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  
Tal Moran  
Chanathip Namprempre  
Phong Nguyen  
Jesper Buus Nielsen  
Rafael Pass  
Kenny Paterson  
Benny Pinkas  
Bart Preneel  
Leonid Reyzin  
Vincent Rijmen  
Rei Safavi-Naini  
Andre Scedrov  
Adam Smith  
François-Xavier Standaert  
Stefano Tessaro  
Bogdan Warinschi  
Hoeteck Wee  

Advisory Members

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

External Reviewers

Michel Abdalla  
Divesh Aggarwal  
Hadi Ahmad  
Mohsen Alimomeni  
Joel Alwen  
Elena Andreeva  
Kazumaro Aoki  
Gilad Asharov  
Maxime Augier  
Paul Baecher  
Kfir Barhum  
Alexandre Berzati  
Gaëtan Bisson  
Bruno Blanchet  
Andrey Bogdanov  
Alexandra Boldyreva  
Joppe Bos  
Charles Bouillaguet  
Niek Bouman  
Colin Boyd  
Christina Brzuska  
Jan Camenisch  
Sebastien Canard  
Ran Canetti  
David Cash  
Nishanth Chandran  
Melissa Chase  
Hao Chen  
Alessandro Chiesa  
Sherman S.M. Chow  
Kai-Min Chung  
Iwen Coisel  
Cas Cremers  
Dana Dachman-Soled  
Ivan Damgård  
Jean Paul Degabriele  
Cécile Delerablée  
Ante Derek  
Claus Diem  
Vivien Dubois  
Maria Dubovitskaya  
Léo Ducas  
Andrej Dujella  
Iwan Duursma  
Stefan Dziembowski
<table>
<thead>
<tr>
<th>Name</th>
<th>Name</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Martin Schläffer</td>
<td>John Steinberger</td>
<td>Ivan Visconti</td>
</tr>
<tr>
<td>Thomas Schneider</td>
<td>Marc Stevens</td>
<td>Huaxiong Wang</td>
</tr>
<tr>
<td>Dominique Schröder</td>
<td>Gabor Tardos</td>
<td>Meiqin Wang</td>
</tr>
<tr>
<td>Gil Segev</td>
<td>Aris Tentes</td>
<td>Yongge Wang</td>
</tr>
<tr>
<td>Jae Hong Seo</td>
<td>Enrico Thomae</td>
<td>Brent Waters</td>
</tr>
<tr>
<td>Yannick Seurin</td>
<td>Mehdi Tibouchi</td>
<td>Gaven Watson</td>
</tr>
<tr>
<td>Siamak Shahandashi</td>
<td>Elmar Tischhauser</td>
<td>Benne de Weger</td>
</tr>
<tr>
<td>Elaine Shi</td>
<td>Tomas Toft</td>
<td>Ralf-Philipp Weinmann</td>
</tr>
<tr>
<td>Thomas Shrimpton</td>
<td>Nikos Triandopoulos</td>
<td>Daniel Wichs</td>
</tr>
<tr>
<td>Marcos A. Simplicio Jr</td>
<td>Tomasz Truderung</td>
<td>Steve Williams</td>
</tr>
<tr>
<td>Thomas Sirvent</td>
<td>Wei-lung Tseng</td>
<td>Christopher Wolf</td>
</tr>
<tr>
<td>William E. Skeith III</td>
<td>Ashraful Tuhin</td>
<td>Jürg Wullschleger</td>
</tr>
<tr>
<td>Arkadii Slinko</td>
<td>Yevgeniy Vahlis</td>
<td>Andy Yao</td>
</tr>
<tr>
<td>Nigel Smart</td>
<td>Vinod Vaikuntanathan</td>
<td>Sarah Zakarias</td>
</tr>
<tr>
<td>Fang Song</td>
<td>Kerem Varci</td>
<td>Hong-Sheng Zhou</td>
</tr>
<tr>
<td>Martijn Stam</td>
<td>Damien Vergnaud</td>
<td>Angela Zottarel</td>
</tr>
</tbody>
</table>
# Table of Contents

## Randomness and Its Use

Leftover Hash Lemma, Revisited .................................................. 1  
   Boaz Barak, Yevgeniy Dodis, Hugo Krawczyk, Olivier Pereira,  
   Krzysztof Pietrzak, François-Xavier Standaert, and Yu Yu

Random Oracle Reducibility .......................................................... 21  
   Paul Baecher and Marc Fischlin

Time-Lock Puzzles in the Random Oracle Model ............................... 39  
   Mohammad Mahmoody, Tal Moran, and Salil Vadhan

Physically Uncloneable Functions in the Universal Composition  
Framework .......................................................................................... 51  
   Christina Brzuska, Marc Fischlin, Heike Schröder, and  
   Stefan Katzenbeisser

## Computer-Assisted Cryptographic Proofs

Computer-Aided Security Proofs for the Working Cryptographer ......... 71  
   Gilles Barthe, Benjamin Grégoire, Sylvain Heraud, and  
   Santiago Zanella Béguelin

## Outsourcing and Delegating Computation

Optimal Verification of Operations on Dynamic Sets ......................... 91  
   Charalampos Papamanthou, Roberto Tamassia, and  
   Nikos Triandopoulos

Verifiable Delegation of Computation over Large Datasets .................. 111  
   Siavosh Benabbas, Rosario Gennaro, and Yevgeniy Vahlis

Secure Computation on the Web: Computing without Simultaneous  
Interaction ......................................................................................... 132  
   Shai Halevi, Yehuda Lindell, and Benny Pinkas

