

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

David Pointcheval Thomas Johansson (Eds.)

Advances in Cryptology – EUROCRYPT 2012

31st Annual International Conference
on the Theory and Applications of Cryptographic Techniques
Cambridge, UK, April 15-19, 2012
Proceedings

Volume Editors

David Pointcheval
École Normale Supérieure
45 rue d'Ulm, 75005 Paris, France
E-mail: david.pointcheval@ens.fr

Thomas Johansson
Lund University
Department of Electrical and Information Technology
P.O. Box 118, 221 00, Lund, Sweden
E-mail: thomas.johansson@eit.lth.se

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-29010-7 e-ISBN 978-3-642-29011-4
DOI 10.1007/978-3-642-29011-4
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012933758

CR Subject Classification (1998): E.3, F.2.1-2, G.2.1, D.4.6, K.6.5, C.2, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

© International Association for Cryptologic Research 2012

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

These are the proceedings of Eurocrypt 2012, the 31st Annual IACR Eurocrypt Conference. The conference, sponsored by the International Association for Cryptologic Research, was held April 15–19, 2012, in Cambridge, UK, within the celebrations of Alan Turing Year. The General Chair was Nigel Smart, from University of Bristol.

The Eurocrypt 2012 Program Committee (PC) consisted of 32 members. There were 195 papers submitted to the conference. Each paper was assigned to at least three PC members, while submissions co-authored by PC members were reviewed by at least four PC members. Papers were refereed anonymously. Due to the large number of high-quality submissions, the review process was challenging: the PC, aided by reports from 177 external reviewers, produced a total of 604 reviews in all. After the reviews were submitted, the committee deliberated online for several weeks, exchanging 738 discussion messages. All of our deliberations were aided by the iChair Web submission and review software written by Thomas Baignères and Matthieu Finiasz. We are indebted to them for letting us use their software and for providing us with some help.

The PC eventually selected 41 submissions for presentation during the conference and these are the articles that are included in this volume. Note that these proceedings contain the revised versions of the selected papers. Since the revisions were not checked again before publication, the authors (and not the committee) bear full responsibility of the contents of their papers.

The PC decided to give the Best Paper Award to Antoine Joux and Vanessa Vitse for their paper “Cover and Decomposition Index Calculus on Elliptic Curves made practical. Application to a previously unreachable curve over F_{p^6} .” The conference program also included two invited lectures, and short abstracts are provided in the proceedings: one by Antoine Joux entitled “A Tutorial on High-Performance Computing Applied to Cryptanalysis,” and the other by Alfred Menezes on “Another Look at Provable Security.” We would like to thank them for accepting our invitation and for contributing to the success of Eurocrypt 2012.

We wish to warmly thank the authors who submitted their papers. The hard task of reading, commenting, debating and finally selecting the papers for the conference fell on the PC members. We are very grateful to the committee members and their sub-reviewers for their hard and conscientious work. We would like to thank Jacques Beigbeder for setting up and maintaining the submission and review server at ENS, and Nigel Smart for his great help.

Finally, we would like to say it has been a great honor to be PC Chairs for Eurocrypt 2012!

April 2012

David Pointcheval
Thomas Johansson

Organization

General Chair

Nigel Smart University of Bristol, UK

Program Chairs

David Pointcheval ENS, CNRS, and INRIA, Paris, France
Thomas Johansson Lund University, Sweden

