Lecture Notes in Computer Science 7178

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

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

Springer

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

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 Out of the 113 submissions, the Committee selected 27 papers for presentation (one of the accepted papers was withdrawn).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

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 Velegalati
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

Digital Signatures I

Public-Key Encryption I

Cryptographic Protocols I

Secure Implementation Methods

Symmetric Key Primitives

Side Channel Attacks II

Digital Signatures II

Cryptographic Protocols II

Public-Key Encryption II

Side Channel Attacks III

Secure Multiparty Computation