Lecture Notes in Computer Science 6841

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

Phillip Rogaway (Ed.)

Advances in Cryptology – CRYPTO 2011

31st Annual Cryptology Conference
Santa Barbara, CA, USA, August 14-18, 2011
Proceedings

Springer

Volume Editor

Phillip Rogaway
University of California
Department of Computer Science
Davis, CA 95616, USA
E-mail: rogaway@cs.ucdavis.edu

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-22791-2 e-ISBN 978-3-642-22792-9
DOI 10.1007/978-3-642-22792-9
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011932695

CR Subject Classification (1998): E.3, G.2.1, F.2.1-2, D.4.6, K.6.5, C.2, 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

CRYPTO 2011, the 31st Annual International Cryptology Conference, was held August 14–18 on the campus of the University of California, Santa Barbara. The event was sponsored by the International Association for Cryptologic Research (the IACR) in cooperation with the UCSB Computer Science Department and the IEEE Computer Society's Technical Committee on Security and Privacy.

We received 230 submissions, a new record, of which 43 were accepted for publication. With one pair of papers merged, these proceedings contain the revised versions of 42 papers.

There were also two invited talks. On Monday, Ron Rivest delivered the 2011 IACR Distinguished Lecture. On Wednesday, Roger Dingledine spoke about Tor, a widely used system for online anonymous communication. For Tuesday afternoon, traditionally left free, Shai Halevi graciously offered a three-hour tutorial on Fully Homomorphic Encryption. That evening, Dan Bernstein and Tanja Lange chaired the traditional rump session.

I have tried to assemble a technical program not only strong, but also balanced. Efforts in this direction included selection of a particularly large and broad Program Committee (PC), and a Call for Papers explicitly indicating receptiveness to cryptographic topics not routinely appearing at recent CRYPTOs. I encouraged PC members to focus on the positive aspects of submissions. When it came time to vote on second-round accepts, partitioning the papers into topical categories may also have helped.

For the Best Paper Award, the PC overwhelmingly selected "Computer-Aided Security Proofs for the Working Cryptographer," by Gilles Barthe, Benjamin Grégoire, Sylvain Heraud, and Santiago Zanella Béguelin. The Committee praised the work for its broad appeal, its connections to programming language, and its potential impact.

Papers were reviewed in the customary way, double-blind, with non-PC contributions generally receiving three or more reviews, and PC contributions getting four or more. I encouraged (anonymized) questions from PC members to authors, and ended up relaying several tens of such messages. Throughout the review process I tried to treat each submission as its authors' well-loved child, never as a three-digit number in need of categorization.

I would like to most sincerely thank the authors of submissions—both those who did and who did not get their papers in. Contributing research from all corners of the earth, it is the fine work of the authors that makes a conference like ours possible and worthwhile.

My deepest appreciation goes out to the PC. I find something wonderful and touching about so many busy and brilliant people putting in enormous amounts of time to perform so thankless and difficult a service. I was repeatedly impressed

by the dedication, integrity, knowledge, and extraordinary technical skills of so many on our PC. A list of PC members appears after this note.

The external reviewers play a key role in assessing the submissions, and are heartily thanked for their contribution. A list of external reviewers likewise appears after this note. My apologies in advance for any errors or omissions.

I would like to thank Tom Shrimpton, the General Chair, for working closely with me and handling the myriad of matters associated to putting on a great conference. Rei Safavi-Naini served double duty as both PC member and Junior Chair. I kept in close touch with John Benaloh, my IACR point of contact, who could always be counted on for timely information and feedback. I repeatedly got invaluable and frank advice from Tal Rabin, the CRYPTO 2010 Program Chair. Shai Halevi wrote, explained, and maintained the superb *websubrev* software on which we conducted our business. Alfred Hofmann and his colleagues at Springer saw to the timely production of this volume. Finally, Bongkotrattana Lailert afforded me the time and space needed to do this piece of work as well as I possibly could, smilingly accepting her and Banlu's exile to distant lands.

In closing, I would like to acknowledge something that all old-timers know, but which, as authors, we may sometimes fail to internalize: that there's an awful lot of randomness in the paper-selection process. Wonderful papers sometimes get rejected; mediocre papers sometimes get in. After serving as PC Chair I am more convinced than ever that it is fundamentally wrong to feel much of anything when any particular paper one submits does or doesn't make the cut. I hope that, over a period of years, important papers do get in, and do get recognized as well.