Memory Delegation .............................................................................. 151  
   Kai-Min Chung, Yael Tauman Kalai, Feng-Hao Liu, and Ran Raz
Symmetric Cryptanalysis and Constructions

Automatic Search of Attacks on Round-Reduced AES and Applications.................................................... 169
  Charles Bouillaguet, Patrick Derbez, and Pierre-Alain Fouque

How to Improve Rebound Attacks........................................ 188
  María Naya-Plasencia

A Cryptanalysis of PRINTcipher: The Invariant Subspace Attack .... 206
  Gregor Leander, Mohamed Ahmed Abdelraheem,
  Hoda AlKhzaimi, and Erik Zenner

The PHOTON Family of Lightweight Hash Functions ................. 222
  Jian Guo, Thomas Peyrin, and Axel Poschmann

Secure Computation

Perfectly-Secure Multiplication for Any $t < n/3$ .................. 240
  Gilad Asharov, Yehuda Lindell, and Tal Rabin

The IPS Compiler: Optimizations, Variants and Concrete Efficiency .... 259
  Yehuda Lindell, Eli Ozman, and Benny Pinkas

1/p-Secure Multiparty Computation without Honest Majority and the Best of Both Worlds .................. 277
  Amos Beimel, Yehuda Lindell, Eran Omri, and Ilan Orlov

Leakage and Side Channels

Leakage-Resilient Zero Knowledge........................................ 297
  Sanjam Garg, Abhishek Jain, and Amit Sahai

A Comprehensive Evaluation of Mutual Information Analysis Using a Fair Evaluation Framework .................. 316
  Carolyn Whitnall and Elisabeth Oswald

Key-Evolution Schemes Resilient to Space-Bounded Leakage........ 335
  Stefan Dziembowski, Tomasz Kazana, and Daniel Wichs

Generic Side-Channel Distinguishers: Improvements and Limitations ... 354
  Nicolas Veyrat-Charvillon and François-Xavier Standaert

Cryptography with Tamperable and Leaky Memory ................... 373
  Yael Tauman Kalai, Bhavana Kanukurthi, and Amit Sahai
## Quantum Cryptography

Merkle Puzzles in a Quantum World .................................................. 391  
*Gilles Brassard, Peter Høyer, Kassem Kalach, Marc Kaplan, Sophie Laplante, and Louis Salvail*

Classical Cryptographic Protocols in a Quantum World ..................... 411  
*Sean Hallgren, Adam Smith, and Fang Song*

Position-Based Quantum Cryptography: Impossibility and Constructions .................................................. 429  
*Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner*

## Lattices and Knapsacks

Analyzing Blockwise Lattice Algorithms Using Dynamical Systems ...... 447  
*Guillaume Hanrot, Xavier Pujol, and Damien Stehlé*

Pseudorandom Knapsacks and the Sample Complexity of LWE  
Search-to-Decision Reductions ..................................................... 465  
*Daniele Micciancio and Petros Mol*

## Invited Talk

Tor and Circumvention: Lessons Learned ........................................ 485  
*Roger Dingledine*

## Public-Key Encryption

Fully Homomorphic Encryption over the Integers with Shorter Public Keys .......................................................... 487  
*Jean-Sébastien Coron, Avradip Mandal, David Naccache, and Mehdi Tibouchi*

Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages ............................................. 505  
*Zvika Brakerski and Vinod Vaikuntanathan*

Bi-Deniable Public-Key Encryption .................................................. 525  
*Adam O’Neill, Chris Peikert, and Brent Waters*

Better Security for Deterministic Public-Key Encryption: The Auxiliary-Input Setting ............................................. 543  
*Zvika Brakerski and Gil Segev*
Symmetric Schemes

The Collision Security of Tandem-DM in the Ideal Cipher Model
Jooyoung Lee, Martijn Stam, and John Steinberger

Order-Preserving Encryption Revisited: Improved Security Analysis and Alternative Solutions
Alexandra Boldyreva, Nathan Chenette, and Adam O’Neill

A New Variant of PMAC: Beyond the Birthday Bound
Kan Yasuda

Authenticated and Misuse-Resistant Encryption of Key-Dependent Data
Mihir Bellare and Sriram Keelveedhi

Signatures

Round Optimal Blind Signatures
Sanjam Garg, Vanishree Rao, Amit Sahai, Dominique Schröder, and Dominique Unruh

Optimal Structure-Preserving Signatures in Asymmetric Bilinear Groups
Masayuki Abe, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo

Oblivious Transfer and Secret Sharing

Constant-Rate Oblivious Transfer from Noisy Channels
Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, Manoj Prabhakaran, Amit Sahai, and Jürg Wullschleger

The Torsion-Limit for Algebraic Function Fields and Its Application to Arithmetic Secret Sharing
Ignacio Cascudo, Ronald Cramer, and Chaoping Xing

Multivariate and Coding-Based Schemes

Public-Key Identification Schemes Based on Multivariate Quadratic Polynomials
Koichi Sakumoto, Taizo Shirai, and Harunaga Hiwatari

Inverting HFE Systems Is Quasi-Polynomial for All Fields
Jintai Ding and Timothy J. Hodges
Smaller Decoding Exponents: Ball-Collision Decoding .......................... 743
  Daniel J. Bernstein, Tanja Lange, and Christiane Peters

McEliece and Niederreiter Cryptosystems That Resist Quantum Fourier Sampling Attacks .................................................... 761
  Hang Dinh, Cristopher Moore, and Alexander Russell

Author Index ................................................................. 781