

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

Phillip Rogaway (Ed.)

Advances in Cryptology – CRYPTO 2011

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

Volume Editor

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

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

e-ISSN 1611-3349
e-ISBN 978-3-642-22792-9

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

© International Association for Cryptologic Research 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

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

Martin Schl affer
Thomas Schneider
Dominique Schr oder
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
J rg Wullschleger
Andy Yao
Sarah Zakarias
Hong-Sheng Zhou
Angela Zottarel

Table of Contents

Randomness and Its Use

| | |
|---|----|
| Leftover Hash Lemma, Revisited | 1 |
| <i>Boaz Barak, Yevgeniy Dodis, Hugo Krawczyk, Olivier Pereira, Krzysztof Pietrzak, François-Xavier Standaert, and Yu Yu</i> | |
| Random Oracle Reducibility | 21 |
| <i>Paul Baecher and Marc Fischlin</i> | |
| Time-Lock Puzzles in the Random Oracle Model | 39 |
| <i>Mohammad Mahmoody, Tal Moran, and Salil Vadhan</i> | |
| Physically Uncloneable Functions in the Universal Composition Framework | 51 |
| <i>Christina Brzuska, Marc Fischlin, Heike Schröder, and Stefan Katzenbeisser</i> | |

Computer-Assisted Cryptographic Proofs

| | |
|--|----|
| Computer-Aided Security Proofs for the Working Cryptographer | 71 |
| <i>Gilles Barthe, Benjamin Grégoire, Sylvain Héraud, and Santiago Zanella Béguelin</i> | |

Outsourcing and Delegating Computation

| | |
|--|-----|
| Optimal Verification of Operations on Dynamic Sets | 91 |
| <i>Charalampos Papamanthou, Roberto Tamassia, and Nikos Triandopoulos</i> | |
| Verifiable Delegation of Computation over Large Datasets | 111 |
| <i>Siavosh Benabbas, Rosario Gennaro, and Yevgeniy Vahlis</i> | |
| Secure Computation on the Web: Computing without Simultaneous Interaction | 132 |
| <i>Shai Halevi, Yehuda Lindell, and Benny Pinkas</i> | |
| Memory Delegation | 151 |
| <i>Kai-Min Chung, Yael Tauman Kalai, Feng-Hao Liu, and Ran Raz</i> | |

Symmetric Cryptanalysis and Constructions

| | |
|---|-----|
| Automatic Search of Attacks on Round-Reduced AES and Applications..... | 169 |
| <i>Charles Bouillaguet, Patrick Derbez, and Pierre-Alain Fouque</i> | |
| How to Improve Rebound Attacks..... | 188 |
| <i>María Naya-Plasencia</i> | |
| A Cryptanalysis of PRINTCIPHER: The Invariant Subspace Attack | 206 |
| <i>Gregor Leander, Mohamed Ahmed Abdelraheem, Hoda AlKhzaimi, and Erik Zenner</i> | |
| The PHOTON Family of Lightweight Hash Functions | 222 |
| <i>Jian Guo, Thomas Peyrin, and Axel Poschmann</i> | |

Secure Computation

| | |
|---|-----|
| Perfectly-Secure Multiplication for Any $t < n/3$ | 240 |
| <i>Gilad Asharov, Yehuda Lindell, and Tal Rabin</i> | |
| The IPS Compiler: Optimizations, Variants and Concrete Efficiency | 259 |
| <i>Yehuda Lindell, Eli Oxman, and Benny Pinkas</i> | |
| $1/p$ -Secure Multiparty Computation without Honest Majority and the Best of Both Worlds..... | 277 |
| <i>Amos Beimel, Yehuda Lindell, Eran Omri, and Ilan Orlov</i> | |

Leakage and Side Channels

| | |
|--|-----|
| Leakage-Resilient Zero Knowledge..... | 297 |
| <i>Sanjam Garg, Abhishek Jain, and Amit Sahai</i> | |
| A Comprehensive Evaluation of Mutual Information Analysis Using a Fair Evaluation Framework..... | 316 |
| <i>Carolyn Whitnall and Elisabeth Oswald</i> | |
| Key-Evolution Schemes Resilient to Space-Bounded Leakage..... | 335 |
| <i>Stefan Dziembowski, Tomasz Kazana, and Daniel Wichs</i> | |
| Generic Side-Channel Distinguishers: Improvements and Limitations ... | 354 |
| <i>Nicolas Veyrat-Charvillon and François-Xavier Standaert</i> | |
| Cryptography with Tamperable and Leaky Memory | 373 |
| <i>Yael Tauman Kalai, Bhavana Kanukurthi, and Amit Sahai</i> | |

