

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

Aggelos Kiayias (Ed.)

Topics in Cryptology – CT-RSA 2011

The Cryptographers' Track at the RSA Conference 2011
San Francisco, CA, USA, February 14-18, 2011
Proceedings

Volume Editor

Aggelos Kiayias
National and Kapodistrian University of Athens
Department of Informatics and Telecommunications
Panepistimiopolis, Ilisia, Athens 15784, Greece
E-mail: aggelos@kiayias.com

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-19073-5 e-ISBN 978-3-642-19074-2
DOI 10.1007/978-3-642-19074-2
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2010943110

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

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2011

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 was initiated in 1991 and is a major international event for cryptography and information security researchers as well as the industry related to these disciplines. It is an annual event that attracts hundreds of vendors and thousands of participants from industry and academia. Since 2001, the RSA conference has included the Cryptographers' Track (called the CT-RSA), which enables the forefront of cryptographic research to be presented within the formal program of the conference. CT-RSA has become a major publication venue for cryptographers worldwide.

This year the RSA conference was held in San Francisco, California, during February 14–18, 2011. The CT-RSA conference servers were running in the University of Athens, Greece, and we received 82 submissions out of which 3 were withdrawn. Every paper was reviewed by at least three committee members. The Program Committee members were also allowed to submit up to one paper for inclusion in the program. Such papers were reviewed by at least five committee members. The reviewing of the submissions proceeded in two stages: in the first stage papers were read individually by committee members without knowledge of other committee members' opinions. In the second stage, all reviews were made available to committee members and discussion through a Web bulletin board ensued. After a total of seven weeks the committee work concluded and a selection of 24 papers was made for inclusion in the conference program. In a small number of cases a final round of reviewing took place as some of the papers were accepted conditionally on specific changes that were requested by the Program Committee. The final revised versions of the accepted papers is what you will find in this volume.

We were very pleased this year to have three keynote talks included in the CT-RSA program. Dan Boneh from Stanford University gave a talk on computing with signed data. Dickie George of the Information Assurance Directorate at NSA spoke on NSA's role in the development of DES. Adi Shamir from the Weizmann Institute of Science gave a talk on the role of academia and industry in the design and analysis of DES. The talk also featured a mini-talk by Martin Hellman on that subject.

A number of people played key roles in the success of the conference this year. First and foremost I would like to thank the authors of all submitted papers; without their contributions the conference would not have been possible. Second, a special thanks is due to the members of the Program Committee and the subreviewers that invested a lot of their time in carefully reading the submitted papers and contributing to the discussion of each paper. The submission and review process was supported by the Web submission software written by Shai Halevi. I would also like to thank Bree LaBollita and Amy Szymanski, who worked very hard to properly organize the conference this year.

CT-RSA 2011

The 11th Cryptographers' Track – RSA 2011

San Francisco, California, USA
February 14–18, 2011

Program Chair

Aggelos Kiayias University of Athens, Greece

Steering Committee

Masayuki Abe	NTT, Japan
Ari Juels	RSA Laboratories, USA
Tal Malkin	Columbia University, USA
Josef Pieprzyk	Macquarie University, Australia
Ron Rivest	MIT, USA
Moti Yung	Google, USA

Program Committee

Giuseppe Ateniese	Johns Hopkins University, USA
Sasha Boldyreva	Georgia Tech, USA
Xavier Boyen	Université de Liège, Belgium
Christophe De Cannière	KU Leuven, Belgium
Jung Hee Cheon	Seoul National University, Korea
Joo Yeon Cho	Nokia, Denmark
Orr Dunkelman	Weizmann Institute, Israel
Steven Galbraith	University of Auckland, New Zealand
Craig Gentry	IBM Research, USA
Philippe Golle	Google, USA
Louis Goubin	Université de Versailles, France
Iftach Haitner	Tel Aviv University, Israel
Amir Herzberg	Bar Ilan University, Israel
Dennis Hofheinz	Karlsruhe University, Germany
Stanislaw Jarecki	UC Irvine, USA
Marc Joye	Technicolor, France
Ralf Küsters	University of Trier, Germany
Anna Lysyanskaya	Brown University, USA

VIII Organization

Alexander May	Ruhr University Bochum, Germany
Daniele Micciancio	UCSD, USA
Tal Moran	Harvard University, USA
Antonio Nicolosi	Stevens Institute of Technology, USA
Tatsuaki Okamoto	NTT, Japan
Rafail Ostrovsky	UCLA, USA
Josef Pieprzyk	Macquarie University, Australia
David Pointcheval	ENS, France
Berry Schoenmakers	TU Eindhoven, The Netherlands
Alice Silverberg	UC Irvine, USA
Martijn Stam	Royal Holloway, University of London, UK
François-Xavier Standaert	UCL, Belgium
Berk Sunar	WPI, USA
Nikos Triandopoulos	RSA Laboratories and Boston University, USA
Huaxiong Wang	NTU, Singapore
Bogdan Warinschi	University of Bristol, UK

