Shai Halevi (Ed.)

Advances in Cryptology – CRYPTO 2009

29th Annual International Cryptology Conference
Santa Barbara, CA, USA, August 16-20, 2009
Proceedings

Springer

Volume Editor

Shai Halevi
IBM Research
Hawthorne, NY, USA
E-mail: shaih@alum.mit.edu

Library of Congress Control Number: 2009931222

CR Subject Classification (1998): E.3, G.2.1, D.4.6, K.6.5, I.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-03355-5 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-03355-1 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12725359 06/3180 5 4 3 2 1 0

Preface

CRYPTO 2009, the 29th Annual International Cryptology Conference, was sponsored by the International Association for Cryptologic Research (IACR) in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy and the Computer Science Department of the University of California at Santa Barbara. The conference was held in Santa Barbara, California, during August 16–20, 2009, and John Black served as the General Chair. The Program Committee consisted of 29 members and two advisory members, whose names are listed on the next page, and I had the privilege of serving as the Program Chair.

The conference received 213 submissions. The Program Committee, aided by 217 external reviewers, reviewed all these submissions and discussed them in depth. After an intensive review period of 11 weeks, the committee accepted 40 of these submissions. Two pairs of submissions were merged, yielding a total of 38 papers in the technical program of the conference. These proceedings include the revised versions of the 38 papers that were presented at the conference. These revised papers were not subject to editorial review and the authors bear full responsibility for their contents. The best-paper award was given to the paper "Short Chosen-Prefix Collisions for MD5 and the Creation of a Rogue CA Certificate" by Stevens, Sotirov, Appelbaum, Lenstra, Molnar, Osvik, and de Weger.

The conference featured two invited lectures: one by Ed Felten and the other by Ueli Maurer. An abstract of Maurer's talk, titled "Abstraction in Cryptography," is included in these proceedings. The program also included a Rump Session, featuring short informal talks on recent results and work in progress.

I wish to thank all the authors who submitted their work to CRYPTO 2009. We received a large number of high-quality submissions, and even though we accepted more submissions than usual, there were still many good ones that we just could not fit in the program (but surely they will be published elsewhere). I am proud to be working in a field that consistently produces such strong results.

I owe a debt of gratitude to members of the Program Committee for their outstanding work. Evaluating such a large number of submissions in the short review period is very demanding, and the committee members contributed their knowledge and time to ensure that all submissions were reviewed in depth. Many thanks also to all the external reviewers who helped us with this task. I also thank Christof Paar, Christopher Wolf, and Alexander May for their help with organizing the PC meeting. And of course, I am thankful for the support that I received from all the members of the Cryptography group in IBM T.J. Watson Research Center: Rosario Gennaro, Craig Gentry, Charanjit Jutla, Jonathan Katz, Hugo Krawczyk, Tal Rabin, and Vinod Vaikuntanathan.

June 2009 Shai Halevi

CRYPTO 2009

The 29th International Cryptology Conference

August 16–20, 2009, Santa Barbara, California, USA

Sponsored by the
International Association for Cryptologic Research (IACR)

in cooperation with
IEEE Computer Society Technical Committee on Security and Privacy,
Computer Science Department, University of California, Santa Barbara

General Chair

John Black	University of Colorado at Boulder, USA

Program Chair

Shai Halevi	IBM Research, USA

Program Committee

Masayuki Abe	NTT, Japan
Dan Boneh	Stanford University, USA
Christophe De Cannière	Katholieke Universiteit Leuven, Belgium
Jean-Sébastien Coron	University of Luxembourg, Luxembourg
Marc Fischlin	Technische Universität Darmstadt, Germany
Steven Galbraith	Royal Holloway, UK
Shafi Goldwasser	MIT, USA and Weizmann Institute, Israel
Jens Groth	University College London, UK
Iftach Haitner	Microsoft Research, USA
Yuval Ishai	Technion, Israel and UCLA, USA
Marc Joye	Thomson R&D, France
Jonathan Katz	University of Maryland and IBM Research, USA
Kaoru Kurosawa	Ibaraki University, Japan
Anna Lysyanskaya	Brown University, USA
Phong Q. Nguyen	INRIA and ENS, France
Jesper Buus Nielsen	University of Aarhus, Denmark
Christof Paar	Ruhr-Universität Bochum, Germany
Rafael Pass	Cornell University, USA
Chris Peikert	SRI International, USA
Krzysztof Pietrzak	CWI Amsterdam, The Netherlands

Benny Pinkas	University of Haifa, Israel
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Renato Renner	ETH Zurich, Switzerland
Igor Shparlinski	Macquarie University, Australia
Adam Smith	Pennsylvania State University, USA
Eran Tromer	MIT, USA
Salil Vadhan	Harvard University, USA
Yiqun Lisa Yin	Independent Consultant, USA
Moti Yung	Google, USA

Advisory Members

David Wagner (CRYPTO 2008 Program Chair)	UC Berkley, USA
Tal Rabin (CRYPTO 2010 Program Chair)	IBM Research, USA