Program Committee

Masayuki Abe NTT, Japan
John Black University of Colorado at Boulder and UC
Santa Barbara, USA
David Cash IBM Research, USA
Dario Catalano Università di Catania, Italy
Jean-Sébastien Coron University of Luxembourg
Orr Dunkelman University of Haifa and Weizmann Institute,
Israel
Marc Fischlin TU Darmstadt, Germany
Pierre-Alain Fouque ENS, France
Steven Galbraith University of Auckland, New Zealand
Henri Gilbert ANSSI, France
Louis Goubin University of Versailles, France
Jens Groth University College London, UK
Dennis Hofheinz Karlsruhe Institut für Technologie, Germany
Tetsu Iwata Nagoya University, Japan
John Kelsey NIST, USA
Aggelos Kiayias University of Athens, Greece
Arjen Lenstra EPFL, Switzerland
Benoit Libert UC Louvain, Belgium
Yehuda Lindell Bar-Ilan University, Israel
Kaisa Nyberg Aalto University and Nokia, Finland
Thomas Peyrin Nanyang Technological University, Singapore
Krzysztof Pietrzak CWI, The Netherlands
Vincent Rijmen KU Leuven and TU Graz, Belgium/Austria
Thomas Ristenpart University of Wisconsin, USA
Kazue Sako NEC, Japan
Palash Sarkar Indian Statistical Institute, India
Igor Shparlinski Macquarie University, Australia

Martijn Stam	University of Bristol, UK
Vinod Vaikuntanathan	Microsoft Research and University of Toronto, Canada
Ivan Visconti	University of Salerno, Italy
Xiaoyun Wang	Tsinghua University, China
Duncan Wong	City University of Hong Kong, SAR China

External Reviewers

Michel Abdalla	Mario Di Raimondo	Antoine Joux
Adi Akavia	Yevgeniy Dodis	Pascal Junod
Joël Alwen	Nico Döttling	Bhavana Kanukurthi
Elena Andreeva	Pooya Farshim	Eike Kiltz
Giuseppe Ateniese	Jean-Charles Faugère	Thorsten Kleinjung
Nuttapong Attrapadung	Sebastian Faust	David Kohel
Man Ho Au	Serge Fehr	Yuichi Komano
Paul Baecher	Dario Fiore	Takeshi Koshiba
Thomas Baignères	David Mandell Freeman	Daniel Kraschewski
Foteini Baldimtsi	Georg Fuchsbauer	Kaoru Kurosawa
Paulo Barreto	Thomas Fuhr	Fabien Laguillaumie
Aurélie Bauer	Eichiro Fujisaki	Mario Larangeira
Stephanie Bayer	Jun Furukawa	Dong Hoon Lee
David Bernhard	David Galindo	Jooyoung Lee
Daniel J. Bernstein	Nicolas Gama	Kwangsue Lee
Sanjay Bhattacharjee	Sanjam Garg	Kaitai Liang
Joppe Bos	Essam Ghadafi	Dongdai Lin
Christoph Bösch	Benedikt Gierlichs	Zhen Liu
Zvika Brakerski	Domingo Gomez	Victor Lomné
Billy Brumley	Sergey Gorbunov	Adriana Lopez-Alt
Christina Brzuska	Dov Gordon	Stefan Lucks
Jesper Buus Nielsen	Robert Granger	Anna Lysyanskaya
Ran Canetti	Adam Groce	Vadim Lyubashevsky
Debrup Chakraborty	Jian Guo	Hemanta Maji
Nishanth Chandran	Carmit Hazay	Avradip Mandal
Donghoon Chang	Javier Herranz	Joana Marim
Lidong Chen	Shoichi Hirose	Damian Markham
Jung Hee Cheon	Susan Hohenberger	Alexander May
Céline Chevalier	Qiong Huang	Florian Mendel
Seung Geol Choi	Toshiyuki Ishiki	Rachel Miller
Ashish Choudhury	Tibor Jäger	Kazuhiko Minematsu
Özgür Dagdelen	Abhishek Jain	Payman Mohassel
Bernardo David	Kimmo Järvinen	Michael Naehrig
Emiliano De Cristofaro	Dimitar Jetchev	Koh-ichi Nagao
Jean Paul Degabriele	Shaoquan Jiang	Svetla Nikova
Claus Diem	Stephen Jordan	Takashi Nishide

Ryo Nishimaki
Ryo Nojima
Satoshi Obana
Miyako Ohkubo
Adam O'Neill
Cristina Onete
Claudio Orlandi
Alina Ostafe
Jong Hwan Park
Kenneth Paterson
Alain Patey
Souradyuti Paul
Chris Peikert
Rene Peralta
Olivier Pereira
Ray Perlner
Ludovic Perret
Edoardo Persichetti
Marcel Pfaffhauser
Benny Pinkas
Axel Poschmann
Carla Ràfols
Ananth Raghunathan
Somindu C. Ramanna