External Reviewers

Onur Aciicmez	Dimitar Jetchev
Kahraman Akdemir	Deniz Karakoyunlu
Martin Albrecht	HongTae Kim
Gilad Asharov	Jihye Kim
Roberto Avanzi	Jinsoo Kim
Foteini Baldimtsi	Minkyu Kim
Lejla Batina	Taechan Kim
Carl Bosley	Mikkel Krøigård
Ran Canetti	Ranjit Kumaresan
Sherman S.M. Chow	Hyung Tae Lee
Léonard Dallot	Anja Lehmann
Yevgeniy Dodis	Helger Lipmaa
Gwenaël Doërr	David M'Raihi
Nelly Fazio	Ilya Mironov
Nicolas Gama	Daisuke Moriyama
Hossein Ghodosi	Erdinc Ozturk
Yossi Gilad	Charalampos Papamanthou
Choudary Gorantla	Olivier Pereira
Jian Guo	Ludovic Perret
Ghaith Hammouri	Christophe Petit
Malin Md Mokammel Haque	Nicolas Prigent
Mathias Herrmann	Tal Rabin
Susan Hohenberger	Francesco Regazzoni
Yin Hu	Andy Rupp
Xinyi Huang	Jae Hong Seo
Malika Izabachene	Elaine Shi

Haya Shulman
Radu Sion
Ron Steinfeld
Hung-Min Sun
Stefano Tessaro
Tomasz Truderung

Max Tuengerthal
Nicolas Veyrat-Charvillon
Andreas Vogt
Liang Feng Zhang
Hong-Sheng Zhou
Vassilis Zikas

Table of Contents

Secure Two-Party Computation

Secure Set Intersection with Untrusted Hardware Tokens	1
<i>Marc Fischlin, Benny Pinkas, Ahmad-Reza Sadeghi, Thomas Schneider, and Ivan Visconti</i>	
Efficient Secure Two-Party Exponentiation	17
<i>Ching-Hua Yu, Sherman S.M. Chow, Kai-Min Chung, and Feng-Hao Liu</i>	

Cryptographic Primitives

A General, Flexible and Efficient Proof of Inclusion and Exclusion	33
<i>Kun Peng</i>	
Non-interactive Confirmer Signatures	49
<i>Sherman S.M. Chow and Kristiyan Haralambiev</i>	
Communication-Efficient 2-Round Group Key Establishment from Pairings	65
<i>Kashi Neupane and Rainer Steinwandt</i>	

Side Channel Attacks

Defeating RSA Multiply-Always and Message Blinding Countermeasures	77
<i>Marc F. Witteman, Jasper G.J. van Woudenberg, and Federico Menarini</i>	
Cryptanalysis of CLEFIA Using Differential Methods with Cache Trace Patterns	89
<i>Chester Rebeiro and Debdeep Mukhopadhyay</i>	
Improving Differential Power Analysis by Elastic Alignment	104
<i>Jasper G.J. van Woudenberg, Marc F. Witteman, and Bram Bakker</i>	

Invited Talk

NSA's Role in the Development of DES	120
<i>Richard M. George</i>	

Authenticated Key Agreement

Designing Efficient Authenticated Key Exchange Resilient to Leakage of Ephemeral Secret Keys	121
<i>Atsushi Fujioka and Koutarou Suzuki</i>	
Contributory Password-Authenticated Group Key Exchange with Join Capability	142
<i>Michel Abdalla, Céline Chevalier, Louis Granboulan, and David Pointcheval</i>	

Proofs of Security

Ideal Key Derivation and Encryption in Simulation-Based Security	161
<i>Ralf Küsters and Max Tuengerthal</i>	
Beyond Provable Security Verifiable IND-CCA Security of OAEP	180
<i>Gilles Barthe, Benjamin Grégoire, Yassine Lakhnech, and Santiago Zanella Béguelin</i>	
(Second) Preimage Attacks on Step-Reduced RIPEMD/RIPEMD-128 with a New Local-Collision Approach	197
<i>Lei Wang, Yu Sasaki, Wataru Komatsubara, Kazuo Ohta, and Kazuo Sakiyama</i>	
MJH: A Faster Alternative to MDC-2	213
<i>Jooyoung Lee and Martijn Stam</i>	

Block Ciphers

Online Ciphers from Tweakable Blockciphers	237
<i>Phillip Rogaway and Haibin Zhang</i>	
Meet-in-the-Middle Attacks on Reduced-Round XTEA	250
<i>Gautham Sekar, Nicky Mouha, Vesselin Velichkov, and Bart Preneel</i>	

Security Notions

Expedient Non-malleability Notions for Hash Functions	268
<i>Paul Baecher, Marc Fischlin, and Dominique Schröder</i>	
Stronger Difficulty Notions for Client Puzzles and Denial-of-Service-Resistant Protocols	284
<i>Douglas Stebila, Lakshmi Kuppusamy, Jothi Rangasamy, Colin Boyd, and Juan Gonzalez Nieto</i>	

Public-Key Encryption

On Shortening Ciphertexts: New Constructions for Compact Public Key and Stateful Encryption Schemes	302
<i>Joonsang Baek, Cheng-Kang Chu, and Jianying Zhou</i>	
Better Key Sizes (and Attacks) for LWE-Based Encryption	319
<i>Richard Lindner and Chris Peikert</i>	

Crypto Tools and Parameters

Binary Huff Curves	340
<i>Julien Devigne and Marc Joye</i>	
A Variant of the F4 Algorithm	356
<i>Antoine Joux and Vanessa Vitse</i>	
Attribute-Based Signatures	376
<i>Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek</i>	

Digital Signatures

Sub-linear Size Traceable Ring Signatures without Random Oracles	393
<i>Euichiro Fujisaki</i>	
Author Index	417