Lecture Notes in Computer Science 9666

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

Editorial Board

More information about this series at http://www.springer.com/series/7410

Marc Fischlin · Jean-Sébastien Coron (Eds.)

Advances in Cryptology – EUROCRYPT 2016

35th Annual International Conference
on the Theory and Applications of Cryptographic Techniques
Vienna, Austria, May 8–12, 2016
Proceedings, Part II

Springer

Editors
Marc Fischlin
Technische Universität Darmstadt
Darmstadt
Germany

Jean-Sébastien Coron
University of Luxembourg
Luxembourg
Luxembourg

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-662-49895-8 ISBN 978-3-662-49896-5 (eBook)
DOI 10.1007/978-3-662-49896-5

Library of Congress Control Number: 2016935585

LNCS Sublibrary: SL4 – Security and Cryptology

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer-Verlag GmbH Berlin Heidelberg

Preface

Eurocrypt 2016, the 35th annual International Conference on the Theory and Applications of Cryptographic Techniques, was held in Vienna, Austria, during May 8–12, 2016. The conference was sponsored by the International Association for Cryptologic Research (IACR). Krzysztof Pietrzak (IST Austria), together with Joël Alwen, Georg Fuchsbauer, Peter Gaži (all IST Austria), and Eike Kiltz (Ruhr-Universität Bochum), were responsible for the local organization. They were supported by a local organizing team consisting of Hamza Abusalah, Chethan Kamath, and Michal Rybár (all IST Austria). We are indebted to them for their support and smooth collaboration.

The conference program followed the now established parallel track system where the works of the authors were presented in two concurrently running tracks. As in the previous edition of Eurocrypt, one track was labeled $\mathcal{R}$ (for real) and the other one was labeled $\mathcal{I}$ (for ideal). Only the invited talks, the tutorial, the best paper, papers with honorable mentions, and the final session of the conference spanned over both tracks.

The proceedings of Eurocrypt contain 62 papers selected from 274 submissions, which corresponds to a record number of submissions in the history of Eurocrypt. Each submission was anonymized for the reviewing process and was assigned to at least three of the 55 Program Committee members. Submissions co-authored by committee members were assigned to at least four members. Committee members were allowed to submit at most one paper, or two if both were co-authored. The reviewing process included a first-round notification followed by a rebuttal for papers that made it to the second round. After extensive deliberations the Program Committee accepted 62 papers. The revised versions of these papers are included in these two-volume proceedings.

The committee decided to give the Best Paper Award to "Tightly Secure CCA-Secure Encryption Without Pairings" by Romain Gay, Dennis Hofheinz, Eike Kiltz, and Hoeteck Wee. The two runners-up to the award, "Indistinguishability Obfuscation from Constant-Degree Graded Encoding Schemes" by Huijia Lin and "Essentially Optimal Robust Secret Sharing with Maximal Corruptions" by Allison Bishop, Valerio Pastro, Rajmohan Rajaraman, Daniel and Wichs, received honorable mentions. All three papers received invitations for the *Journal of Cryptology*.

The program also included invited talks by Karthikeyan Bhargavan, entitled "Protecting Transport Layer Security from Legacy Vulnerabilities", Bart Preneel, entitled "The Future of Cryptography" (IACR distinguished lecture), and Christian Collberg, entitled "Engineering Code Obfuscation." In addition, Emmanuel Prouff gave a tutorial about "Securing Cryptography Implementations in Embedded Systems." All the speakers were so kind as to also provide a short abstract for the proceedings.

We would like to thank all the authors who submitted papers. We know that the Program Committee's decisions, especially rejections of very good papers that did not find a slot among the sparse number of accepted papers, can be very disappointing. We sincerely hope that the rejected works eventually get the attention they deserve.

We are also indebted to the Program Committee members and all external reviewers for their voluntary work, especially since the newly established and unified page limits and the increasing number of submissions induce quite a workload. It has been an honor to work with everyone. The committee's work was tremendously simplified by Shai Halevi's submission software and his support, including running the service on IACR servers.