Quantum Cryptography

| | |
|---|-----|
| Merkle Puzzles in a Quantum World | 391 |
| <i>Gilles Brassard, Peter Høyer, Kassem Kalach, Marc Kaplan, Sophie Laplante, and Louis Salvail</i> | |
| Classical Cryptographic Protocols in a Quantum World | 411 |
| <i>Sean Hallgren, Adam Smith, and Fang Song</i> | |
| Position-Based Quantum Cryptography: Impossibility and Constructions | 429 |
| <i>Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner</i> | |

Lattices and Knapsacks

| | |
|--|-----|
| Analyzing Blockwise Lattice Algorithms Using Dynamical Systems | 447 |
| <i>Guillaume Hanrot, Xavier Pujol, and Damien Stehlé</i> | |
| Pseudorandom Knapsacks and the Sample Complexity of LWE Search-to-Decision Reductions | 465 |
| <i>Daniele Micciancio and Petros Mol</i> | |

Invited Talk

| | |
|--|-----|
| Tor and Circumvention: Lessons Learned | 485 |
| <i>Roger Dingledine</i> | |

Public-Key Encryption

| | |
|---|-----|
| Fully Homomorphic Encryption over the Integers with Shorter Public Keys | 487 |
| <i>Jean-Sébastien Coron, Avradip Mandal, David Naccache, and Mehdi Tibouchi</i> | |
| Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages | 505 |
| <i>Zvika Brakerski and Vinod Vaikuntanathan</i> | |
| Bi-Deniable Public-Key Encryption | 525 |
| <i>Adam O’Neill, Chris Peikert, and Brent Waters</i> | |
| Better Security for Deterministic Public-Key Encryption: The Auxiliary-Input Setting | 543 |
| <i>Zvika Brakerski and Gil Segev</i> | |

Symmetric Schemes

| | |
|--|-----|
| The Collision Security of Tandem-DM in the Ideal Cipher Model | 561 |
| <i>Jooyoung Lee, Martijn Stam, and John Steinberger</i> | |
| Order-Preserving Encryption Revisited: Improved Security Analysis and Alternative Solutions | 578 |
| <i>Alexandra Boldyreva, Nathan Chenette, and Adam O’Neill</i> | |
| A New Variant of PMAC: Beyond the Birthday Bound | 596 |
| <i>Kan Yasuda</i> | |
| Authenticated and Misuse-Resistant Encryption of Key-Dependent Data | 610 |
| <i>Mihir Bellare and Sriram Keelveedhi</i> | |

Signatures

| | |
|--|-----|
| Round Optimal Blind Signatures | 630 |
| <i>Sanjam Garg, Vanishree Rao, Amit Sahai, Dominique Schröder, and Dominique Unruh</i> | |
| Optimal Structure-Preserving Signatures in Asymmetric Bilinear Groups | 649 |
| <i>Masayuki Abe, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo</i> | |

Oblivious Transfer and Secret Sharing

| | |
|--|-----|
| Constant-Rate Oblivious Transfer from Noisy Channels | 667 |
| <i>Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, Manoj Prabhakaran, Amit Sahai, and Jürg Wullschleger</i> | |
| The Torsion-Limit for Algebraic Function Fields and Its Application to Arithmetic Secret Sharing | 685 |
| <i>Ignacio Cascudo, Ronald Cramer, and Chaoping Xing</i> | |

Multivariate and Coding-Based Schemes

| | |
|--|-----|
| Public-Key Identification Schemes Based on Multivariate Quadratic Polynomials | 706 |
| <i>Koichi Sakumoto, Taizo Shirai, and Harunaga Hiwatari</i> | |
| Inverting HFE Systems Is Quasi-Polynomial for All Fields | 724 |
| <i>Jintai Ding and Timothy J. Hodges</i> | |

| | |
|---|-----|
| Smaller Decoding Exponents: Ball-Collision Decoding | 743 |
| <i>Daniel J. Bernstein, Tanja Lange, and Christiane Peters</i> | |
| McEliece and Niederreiter Cryptosystems That Resist Quantum Fourier Sampling Attacks | 761 |
| <i>Hang Dinh, Cristopher Moore, and Alexander Russell</i> | |
| Author Index | 781 |