Lecture Notes in Computer Science 4622

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

Alfred Menezes (Ed.)

# Advances in Cryptology – CRYPTO 2007

27th Annual International Cryptology Conference
Santa Barbara, CA, USA, August 19-23, 2007
Proceedings

Volume Editor

Alfred Menezes
University of Waterloo
Department of Combinatorics & Optimization
Waterloo, Ontario N2L 3G1, Canada
E-mail: ajmeneze@uwaterloo.ca

Library of Congress Control Number: 2007932207

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

ISSN 0302-9743
ISBN-10 3-540-74142-9 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-74142-8 Springer Berlin Heidelberg New York



Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12104802 06/3180 5 4 3 2 1 0

# Preface

CRYPTO 2007, the 27th 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, August 19-23 2007. CRYPTO 2007 was chaired by Markus Jakobsson, and I had the privilege of serving as the Program Chair.

The conference received 186 submissions. Each paper was assigned at least three reviewers, while submissions co-authored by Program Committee members were reviewed by at least five people. After 11 weeks of discussion and deliberation, the Program Committee, aided by reports from over 148 external reviewers, selected 33 papers for presentation. The authors of accepted papers had four weeks to prepare final versions for these proceedings. These revised papers were not subject to editorial review and the authors bear full responsibility for their contents.

The Committee identified the following three papers as the best papers: "Cryptography with Constant Input Locality" by Benny Applebaum, Yuval Ishai and Eyal Kushilevitz; "Practical Cryptanalysis of SFLASH" by Vivien Dubois, Pierre-Alain Fouque, Adi Shamir and Jacques Stern; and "Finding Small Roots of Bivariate Integer Polynomial Equations: A Direct Approach" by Jean-Sébastien Coron. The authors of these papers received invitations to submit full versions to the *Journal of Cryptology*. After a close vote, the Committee selected Benny Applebaum, Yuval Ishai and Eyal Kushilevitz, the authors of the first paper, as recipients of the Best Paper Award.

The conference featured invited lectures by Ross Anderson and Paul Kocher. Ross Anderson's paper "Information Security Economics – And Beyond" has been included in these proceedings.

There are many people who contributed to the success of CRYPTO 2007. I would like the thank the many authors from around the world for submitting their papers. I am deeply grateful to the Program Committee for their hard work, enthusiasm, and conscientious efforts to ensure that each paper received a thorough and fair review. Thanks also to the external reviewers, listed on the following pages, for contributing their time and expertise. It was a pleasure working with Markus Jakobsson and the staff at Springer. I am grateful to Andy Clark, Cynthia Dwork, Arjen Lenstra and Bart Preneel for their advice. Finally, I would like to thank Dan Bernstein for organizing a lively Rump Session, and Shai Halevi for developing and maintaining his most useful Web Submission and Review Software.

June 2007 Alfred Menezes

# CRYPTO 2007

August 19-23, 2007, 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

Markus Jakobsson, Indiana University, USA

## Program Chair

Alfred Menezes, University of Waterloo, Canada

## Program Committee

Amos Beimel ..... Ben-Gurion University, Israel
Alex Biryukov ..... University of Luxembourg, Luxembourg
Xavier Boyen ..... Voltage Security, USA
Yevgeniy Dodis ..... New York University, USA
Orr Dunkelman ..... Katholieke Universiteit Leuven, Belgium
Matt Franklin ..... UC Davis, USA
Steven Galbraith ..... Royal Holloway, University of London, UK
Rosario Gennaro ..... IBM Research, USA
Martin Hirt ..... ETH Zurich, Switzerland
Nick Howgrave-Graham ..... NTRU, USA
Antoine Joux ..... DGA and Université de Versailles, France
John Kelsey ..... NIST, USA
Neal Koblitz ..... University of Washington, USA
Kaoru Kurosawa ..... Ibaraki University, Japan
Tanja Lange ..... Technische Universiteit Eindhoven, Netherlands
Kristin Lauter ..... Microsoft Research, USA
Kenny Paterson ..... Royal Holloway, University of London, UK
David Pointcheval ..... École Normale Supérieure, France
Bart Preneel ..... Katholieke Universiteit Leuven, Belgium
Zulfikar Ramzan ..... Symantec, USA
Omer Reingold ..... Weizmann Institute of Science, Israel
Rei Safavi-Naini ..... University of Calgary, Canada
Amit Sahai ..... UCLA, USA
Palash Sarkar ..... Indian Statistical Institute, India
Nigel Smart ..... University of Bristol, UK
Adam Smith ..... UCLA and Penn State University, USA
Rainer Steinwandt ..... Florida Atlantic University, USA
Yiqun Lisa Yin ..... Independent Consultant, USA

