neval
nsson (Eds.)

LNCS 7237

Advances in Cryptology – EUROCRYPT 2012

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

INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH

i a c r

Springer

Lecture Notes in Computer Science 7237

Comenced Publication in 1973
Founing and Former Series Editors:
Gerhrd 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 ISBN 978-3-642-29011-4 (eBook)
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
Adi Akavia
Joël Alwen
Elena Andreeva
Giuseppe Ateniese
Nuttapong Attrapadung
Man Ho Au
Paul Baecher
Thomas Baignères
Foteini Baldimtsi
Paulo Barreto
Aurélie Bauer
Stephanie Bayer
David Bernhard
Daniel J. Bernstein
Sanjay Bhattacherjee
Joppe Bos
Christoph Bösch
Zvika Brakerski
Billy Brumley
Christina Brzuska
Jesper Buus Nielsen
Ran Canetti
Debrup Chakraborty
Nishanth Chandran
Donghoon Chang
Lidong Chen
Jung Hee Cheon
Céline Chevalier
Seung Geol Choi
Ashish Choudhury
Özgür Dagdelen
Bernardo David
Emiliano De Cristofaro
Jean Paul Degabriele
Claus Diem
Mario Di Raimondo
Yevgeniy Dodis
Nico Döttling
Pooya Farshim
Jean-Charles Faugère
Sebastian Faust
Serge Fehr
Dario Fiore
David Mandell Freeman
Georg Fuchsbauer
Thomas Fuhr
Eichiro Fujisaki
Jun Furukawa
David Galindo
Nicolas Gama
Sanjam Garg
Essam Ghadafi
Benedikt Gierlichs
Domingo Gomez
Sergey Gorbunov
Dov Gordon
Robert Granger
Adam Groce
Jian Guo
Carmit Hazay
Javier Herranz
Shoichi Hirose
Susan Hohenberger
Qiong Huang
Toshiyuki Isshiki
Tibor Jager
Abhishek Jain
Kimmo Järvinen
Dimitar Jetchev
Shaoquan Jiang
Stephen Jordan
Antoine Joux
Pascal Junod
Bhavana Kanukurthi
Eike Kiltz
Thorsten Kleinjung
David Kohel
Yuichi Komano
Takeshi Koshiba
Daniel Kraschewski
Kaoru Kurosawa
Fabien Laguillaumie
Mario Larangeira
Dong Hoon Lee
Jooyoung Lee
Kwangsu Lee
Kaitai Liang
Dongdai Lin
Zhen Liu
Victor Lomné
Adriana Lopez-Alt
Stefan Lucks
Anna Lysyanskaya
Vadim Lyubashevsky
Hemanta Maji
Avradip Mandal
Joana Marim
Damian Markham
Alexander May
Florian Mendel
Rachel Miller
Kazuhiko Minematsu
Payman Mohassel
Michael Naehrig
Koh-ichi Nagao
Svetla Nikova
Takashi Nishide