Lecture Notes in Computer Science 7237

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

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

Springer

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



*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 | Karlsruher 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 | Kwangsu Lee |
| Sanjay Bhattacherjee | 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 Isshiki | Rachel Miller |
| Ashish Choudhury | Tibor Jager | 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 Varıcı
Muthu Venkitasubramaniam
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

## Protocols



## Lossy Trapdoor Functions



## Tools



## Symmetric Constructions II

## Symmetric Cryptanalysis



## Fully Homomorphic Encryption



## Asymmetric Cryptanalysis



## Efficient Reductions

## Public-Key Schemes



## Security Models



## Lattices