Oded Regev
Leonid Reyzin
Yannis Rouselakis
Subhabrata Samajder
Bagus Santoso
Santanu Sarkar
Alessandra Scafuro
Christian Schaffner
Sven Schäge
Werner Schindler
Martin Schläffer
Yannick Seurin
Barhum Kfir Shlomo
Thomas Shrimpton
Shashank Singh
Daniel Smith
Damien Stehlé
John Steinberger
Ron Steinfeld
Fatih Sulak
Koutarou Suzuki
Xiao Tan
Isamu Teranishi
Stefano Tessaro

Nicolas Theriault
Mehdi Tibouchi
Elmar Tischhauser
Tomas Toft
Deniz Toz
Meltem Sonmez Turan
Dominique Unruh
Kerem Varici
Muthu
Venkatasubramaniam
Akshay Wadia
Bogdan Warinschi
Brent Waters
Daniel Wichs
Keita Xagawa
Dongsheng Xing
Guomin Yang
Kan Yasuda
Bingsheng Zhang
Yunlei Zhao
Hong-Sheng Zhou
Vassilis Zikas

Table of Contents

Invited Talks

A Tutorial on High Performance Computing Applied to Cryptanalysis (Invited Talk Abstract)	1
<i>Antoine Joux</i>	
Another Look at Provable Security	8
<i>Alfred Menezes</i>	

Index Calculus

Cover and Decomposition Index Calculus on Elliptic Curves Made Practical: Application to a Previously Unreachable Curve over \mathbb{F}_{p^6}	9
<i>Antoine Joux and Vanessa Vitse</i>	
Improving the Complexity of Index Calculus Algorithms in Elliptic Curves over Binary Fields	27
<i>Jean-Charles Faugère, Ludovic Perret, Christophe Petit, and Guénaél Renault</i>	

Symmetric Constructions I

Key-Alternating Ciphers in a Provable Setting: Encryption Using a Small Number of Public Permutations (Extended Abstract)	45
<i>Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Francois-Xavier Standaert, John Steinberger, and Elmar Tischhauser</i>	
Efficient and Optimally Secure Key-Length Extension for Block Ciphers via Randomized Cascading	63
<i>Peter Gaži and Stefano Tessaro</i>	

Secure Computation

Fair Computation with Rational Players	81
<i>Adam Groce and Jonathan Katz</i>	
Concurrently Secure Computation in Constant Rounds	99
<i>Sanjam Garg, Vipul Goyal, Abhishek Jain, and Amit Sahai</i>	
Identity-Based Encryption Resilient to Continual Auxiliary Leakage	117
<i>Tsz Hon Yuen, Sherman S.M. Chow, Ye Zhang, and Siu Ming Yiu</i>	

Protocols

Quantum Proofs of Knowledge 135
Dominique Unruh

On Round-Optimal Zero Knowledge in the Bare Public-Key Model 153
Alessandra Scafuro and Ivan Visconti

Robust Coin Flipping 172
Gene S. Kopp and John D. Wiltshire-Gordon

Unconditionally-Secure Robust Secret Sharing with Compact Shares 195
Alfonso Cevallos, Serge Fehr, Rafail Ostrovsky, and Yuval Rabani

Lossy Trapdoor Functions

All-But-Many Lossy Trapdoor Functions 209
Dennis Hofheinz

Identity-Based (Lossy) Trapdoor Functions and Applications 228
Mihir Bellare, Eike Kiltz, Chris Peikert, and Brent Waters

Dual Projective Hashing and Its Applications — Lossy Trapdoor
 Functions and More 246
Hoeteck Wee

Tools

Efficient Zero-Knowledge Argument for Correctness of a Shuffle 263
Stephanie Bayer and Jens Groth