Finally, we thank everyone else—speakers, session chairs, and rump session chairs—for their contribution to the program of Eurocrypt 2016.

May 2016

Marc Fischlin
Jean-Sébastien Coron

Eurocrypt 2016

The 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques

Vienna, Austria
May 8–12, 2016

Track $\mathcal{I}$

General Chair

Krzysztof Pietrzak	IST Austria

Program Chairs

Marc Fischlin	Technische Universität Darmstadt, Germany
Jean-Sébastien Coron	University of Luxembourg, Luxembourg

Program Committee

Michel Abdalla	Ecole Normale Superieure and CNRS, France
Shweta Agrawal	IIT Delhi, India
Elette Boyle	IDC Herzliya, Israel
Christina Brzuska	TU Hamburg-Harburg, Germany
Ran Canetti	Tel Aviv University, Israel, and Boston University, USA
David Cash	Rutgers University, USA
Dario Catalano	University of Catania, Italy
Jean-Sébastien Coron	University of Luxembourg, Luxembourg
Cas Cremers	University of Oxford, UK
Yevgeniy Dodis	New York University, USA
Nico Döttling	Aarhus University, Denmark
Pooya Farshim	Queen's University Belfast, UK
Jean-Charles Faugère	Inria Paris-Rocquencourt, France
Sebastian Faust	Ruhr University Bochum, Germany
Dario Fiore	IMDEA Software Institute, Spain
Marc Fischlin	TU Darmstadt, Germany
Georg Fuchsbauer	IST, Austria
Juan A. Garay	Yahoo Labs, USA
Vipul Goyal	Microsoft Research, India
Tim Güneysu	University of Bremen, Germany
Shai Halevi	IBM, USA

Goichiro Hanaoka	AIST, Japan
Martin Hirt	ETH Zurich, Switzerland
Dennis Hofheinz	Karlsruhe KIT, Germany
Tibor Jager	Ruhr University Bochum, Germany
Abhishek Jain	Johns Hopkins University, USA
Aniket Kate	Purdue University, USA
Dmitry Khovratovich	University of Luxembourg, Luxembourg
Vadim Lyubashevsky	Ecole Normale Superieure, France
Sarah Meiklejohn	University College London, UK
Mridul Nandi	Indian Statistical Institute, Kolkata, India
María Naya-Plasencia	Inria, France
Svetla Nikova	KU Leuven, Belgium
Adam O'Neill	Georgetown University, USA
Claudio Orlandi	Aarhus University, Denmark
Josef Pieprzyk	Queensland University of Technology, Australia
Mariana Raykova	Yale University, USA
Thomas Ristenpart	Cornell Tech, USA
Matthieu Rivain	CryptoExperts, France
Arnab Roy	Fujitsu Laboratories of America, USA
Benedikt Schmidt	IMDEA Software Institute, Spain
Thomas Schneider	TU Darmstadt, Germany
Berry Schoenmakers	TU Eindhoven, The Netherlands
Peter Schwabe	Radboud University, The Netherlands
Yannick Seurin	ANSSI, France
Thomas Shrimpton	University of Florida, USA
Nigel P. Smart	University of Bristol, UK
John P. Steinberger	Tsinghua University, China
Ron Steinfeld	Monash University, Australia
Emmanuel Thomé	Inria Nancy, France
Yosuke Todo	NTT, Japan
Dominique Unruh	University of Tartu, Estonia
Daniele Venturi	Sapienza University of Rome, Italy
Ivan Visconti	University of Salerno, Italy
Stefan Wolf	USI Lugano, Switzerland

External Reviewers

Divesh Aggarwal	Kazumaro Aoki	Subhadeep Banik
Shashank Agrawal	Afonso Arriaga	Harry Bartlett
Adi Akavia	Gilad Asharov	Lejla Batina
Martin Albrecht	Gilles Van Assche	Carsten Baum
Joël Alwen	Nuttapong Attrapadung	Aemin Baumeler
Prabhanjan Ananth	Christian Badertscher	Christof Beierle
Ewerton Rodrigues Andrade	Thomas Baignères	Sonia Belaïd
Elena Andreeva	Josep Balasch	Fabrice Benhamouda
	Foteini Baldimtsi	David Bernhard