## Advisory Members

Cynthia Dwork (CRYPTO 2006 Program Chair) . . . . . Microsoft, USA
David Wagner (CRYPTO 2008 Program Chair) . . . . . UC Berkeley, USA

## External Reviewers

Michel Abdalla
Masayuki Abe
Joel Alwen
Elena Andreeva
Tomoyuki Asano
Nuttapong Attrapadung
Georges Baatz
Lejla Batina
Aurélie Bauer
Zuzana Beerliová
Josh Benaloh
Waldyr Benits Jr.
Daniel J. Bernstein
Jens-Matthias Bohli
Alexandra Boldyreva
Carl Bosley
Colin Boyd
Daniel R.L. Brown
Ran Canetti
David Cash
Dario Catalano
Denis Charles
Lily Chen
Benoît Chevallier-Mames
Sherman Chow
Carlos Cid
Henry Cohn
Scott Contini
Jason Crampton
Joan Daemen
Quynh Dang
Cécile Delerablée
Alex Dent
Zeev Dvir
Morris Dworkin
Phil Eagle
Pooya Farshim
Marc Fischlin
Matthias Fitzi
Georg Fuschbauer
Nicolas Gama
Joachim von zur Gathen
Willi Geiselmann
Craig Gentry
Marc Girault
Mark Gondree
Jens Groth
Manabu Hagiwara
Iftach Haitner
Shai Halevi
Goichiro Hanaoka
Kristiyan Haralambiev
Danny Harnik
Swee-Huay Heng
Shoichi Hirose
Katrin Hoepper
Susan Hohenberger
Thomas Holenstein
Emeline Hufschmitt
Russell Impagliazzo
Yuval Ishai
Tetsu Iwata
Malika Izabachène
Shaoquan Jiang
Charanjit Jutla
Jonathan Katz
Aggelos Kiayias
Eike Kiltz
Darko Kirovski
Lars Knudsen
Yuichi Komano
Hugo Krawczyk
Sébastien Kunz-Jacques
Brian LaMacchia
Gaëtan Leurent
Yehuda Lindell
Joseph Liu
Stefan Lucks
Norbert Lütkenhaus
Philip MacKenzie
Tal Malkin
Keith Martin
Alexander Maximov
David Mireles
Ilya Mironov
Anton Mityagin
Payman Mohassel
David Molnar
Tal Moran
Moni Naor
Ashwin Nayak
Adam O'Neill
Gregory Neven
Phong Nguyen
Jesper Buus Nielsen
Kobbi Nissim
Wakaha Ogata
Rafail Ostrovsky
Elisabeth Oswald
Rafael Pass
Maura Paterson
Olivier Pereira
Giuseppe Persiano
Duong Hieu Phan
Benny Pinkas
Angela Piper
Alf van der Poorten
Manoj Prabhakaran
Bartosz Przydatek
Prashant Puniya
Tal Rabin
Dominik Raub
Oded Regev
Jean-René Reinhard

Renato Renner
Reza Reyhanitabar
Alon Rosen
Guy Rothblum
Jacob Schuldt
Gil Segev
Siamak Shahandashti
Jamshid Shokrollahi
Igor Shparlinski
Tom Shrimpton
Andrey Sidorenko
Johan Sjödin
Till Stegers
Christine Swart
Mike Szydlo
Stefano Tessaro
Jacques Traoré
José Villegas
Ivan Visconti
Shabsi Walfish
Huaxiong Wang
Bogdan Warinschi
Brent Waters
Enav Weinreb
Daniel Wichs
Douglas Wikström
Christopher Wolf
Stefan Wolf
Ronald de Wolf
David Woodruff
Hongjun Wu
Qianhong Wu
Jürg Wullschleger
Vassilis Zikas

# Table of Contents


## I Cryptanalysis I

Practical Cryptanalysis of SFLASH . . . . . 1
*Vivien Dubois, Pierre-Alain Fouque, Adi Shamir, and Jacques Stern*

Full Key-Recovery Attacks on HMAC/NMAC-MD4 and NMAC-MD5 . . . . . 13
*Pierre-Alain Fouque, Gaëtan Leurent, and Phong Q. Nguyen*

## II Secure Searching

How Should We Solve Search Problems Privately? . . . . . 31
*Amos Beimel, Tal Malkin, Kobbi Nissim, and Enav Weinreb*

Public Key Encryption That Allows PIR Queries . . . . . 50
*Dan Boneh, Eyal Kushilevitz, Rafail Ostrovsky, and William E. Skeith III*

## III Invited Talk

Information Security Economics – and Beyond . . . . . 68
*Ross Anderson and Tyler Moore*