Malleable Proof Systems and Applications 281
Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Sarah Meiklejohn

Group to Group Commitments Do Not Shrink 301
Masayuki Abe, Kristiyan Haralambiev, and Miyako Ohkubo

Tools for Simulating Features of Composite Order Bilinear Groups in
 the Prime Order Setting 318
Allison Lewko

Symmetric Constructions II

Minimalism in Cryptography: The Even-Mansour Scheme Revisited 336
Orr Dunkelman, Nathan Keller, and Adi Shamir

Message Authentication, Revisited 355
Yevgeniy Dodis, Eike Kiltz, Krzysztof Pietrzak, and Daniel Wichs

Property Preserving Symmetric Encryption	375
<i>Omkant Pandey and Yannis Rouselakis</i>	

Symmetric Cryptanalysis

Narrow-Bicliques: Cryptanalysis of Full IDEA	392
<i>Dmitry Khovratovich, Gaëtan Leurent, and Christian Rechberger</i>	
Cryptanalyses on a Merkle-Damgård Based MAC — Almost Universal Forgery and Distinguishing- H Attacks	411
<i>Yu Sasaki</i>	
Statistical Tools Flavor Side-Channel Collision Attacks	428
<i>Amir Moradi</i>	

Fully Homomorphic Encryption

Public Key Compression and Modulus Switching for Fully Homomorphic Encryption over the Integers	446
<i>Jean-Sébastien Coron, David Naccache, and Mehdi Tibouchi</i>	
Fully Homomorphic Encryption with Polylog Overhead	465
<i>Craig Gentry, Shai Halevi, and Nigel P. Smart</i>	
Multiparty Computation with Low Communication, Computation and Interaction via Threshold FHE	483
<i>Gilad Asharov, Abhishek Jain, Adriana López-Alt, Eran Tromer, Vinod Vaikuntanathan, and Daniel Wichs</i>	

Asymmetric Cryptanalysis

Faster Algorithms for Approximate Common Divisors: Breaking Fully-Homomorphic-Encryption Challenges over the Integers	502
<i>Yuanmi Chen and Phong Q. Nguyen</i>	
Decoding Random Binary Linear Codes in $2^{n/20}$: How $1 + 1 = 0$ Improves Information Set Decoding	520
<i>Anja Becker, Antoine Joux, Alexander May, and Alexander Meurer</i>	

Efficient Reductions

Optimal Security Proofs for Full Domain Hash, Revisited	537
<i>Saqib A. Kakvi and Eike Kiltz</i>	
On the Exact Security of Schnorr-Type Signatures in the Random Oracle Model	554
<i>Yannick Seurin</i>	

Tightly-Secure Signatures from Lossy Identification Schemes 572
Michel Abdalla, Pierre-Alain Fouque, Vadim Lyubashevsky, and Mehdi Tibouchi

Public-Key Schemes

Adaptively Attribute-Hiding (Hierarchical) Inner Product Encryption 591
Tatsuaki Okamoto and Katsuyuki Takashima

Scalable Group Signatures with Revocation 609
Benoît Libert, Thomas Peters, and Moti Yung

Incremental Deterministic Public-Key Encryption 628
Ilya Mironov, Omkant Pandey, Omer Reingold, and Gil Segev

Security Models

Standard Security Does Not Imply Security against Selective-Opening 645
Mihir Bellare, Rafael Dowsley, Brent Waters, and Scott Yilek

Detecting Dangerous Queries: A New Approach for Chosen Ciphertext Security 663
Susan Hohenberger, Allison Lewko, and Brent Waters

Security of Symmetric Encryption in the Presence of Ciphertext Fragmentation 682
Alexandra Boldyreva, Jean Paul Degabriele, Kenneth G. Paterson, and Martijn Stam

Lattices

Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller 700
Daniele Micciancio and Chris Peikert

Pseudorandom Functions and Lattices 719
Abhishek Banerjee, Chris Peikert, and Alon Rosen

Lattice Signatures without Trapdoors 738
Vadim Lyubashevsky

Author Index 757