Serving as a CRYPTO Program Chair is a big job, and it can be a stressful one as well. Yet, somehow, I feel like I have grown more than gray hairs with this job, and am happy to have taken it on.

June 2011 Phillip Rogaway

CRYPTO 2011

The 31st Annual International Cryptology Conference

Santa Barbara, California, USA
August 14–18, 2011

Sponsored by the
International Association of Cryptologic Research (IACR)

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

General Chair

Thomas Shrimpton	Portland State University, USA

Program Chair

Phillip Rogaway	University of California, Davis, USA

Program Committee

Masayuki Abe	NTT, Japan
Michael Backes	Saarland University and MPI-SWS, Germany
Paulo Barreto	University of São Paulo, Brazil
Mihir Bellare	UC San Diego, USA
Alex Biryukov	University of Luxembourg
Dan Boneh	Stanford, USA
Jung Hee Cheon	Seoul National University, Korea
Jean-Sébastien Coron	University of Luxembourg
Marten van Dijk	RSA Labs and MIT/CSAIL, USA
Yevgeniy Dodis	New York University, USA
Orr Dunkelman	University of Haifa and Weizmann Institute, Israel
Serge Fehr	CWI, The Netherlands
Steven Galbraith	University of Auckland, New Zealand
Craig Gentry	IBM Research, USA
Louis Goubin	Université de Versailles, France
Vipul Goyal	Microsoft Research, India
Aggelos Kiayias	University of Connecticut, USA
Eike Kiltz	Ruhr-Universität Bochum, Germany
Anja Lehmann	IBM Zurich, Switzerland
Arjen Lenstra	EPFL, Switzerland
Stefan Mangard	Infineon Technologies, Germany

Program Committee (Continued)

Daniele Micciancio	UC San Diego, USA
Tal Moran	Harvard, USA
Chanathip Namprempre	Thammasat University, Thailand
Phong Nguyen	INRIA and ENS, France
Jesper Buus Nielsen	Aarhus University, Denmark
Rafael Pass	Cornell University, USA
Kenny Paterson	Royal Holloway, University of London, UK
Benny Pinkas	Bar Ilan University, Israel
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Leonid Reyzin	Boston University, USA
Vincent Rijmen	Katholieke Universiteit Leuven, Belgium and TU Graz, Austria
Rei Safavi-Naini	University of Calgary, Canada
Andre Scedrov	University of Pennsylvania, USA
Adam Smith	Pennsylvania State University, USA
François-Xavier Standaert	UCL, Belgium
Stefano Tessaro	UC San Diego, USA
Bogdan Warinschi	University of Bristol, UK
Hoeteck Wee	Queens College, CUNY, USA

Advisory Members

Tal Rabin (CRYPTO 2010 Program Chair)	IBM Research, USA
Rei Safavi-Naini (CRYPTO 2012 Program Chair)	University of Calgary, Canada

External Reviewers

Michel Abdalla	Alexandra Boldyreva	Kai-Min Chung
Divesh Aggarwal	Joppe Bos	Iwen Coisel
Hadi Ahmad	Charles Bouillaguet	Cas Cremers
Mohsen Alimomeni	Niek Bouman	Dana Dachman-Soled
Joel Alwen	Colin Boyd	Ivan Damgård
Elena Andreeva	Christina Brzuska	Jean Paul Degabriele
Kazumaro Aoki	Jan Camenisch	Cécile Delerablée
Gilad Asharov	Sebastien Canard	Ante Derek
Maxime Augier	Ran Canetti	Claus Diem
Paul Baecher	David Cash	Vivien Dubois
Kfir Barhum	Nishanth Chandran	Maria Dubovitskaya
Alexandre Berzati	Melissa Chase	Léo Ducas
Gaëtan Bisson	Hao Chen	Andrej Dujella
Bruno Blanchet	Alessandro Chiesa	Iwan Duursma
Andrey Bogdanov	Sherman S.M. Chow	Stefan Dziembowski