External Reviewers

Johan Aaberg	DongHoon Chang	Jun Furukawa
Michel Abdalla	Melissa Chase	Georg Fuchsbauer
Divesh Aggarwal	Sanjit Chatterjee	Philippe Gaborit
Omran Ahmadi	Jung Hee Cheon	Kris Gaj
Martin Albrecht	Céline Chevalier	David Galindo
Elena Andreeva	Benoît Chevallier-Mames	Nicolas Gama
Michael Anshel	Kai-Min Chung	Juan Garay
Kazumaro Aoki	Bertrand Chupeau	Pierrick Gaudry
Benny Applebaum	Carlos Cid	Rosario Gennaro
Tadashi Araragi	Roger Colbeck	Craig Gentry
Nuttapong Attrapadung	Robert Cordery	Benedikt Gierlichs
Dan Bailey	Oscar Dahlsten	Parikshit Gopalan
Aurélie Bauer	Ivan Damgård	Vipul Goyal
Georg Becker	Alex Dent	Jorge Guajardo
Zuzana Beerliova	Mario DiRaimondo	Venkatesan Guruswami
Amos Beimel	Claudia Diaz	Esther Haenggi
Mira Belenkiy	Jintai Ding	Mike Hamburg
Mihir Bellare	Yevgeniy Dodis	Goichiro Hanaoka
Côme Berbain	Dejan Dukaric	Helena Handschuh
Alex Biryukov	Orr Dunkelman	Darrel Hankerson
Andrey Bogdanov	Stefan Dziembowski	Carmit Hazay
Charles Bouillaguet	Klim Efremko	Swee-Huay Heng
Colin Boyd	Thomas Eisenbarth	Stefan Heyse
Xavier Boyen	Serge Fehr	Dennis Hofheinz
Zvika Brakerski	Vitaly Feldman	Susan Hohenberger
Ran Canetti	Dario Fiore	Thomas Holenstein
Claude Carlet	Pierre-Alain Fouque	Nick Howgrave-Graham
Nishanth Chandran	Eiichiro Fujisaki	Thomas Icart

Sebastiaan Indesteege
Tetsu Iwata
Stas Jarecki
Antoine Joux
Yael Tauman Kalai
Bhavana Kanukurthi
Markus Kaspar
Stefan Katzenbeisser
Yutaka Kawai
Aggelos Kiayias
Eike Kiltz
Markulf Kohlweiss
Gillat Kol
Yuichi Komano
Takeshi Koshiba
Noboru Kunihiro
Alptekin Küpçü
Anja Lehmann
Reynald Lercier
Gaëtan Leurent
Benoît Libert
Huijia Lin
Yehuda Lindell
Richard Lindner
Moses Liskov
Feng-Hao Liu
Vadim Lyubashevsky
Hiren Maharaj
Mohammad Mahmoody-Ghidary
Alexander May
Catherine Meadows
Alfred Menezes
Daniele Micciancio
Payman Mohassel
Tal Moran
Ciaran Mullan
David Naccache
Moni Naor
Gregory Neven
Gonzaler Nieto
Svetla Nikova
Ryo Nishimaki
Ryo Nojima
Martin Novotny
Koji Nuida
Adam O'Neill
Wakaha Ogata
Miyako Ohkubo
Cristina Onete
Claudio Orlandi
Carles Padro
Pascal Paillier
Omkant Pandey
David Parkes
Jacques Patarin
Olivier Pereira
Ludovic Perret
Christiane Peters
David Pointcheval
Carl Pomerance
Christopher Portmann
Manoj M Prabhakaran
Jörn Müller Quade
Tal Rabin
Dominik Raub
Christian Rechberger
Omer Reingold
Leonid Reyzin
Vincent Rijmen
Matthieu Rivain
Phillip Rogaway
Alon Rosen
Guy Rothblum
Andy Rupp
Amit Sahai
Palash Sarkar
Werner Schindler
Christian Schridde
Dominique Schröder
Michael Scott
Gil Segev
Nicolas Sendrier
abhi shelat
Emily Shen
Amir Shpilka
Thomas Shrimpton
Nigel Smart
François-Xavier Standaert
Cyril Stark
Damien Stehlé
Asgeir Steine
Ron Steinfeld
Marc Stevens
Makoto Sugita
Willy Susilo
Koutarou Suzuki
Bjoern Tackmann
Keisuke Tanaka
Stefano Tessaro
Marco Tomamichel
Nikos Triandopoulos
Wei-lung Tseng
Yasuyuki Tsukada
Jorge Jimenez Urroz
Alexander Ushakov
Berkant Ustaoglu
Vinod Vaikuntanathan
Mayank Varia
Maria Isabel Gonzalez Vasco
Muthu Venkitasubramaniam
Frederik Vercauteren
Damien Vergnaud
Thomas Vidick
Charlotte Vikkelsoe
Ivan Visconti
David Wagner
Shabsi Walfish
Huaxiong Wang
Bogdan Warinschi
Brent Waters
Hoeteck Wee
Enav Weinreb
Susanne Wetzel
Daniel Wichs
Christopher Wolf
Stefan Wolf
Hongjun Wu
David Xiao
Sergey Yekhanin
Hila Zarosim
Yunlei Zhao
Hong-Sheng Zhou
Vassilis Zikas

Table of Contents

Key Leakage

Hash-Function Cryptanalysis

Privacy and Anonymity

Interactive Proofs and Zero-Knowledge

Block-Cipher Cryptanalysis

Modes of Operation

Elliptic Curves

Cryptographic Hardness

Merkle Puzzles

Cryptography in the Physical World

Attacks on Signature Schemes

Invited Talk

Secret Sharing and Secure Computation

Cryptography and Game-Theory

Cryptography and Lattices

Identity-Based Encryption

Cryptographers' Toolbox