Ritam Bhaumik
Begül Bilgin
Nir Bitansky
Matthieu Bloch
Andrey Bodgnanov
Cecilia Boschini
Vitor Bosshard
Christina Boura
Florian Bourse
Cerys Bradley
Zvika Brakerski
Anne Broadbent
Dan Brown
Seyit Camtepe
Anne Canteaut
Angelo De Caro
Avik Chakraborti
Nishanth Chandran
Melissa Chase
Rahul Chatterjee
Yilei Chen
Jung Hee Cheon
Céline Chevalier
Alessandro Chiesa
Seung Geol Choi
Tom Chothia
Arka Rai Choudhuri
Kai-Min Chung
Yu-Chi Chen
Michele Ciampi
Michael Clear
Aloni Cohen
Ran Cohen
Katriel Cohn-Gordon
Sandro Coretti
Cas Cremers
Dana Dachman-Soled
Yuanxi Dai
Nilanjan Datta
Bernardo Machado David
Gareth T. Davies
Ed Dawson
Jean Paul Degabriele
Martin Dehnel-Wild
Jeroen Delvaux
Grégory Demay
Daniel Demmler
David Derler
Vasil Dimitrov
Yarkin Doroz
Léo Ducas
François Dupressoir
Frederic Dupuis
Avijit Dutta
Stefan Dziembowski
Keita Emura
Antonio Faonio
Serge Fehr
Claus Fieker
Matthieu Finiasz
Viktor Fischer
Jean-Pierre Flori
Pierre-Alain Fouque
Tore Kasper Frederiksen
Tommaso Gagliardoni
Steven Galbraith
David Galindo
Chaya Ganesh
Luke Garratt
Romain Gay
Peter Gaži
Daniel Genkin
Craig Gentry
Hossein Ghodosi
Satrajit Ghosh
Benedikt Gierlichs
Kristian Gjøsteen
Aleksandr Golovnev
Alonso Gonzalez
Dov Gordon
Louis Goubin
Jens Groth
Aurore Guillevic
Sylvain Guilley
Siyao Guo
Divya Gupta
Sourav Sen Gupta
Helene Flyvholm Haagh
Tzipora Halevi
Michael Hamburg
Carmit Hazay
Gottfried Herold
Susan Hohenberger
Justin Holmgren
Pavel Hubacek
Tsung-Hsuan Hung
Christopher Huth
Michael Hutter
Andreas Hülsing
Vincenzo Iovino
Håkon Jacobsen
Aayush Jain
Jérémy Jean
Claude-Pierre Jeannerod
Evan Jeffrey
Ashwin Jha
Daniel Jost
Charanjit Jutla
Ali El Kaafarani
Liang Kaitai
Saqib A. Kakvi
Chethan Kamath
Bhavana Kanukurthi
Pierre Karpman
Elham Kashefi
Tomasz Kazana
Marcel Keller
Dakshita Khurana
Aggelos Kiayias
Paul Kirchner
Elena Kirshanova
Ágnes Kiss
Fuyuki Kitagawa
Ilya Kizhvatov
Thorsten Kleinjung
Vlad Kolesnikov
Venkata Koppala
Luke Kowalczyk
Ranjit Kumaresan
Kaoru Kurosawa
Felipe Lacerda
Virginie Lallemand
Adeline Langlois
Enrique Larraia
Sebastian Lauer
Gregor Leander
Chin Ho Lee
Tancrède Lepoint

