

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

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

Orr Dunkelman (Ed.)

Topics in Cryptology – CT-RSA 2012

The Cryptographers' Track at the RSA Conference 2012
San Francisco, CA, USA, February 27 – March 2, 2012
Proceedings

Volume Editor

Orr Dunkelman
University of Haifa
Computer Science Department
31905 Haifa, Israel
E-mail: orrd@cs.haifa.ac.il

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-27953-9 e-ISBN 978-3-642-27954-6
DOI 10.1007/978-3-642-27954-6
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012930020

CR Subject Classification (1998): E.3, D.4.6, K.6.5, C.2, K.4.4, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2012

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.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

The RSA conference has been a major international event for information security experts since its introduction in 1991, including hundreds of vendors and thousands of attendees with 20 tracks of talks. Among these tracks of the RSA conference, the Cryptographers' Track stands out, offering a glimpse of academic research in the field of cryptography. Founded in 2001, the Cryptographers' Track has established its presence in the cryptographic community as a place where researchers meet with industry.

This year the RSA conference was held in San Francisco, California, from February 27 to March 2, 2012. The CT-RSA conference servers were hosted by the university of Haifa, Israel. This year, 113 submissions were received, a record number of submissions. Out of the 113 submissions, the Committee selected 27 papers for presentation (one of the accepted papers was withdrawn). It is my pleasure to thank all the authors of the submissions for the high-quality research. The review process was thorough (each submission received the attention of at least three reviewers and at least five for submissions involving a Committee member). The record number of submissions, as well as their high quality, made the selection process a challenging task, and I wish to thank all Committee members and the referees for their hard and dedicated work.

Two invited talks were given. The first was given by Ernie Brickell about "The Impact of Cryptography on Platform Security" and the second was given by Dmitry Khovratovich on "Attacks on Advanced Encryption Standard: Results and Perspectives."

The entire Committee, and especially myself, are extremely grateful to Thomas Baignères and Matthieu Finiasz for the iChair software, which facilitated a smooth and easy submission and review process. I would also like to thank Amy Szymanski who worked very hard to properly organize the conference this year.

December 2011

Orr Dunkelman

CT-RSA 2012

The 12th Cryptographers' Track — RSA 2012

San Francisco, California, USA, February 27–March 2, 2012

Program Chair

Orr Dunkelman

University of Haifa, Israel

Steering Committee

Marc Fischlin

Darmstadt University of Technology, Germany

Ari Juels

RSA Laboratories, USA

Aggelos Kiayias

University of Connecticut, USA

Josef Pieprzyk

Macquarie University, Australia

Ron Rivest

MIT, USA

Moti Yung

Google, USA

Program Committee

Adi Akavia

Weizmann Institute of Science, Israel

Giuseppe Ateniese

Sapienza-University of Rome, Italy and

Johns Hopkins University, USA

Jean-Philippe Aumasson

Nagravision, Switzerland

Roberto Avanzi

Ruhr-Universität Bochum, and

Qualcomm CDMA Technologies GmbH,

Germany

Josh Benaloh

Microsoft Research, USA

Alexandra Boldyreva

Georgia Institute of Technology, USA

Carlos Cid

Royal Holloway, University of London, UK

Ed Dawson

Queensland University of Technology, Australia

Alexander W. Dent

Royal Holloway, University of London, UK

Orr Dunkelman (Chair)

University of Haifa, Israel

Marc Fischlin

Darmstadt University of Technology, Germany

Pierre-Alain Fouque

École Normale Supérieure and INRIA, France

Kris Gaj

George Mason University, USA

Marc Joye

Technicolor, France

Jonathan Katz

University of Maryland, USA

Nathan Keller

Weizmann Institute of Science, Israel

John Kelsey

National Institute of Standards and Technology,
USA

Aggelos Kiayias

University of Connecticut, USA

Çetin Kaya Koç

Istanbul Şehir University, Turkey and

University of California, Santa Barbara, USA

Markulf Kohlweiss
Tanja Lange

Arjen Lenstra

Julio López
Tatsuaki Okamoto
Axel Poschmann
Bart Preneel
Kazue Sako
Martin Schläffer
Alice Silverberg
Nigel Smart
Nicolas Thériault
Bo-Yin Yang

