cryptanalysis of CTC2	226
<i>Orr Dunkelman and Nathan Keller</i>	

Alternative Encryption

A CCA2 Secure Public Key Encryption Scheme Based on the McEliece Assumptions in the Standard Model	240
<i>Rafael Dowsley, Jörn Müller-Quade, and Anderson C.A. Nascimento</i>	
Square, a New Multivariate Encryption Scheme	252
<i>Crystal Clough, John Baena, Jintai Ding, Bo-Yin Yang, and Ming-shing Chen</i>	

Privacy and Anonymity

Communication-Efficient Private Protocols for Longest Common Subsequence	265
<i>Matthew Franklin, Mark Gondree, and Payman Mohassel</i>	
Key-Private Proxy Re-encryption	279
<i>Giuseppe Ateniese, Karyn Benson, and Susan Hohenberger</i>	
Dynamic Universal Accumulators for DDH Groups and Their Application to Attribute-Based Anonymous Credential Systems	295
<i>Man Ho Au, Patrick P. Tsang, Willy Susilo, and Yi Mu</i>	

Efficiency Improvements

Practical Short Signature Batch Verification	309
<i>Anna Lisa Ferrara, Matthew Green, Susan Hohenberger, and Michael Østergaard Pedersen</i>	

Single-Layer Fractal Hash Chain Traversal with Almost Optimal Complexity	325
<i>Dae Hyun Yum, Jae Woo Seo, Sungwook Eom, and Pil Joong Lee</i>	

Recursive Double-Size Modular Multiplications without Extra Cost for Their Quotients	340
<i>Masayuki Yoshino, Katsuyuki Okeya, and Camille Vuillaume</i>	

Multi-Party Protocols

Constant-Rounds, Almost-Linear Bit-Decomposition of Secret Shared Values	357
<i>Tomas Toft</i>	
Local Sequentiality Does Not Help for Concurrent Composition	372
<i>Andrew Y. Lindell</i>	

Security of Encryption Schemes

Breaking and Repairing Damgård <i>et al.</i> Public Key Encryption Scheme with Non-interactive Opening	389
<i>David Galindo</i>	
Strengthening Security of RSA-OAEP	399
<i>Alexandra Boldyreva</i>	

Faults and Countermeasures

Fault Attacks on RSA Public Keys: <i>Left-To-Right</i> Implementations Are Also Vulnerable	414
<i>Alexandre Berzati, Cécile Canovas, Jean-Guillaume Dumas, and Louis Goubin</i>	
Fault Analysis Attack against an AES Prototype Chip Using RSL	429
<i>Kazuo Sakiyama, Tatsuya Yagi, and Kazuo Ohta</i>	

Countermeasures and Faults

Evaluation of the Detached Power Supply as Side-Channel Analysis Countermeasure for Passive UHF RFID Tags	444
<i>Thomas Plos</i>	
Securing RSA against Fault Analysis by Double Addition Chain Exponentiation	459
<i>Matthieu Rivain</i>	

Author Index	481
---------------------------	-----