Lecture Notes in Computer Science 5473

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

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

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

Table of Contents

Identity-Based Encryption

Protocol Analysis

Two-Party Protocols

More Than Signatures

Collisions for Hash Functions

Cryptanalysis

Alternative Encryption

Privacy and Anonymity

Effciency Improvements

Multi-Party Protocols

Security of Encryption Schemes

Faults and Countermeasures

Countermeasures and Faults