Microsoft Research, UK
Technische Universiteit Eindhoven,
The Netherlands
École Polytechnique Fédérale de Lausanne,
Switzerland
University of Campinas, Brazil
NTT, Japan
Nanyang Technological University, Singapore
Katholieke Universiteit Leuven, Belgium
NEC, Japan
Graz University of Technology, Austria
University of California, Irvine, USA
Bristol University, UK
Universidad del Bio-Bio, Chile
Academia Sinica, Taiwan

Referees

Rodrigo Abarzúa
Shweta Agrawal
Elena Andreeva
Diego F. Aranha
Paul Baecher
Gregory Bard
Aurélié Bauer
David Bernhard
Daniel J. Bernstein
Joppe Bos
Christina Brzuska
Dario Catalano
Chien-Ning Chen
Lily Chen
Sherman Chow
Özgür Dagdelen
Emiliano De Cristofaro
Elke De Mulder
Jintai Ding
Laila El Aïmani
Junfeng Fan
Pooya Farshim
Sebastian Faust
Cedric Fournet
Georg Fuchsbauer
Jun Furukawa
Philippe Gaborit

Steven Galbraith
Nicolas Gama
Paolo Gasti
Martin Goldack
Conrado Gouvêa
Eric Guo
Carmit Hazay
Nadia Heninger
Jens Hermans
Clemens Heuberger
Michael Hutter
Yuval Ishai
Toshiyuki Ishiki
Dimitar Jetchev
Marcio Juliato
Marcelo Kaihara
Nikolaos Karvelas
Markus Kasper
Mario Kirschbaum
Thorsten Kleinjung
Virendra Kumar
Sebastian Kutzner
Jorn Lapon
Marc Le Guin
Kerstin Lemke-Rust
Tancrede Lepoint
Richard Lindner

Marco Macchetti
Alexander May
Florian Mendel
Daniele Micciancio
Oliver Mischke
Amir Moradi
Eduardo Morais
Andrew Moss
Debdeep Mukhopadhyay
Tomislav Nad
Samuel Neves
Juan Gonzalez Nieto
Maria Cristina Onete
Elisabeth Oswald
Roger Oyono
Pascal Paillier
Kenny Paterson
Souradyuti Paul
Ray Perlner
Ludovic Perret
Viet Pham
Thomas Plos
David Pointcheval
Elizabeth Quaglia
Christian Rechberger
Alfredo Rial

Thomas Ristenpart
Marcin Rogawski
Werner Schindler
Berry Schoenmakers
Dominique Schröder
Pouyan Sepehrdad
Igor Shparlinski
Rosemberg Silva
Joseph H. Silverman
Martijn Stam
Jaechul Sung
Qiang Tang
Isamu Teranishi
Mehdi Tibouchi
Michael Tunstall
Leif Uhsadel
Jeroen van de Graaf
Rajesh Velegati
Frederik Vercauteren
Bogdan Warinschi
William Whyte
Kenneth Wong
M.-E. Wu
Keita Xagawa
Panasayya Yalla
Ching-Hua Yu

Table of Contents

Side Channel Attacks I

Black-Box Side-Channel Attacks Highlight the Importance of Countermeasures: An Analysis of the Xilinx Virtex-4 and Virtex-5 Bitstream Encryption Mechanism	1
<i>Amir Moradi, Markus Kasper, and Christof Paar</i>	
Power Analysis of Atmel CryptoMemory – Recovering Keys from Secure EEPROMs	19
<i>Josep Balasch, Benedikt Gierlichs, Roel Verdult, Lejla Batina, and Ingrid Verbauwhede</i>	

Digital Signatures I

Short Transitive Signatures for Directed Trees	35
<i>Philippe Camacho and Alejandro Hevia</i>	
Short Attribute-Based Signatures for Threshold Predicates	51
<i>Javier Herranz, Fabien Laguillaumie, Benoît Libert, and Carla Ràfols</i>	

