Lecture Notes in Computer Science 6558

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

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

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conference servers were running in the University of Athens, Greece, and we received 82 submissions out of which 3 were withdrawn.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.

December 2010 Aggelos Kiayias

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

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

Cryptographic Primitives

Side Channel Attacks

Invited Talk

Authenticated Key Agreement

Proofs of Security

Block Ciphers

Security Notions

Public-Key Encryption

Crypto Tools and Parameters

Digital Signatures