Pooya Farshim
Sebastian Faust
Matthieu Finiasz
Dario Fiore
Marc Fischlin
Pierre-Alain Fouque
David Freeman
Georg Fuchsbauer
Eiichiro Fujisaki
Jakob Funder
Martin Gagne
David Galindo
Sanjam Garg
Peter Gaži
Ran Gelles
Rosario Gennaro
Benedikt Gierlichs
Henri Gilbert
Michael Goodrich
Thomas Gross
Jeffrey Guarente
Kil-Chan Ha
Robbert de Haan
Iftach Haitner
Shai Halevi
Sean Hallgren
Mike Hamburg
Safuat Hamdy
Goichiro Hanaoka
Danny Harnik
Carmit Hazay
Jens Hermans
Mathias Herrmann
Florian Hess
Martin Hirt
Viet Tung Hoang
Dennis Hofheinz
Susan Hohenberger
Peter Hoyer
Pavel Hubacek
Andreas Hülsing
Sebastiaan Indesteege
Yuval Ishai
Tibor Jager
Abhishek Jain
Dimitar Jetchev
Shaoquan Jiang
Antoine Joux
Pascal Junod
Seny Kamara
Bhavana Kanukurthi
Alexandre Karlov
Shiva Kasiviswanathan
Jonathan Katz
Marcel Keller
Jihye Kim
Minkyu Kim
Myungsun Kim
Sungwook Kim
Thorsten Kleinjung
Robin Künzler
Ralf Küsters
Soonhak Kwon
Taekyoung Kwon
Mario Lamberger
Hyung Tae Lee
Younho Lee
Gaëtan Leurent
Allison Lewko
Benoit Libert
Changlu Lin
Huijia Lin
Yehuda Lindell
Satya Lokam
Adriana López-Alt
Carolin Lunemann
Anna Lysyanskaya
Vadim Lyubashevsky
Mohammad Mahmoody
Alexander May
Marcel Medwed
Sebastian Meiser
Florian Mendel
Bart Mennink
Alexander Meurer
Petros Mol
Hart Montogomery
Kirill Morozov
Elchanan Mossel
Serban Nacu
Tomislav Nad
Michael Naehrig
Arvind Narayanan
Gregory Neven
Ivica Nikolic
Ryo Nishimaki
Kobbi Nissim
Peter Sebastian Nordholt
Adam O'Neill
Miyako Ohkubo
Tatsuaki Okamoto
Elisabeth Oswald
Onur Ozen
Pascal Paillier
Paolo Palmieri
Omkant Pandey
Valerio Pastro
Jacques Patarin
Arpita Patra
Thomas Peeters
Serdar Pehlivanoglu
Chris Peikert
Robin Pemantle
Olivier Pereira
Edoardo Persichetti
Christophe Petit
Krzysztof Pietrzak
David Pointcheval
Manoj Prabhakaran
Ananth Raghunathan
Francesco Regazzoni
Oded Regev
Tzachy Reinman
Renato Renner
Thomas Ristenpart
Matthieu Rivain
Guy Rothblum
Yannis Rouselakis
Arnab Roy
Nashad Safa
Louis Salvail
Juraj Sarinay
Sumanta Sarkar
Yu Sasaki
Christian Schaffner

Martin Schläffer
Thomas Schneider
Dominique Schröder
Gil Segev
Jae Hong Seo
Yannick Seurin
Siamak Shahandashi
Elaine Shi
Thomas Shrimpton
Marcos A. Simplicio Jr
Thomas Sirvent
William E. Skeith III
Arkadii Slinko
Nigel Smart
Fang Song
Martijn Stam
John Steinberger
Marc Stevens
Gabor Tardos
Aris Tentes
Enrico Thomae
Mehdi Tibouchi
Elmar Tischhauser
Tomas Toft
Nikos Triandopoulos
Tomasz Truderung
Wei-lung Tseng
Ashraful Tuhin
Yevgeniy Vahlis
Vinod Vaikuntanathan
Kerem Varıcı
Damien Vergnaud
Ivan Visconti
Huaxiong Wang
Meiqin Wang
Yongge Wang
Brent Waters
Gaven Watson
Benne de Weger
Ralf-Philipp Weinmann
Daniel Wichs
Steve Williams
Christopher Wolf
Jürg Wullschleger
Andy Yao
Sarah Zakarias
Hong-Sheng Zhou
Angela Zottarel

Table of Contents

Randomness and Its Use

Computer-Assisted Cryptographic Proofs

Outsourcing and Delegating Computation

Symmetric Cryptanalysis and Constructions

Secure Computation

Leakage and Side Channels

Quantum Cryptography

Lattices and Knapsacks

Invited Talk

Public-Key Encryption

Symmetric Schemes

Signatures

Oblivious Transfer and Secret Sharing

Multivariate and Coding-Based Schemes