Public-Key Encryption I

Reducing the Key Size of Rainbow Using Non-commutative Rings	68
<i>Takanori Yasuda, Kowichi Sakurai, and Tsuyoshi Takagi</i>	
A Duality in Space Usage between Left-to-Right and Right-to-Left Exponentiation	84
<i>Colin D. Walter</i>	
Optimal Eta Pairing on Supersingular Genus-2 Binary Hyperelliptic Curves	98
<i>Diego F. Aranha, Jean-Luc Beuchat, Jérémie Detrey, and Nicolas Estibals</i>	

Cryptographic Protocols I

On the Joint Security of Encryption and Signature in EMV	116
<i>Jean Paul Degabriele, Anja Lehmann, Kenneth G. Paterson, Nigel P. Smart, and Mario Strefler</i>	
New Constructions of Efficient Simulation-Sound Commitments Using Encryption and Their Applications	136
<i>Eiichi Fujisaki</i>	

Secure Implementation Methods

A First-Order Leak-Free Masking Countermeasure	156
<i>Houssem Maghrebi, Emmanuel Prouff, Sylvain Guilley, and Jean-Luc Danger</i>	
Practical Realisation and Elimination of an ECC-Related Software Bug Attack.....	171
<i>Billy B. Brumley, Manuel Barbosa, Dan Page, and Frederik Vercauteren</i>	

Symmetric Key Primitives

A New Pseudorandom Generator from Collision-Resistant Hash Functions	187
<i>Alexandra Boldyreva and Virendra Kumar</i>	
PMAC with Parity: Minimizing the Query-Length Influence	203
<i>Kan Yasuda</i>	
Boomerang Attacks on Hash Function Using Auxiliary Differentials	215
<i>Gaëtan Leurent and Arnab Roy</i>	

Side Channel Attacks II

Localized Electromagnetic Analysis of Cryptographic Implementations	231
<i>Johann Heyszl, Stefan Mangard, Benedikt Heinz, Frederic Stumpf, and Georg Sigl</i>	
Towards Different Flavors of Combined Side Channel Attacks.....	245
<i>Youssef Souissi, Shivam Bhasin, Sylvain Guilley, Maxime Nassar, and Jean-Luc Danger</i>	

Digital Signatures II

Two-Dimensional Representation of Cover Free Families and Its Applications: Short Signatures and More	260
<i>Shota Yamada, Goichiro Hanaoka, and Noboru Kunihiro</i>	
Secure Computation, I/O-Efficient Algorithms and Distributed Signatures	278
<i>Ivan Damgård, Jonas Kölker, and Tomas Toft</i>	

Cryptographic Protocols II

Delegatable Homomorphic Encryption with Applications to Secure Outsourcing of Computation	296
<i>Manuel Barbosa and Pooya Farshim</i>	
Efficient RSA Key Generation and Threshold Paillier in the Two-Party Setting	313
<i>Carmit Hazay, Gert Læssøe Mikkelsen, Tal Rabin, and Tomas Toft</i>	

Public-Key Encryption II

Plaintext-Checkable Encryption	332
<i>Sébastien Canard, Georg Fuchsbaauer, Aline Gouget, and Fabien Laguillaumie</i>	
Generic Construction of Chosen Ciphertext Secure Proxy Re-Encryption	349
<i>Goichiro Hanaoka, Yutaka Kawai, Noboru Kunihiro, Takahiro Matsuda, Jian Weng, Rui Zhang, and Yunlei Zhao</i>	

Side Channel Attacks III

A New Difference Method for Side-Channel Analysis with High-Dimensional Leakage Models	365
<i>Annelie Heuser, Michael Kasper, Werner Schindler, and Marc Stöttinger</i>	
Getting More from PCA: First Results of Using Principal Component Analysis for Extensive Power Analysis	383
<i>Lejla Batina, Jip Hogenboom, and Jasper G.J. van Woudenberg</i>	

Secure Multiparty Computation

An Efficient Protocol for Oblivious DFA Evaluation and Applications...	398
<i>Payman Mohassel, Salman Niksefat, Saeed Sadeghian, and Babak Sadeghiyan</i>	
Secure Multi-Party Computation of Boolean Circuits with Applications to Privacy in On-Line Marketplaces	416
<i>Seung Geol Choi, Kyung-Wook Hwang, Jonathan Katz, Tal Malkin, and Dan Rubenstein</i>	

Author Index	433
---------------------------	-----