## IV Theory I

Cryptography with Constant Input Locality . . . . . 92
*Benny Applebaum, Yuval Ishai, and Eyal Kushilevitz*

Universally-Composable Two-Party Computation in Two Rounds . . . . . 111
*Omer Horvitz and Jonathan Katz*

Indistinguishability Amplification . . . . . 130
*Ueli Maurer, Krzysztof Pietrzak, and Renato Renner*

## V Lattices

A Hybrid Lattice-Reduction and Meet-in-the-Middle Attack Against NTRU . . . . . 150
*Nick Howgrave-Graham*

Improved Analysis of Kannan's Shortest Lattice Vector Algorithm (Extended Abstract) . . . . . 170
*Guillaume Hanrot and Damien Stehlé*

## VI Random Oracles

Domain Extension of Public Random Functions: Beyond the Birthday Barrier . . . . . 187
*Ueli Maurer and Stefano Tessaro*

Random Oracles and Auxiliary Input . . . . . 205
*Dominique Unruh*

## VII Hash Functions

Security-Amplifying Combiners for Collision-Resistant Hash Functions . . . . . 224
*Marc Fischlin and Anja Lehmann*

Hash Functions and the (Amplified) Boomerang Attack . . . . . 244
*Antoine Joux and Thomas Peyrin*

Amplifying Collision Resistance: A Complexity-Theoretic Treatment . . . 264
*Ran Canetti, Ron Rivest, Madhu Sudan, Luca Trevisan, Salil Vadhan, and Hoeteck Wee*

## VIII Theory II

How Many Oblivious Transfers Are Needed for Secure Multiparty Computation? . . . . . 284
*Danny Harnik, Yuval Ishai, and Eyal Kushilevitz*

Simulatable VRFs with Applications to Multi-theorem NIZK . . . . . 303
*Melissa Chase and Anna Lysyanskaya*

Cryptography in the Multi-string Model . . . . . 323
*Jens Groth and Rafail Ostrovsky*

## IX Quantum Cryptography

Secure Identification and QKD in the Bounded-Quantum-Storage Model . . . . . 342
*Ivan B. Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner*

A Tight High-Order Entropic Quantum Uncertainty Relation with Applications . . . . . 360
*Ivan B. Damgård, Serge Fehr, Renato Renner, Louis Salvail, and Christian Schaffner*

## X Cryptanalysis II

Finding Small Roots of Bivariate Integer Polynomial Equations: A Direct Approach . . . . . 379
*Jean-Sébastien Coron*

A Polynomial Time Attack on RSA with Private CRT-Exponents Smaller Than $N^{0.073}$ . . . . . 395
*Ellen Jochemsz and Alexander May*

## XI Encryption

Invertible Universal Hashing and the TET Encryption Mode . . . . . 412
*Shai Halevi*

Reducing Trust in the PKG in Identity Based Cryptosystems . . . . . 430
*Vipul Goyal*

Pirate Evolution: How to Make the Most of Your Traitor Keys . . . . . 448
*Aggelos Kiayias and Serdar Pehlivanoglu*

## XII Protocol Analysis

A Security Analysis of the NIST SP 800-90 Elliptic Curve Random Number Generator . . . . . 466
*Daniel R.L. Brown and Kristian Gjøsteen*

A Generalization of DDH with Applications to Protocol Analysis and Computational Soundness . . . . . 482
*Emmanuel Bresson, Yassine Lakhnech, Laurent Mazaré, and Bogdan Warinschi*

Chernoff-Type Direct Product Theorems . . . . . 500
*Russell Impagliazzo, Ragesh Jaiswal, and Valentine Kabanets*

## XIII Public-Key Encryption

Rerandomizable RCCA Encryption . . . . . 517
*Manoj Prabhakaran and Mike Rosulek*

Deterministic and Efficiently Searchable Encryption ..... 535
*Mihir Bellare, Alexandra Boldyreva, and Adam O'Neill*

Secure Hybrid Encryption from Weakened Key Encapsulation ..... 553
*Dennis Hofheinz and Eike Kiltz*

## XIV Multi-party Computation

Scalable and Unconditionally Secure Multiparty Computation ..... 572
*Ivan Damgård and Jesper Buus Nielsen*

On Secure Multi-party Computation in Black-Box Groups ..... 591
*Yvo Desmedt, Josef Pieprzyk, Ron Steinfeld, and Huaxiong Wang*

A Note on Secure Computation of the Moore-Penrose Pseudoinverse and Its Application to Secure Linear Algebra ..... 613
*Ronald Cramer, Eike Kiltz, and Carles Padró*

**Author Index** ..... 631