Gaëtan Leurent
Benoît Libert
Huijia (Rachel) Lin
Wei-Kai Lin
Bin Liu
Dongxi Liu
Yunwen Liu
Steve Lu
Atul Luykx
Bernardo Magri
Mohammad Mahmoody
Subhamoy Maitra
Hemanta Maji
Giulio Malavolta
Avradip Mandal
Daniel Masny
Takahiro Matsuda
Christian Matt
Willi Meier
Sebastian Meiser
Florian Mendel
Bart Mennink
Eric Miles
Kevin Milner
Ilya Mironov
Arno Mittelbach
Ameer Mohammad
Payman Mohassel
Hart Montgomery
Amir Moradi
François Morain
Paweł Morawiecki
Pedro Moreno-Sanchez
Nicky Mouha
Pratyay Mukherjee
Elke De Mulder
Anderson Nascimento
Muhammad Naveed
Phong Nguyen
Ivica Nikolic
Tobias Nilges
Peter Sebastian Nordholt
Koji Nuida
Maciej Obremski
Frederique Elise Oggier
Emmanuela Orsini
Mohammad Ali Orumiehchi
Elisabeth Oswald
Ekin Ozman
Jiaxin Pan
Giorgos Panagiotakos
Omkant Pandey
Omer Paneth
Dimitris Papadopoulos
Kostas Papagiannopoulos
Bryan Parno
Valerio Pastro
Chris Peikert
Ludovic Perret
Leo Paul Perrin
Christophe Petit
Krzysztof Pietrzak
Benny Pinkas
Oxana Poburinnaya
Bertram Poettering
Joop van de Pol
Antigoni Polychroniadou
Manoj Prabhakaran
Thomas Prest
Emmanuel Prouff
Jörn Müller-Quade
Tal Rabin
Kenneth Radke
Carla Rafols
Mario Di Raimondo
Samuel Ranellucci
Pavel Raykov
Francesco Regazzoni
Omer Reingold
Michał Ren
Guénaël Renault
Oscar Reparaz
Vincent Rijmen
Ben Riva
Tim Ruffing
Ulrich Rührmair
Yusuke Sakai
Amin Sakzad
Benno Salwey
Kai Samelin
Yu Sasaki
Alessandra Scafuro
Christian Schaffner
Tobias Schneider
Peter Scholl
Jacob Schuldt
Gil Segev
Nicolas Sendrier
Abhi Shelat
Leonie Simpson
Shashank Singh
Luisa Siniscalchi
Boris Skoric
Ben Smith
Juraj Somorovsky
John Steinberger
Noah Stephens-Dawidovitz
Björn Tackmann
Vanessa Teague
Sidharth Telang
R. Seth Terashima
Stefano Tessaro
Adrian Thillard
Susan Thomson
Mehdi Tibouchi
Jacques Traoré
Daniel Tschudi
Hoang Viet Tung
Aleksei Udovenko
Margarita Vald
Maria Isabel Gonzalez Vasco
Meilof Veeningen
Vesselin Velichkov
Alexandre Venelli
Muthuramakrishnan Venkitasubramaniam
Frederik Vercauteren
Marion Videau
Vinod Vikuntanathan
Gilles Villard
Damian Vizar
Emmanuel Volte
Christine van Vredendaal
Niels de Vreede
Qingju Wang

Bogdan Warinschi
Hoeteck Wee
Carolyn Whitnall
Daniel Wichs
Alexander Wild
David Wu
Jürg Wullschleger
Masahiro Yagisawa
Shota Yamada
Kan Yasuda
Scott Yilek
Kazuki Yoneyama
Ching-Hua Yu
Samee Zahur
Mark Zhandry
Zongyang Zhang
Vassilis Zikas
Michael Zohner

Contents – Part II

Separations

Zero-Knowledge II

Protocols

Round Complexity

Commitments

Lattices

Leakage

Indifferentiability

Multi-Party Computation II

Obfuscation

Automated Analysis, Functional Encryption, and Non-malleable Codes

Contents – Part I

Masking

Fully Homomorphic Encryption

Cryptanalysis II

Number Theory

Hash Functions

Multilinear Maps

Message Authentication Codes

Attacks on SSL/TLS

Real-World Protocols

Robust Designs

Lattice Reduction