

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, Lancaster, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Zürich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbrücken, Germany

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

Matthew Robshaw · Jonathan Katz (Eds.)

Advances in Cryptology – CRYPTO 2016

36th Annual International Cryptology Conference
Santa Barbara, CA, USA, August 14–18, 2016
Proceedings, Part II

Editors

Matthew Robshaw
Impinj, Inc.
Seattle, WA
USA

Jonathan Katz
University of Maryland
College Park, MD
USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-662-53007-8 ISBN 978-3-662-53008-5 (eBook)
DOI 10.1007/978-3-662-53008-5

Library of Congress Control Number: 2016945783

LNCS Sublibrary: SL4 – Security and Cryptology

© International Association for Cryptologic Research 2016

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, 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.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

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

Preface

The 36th International Cryptology Conference (Crypto 2016) was held at UCSB, Santa Barbara, CA, USA, during August 14–18, 2016. The workshop was sponsored by the International Association for Cryptologic Research.

Crypto continues to grow. This year the Program Committee evaluated a record 274 submissions out of which 70 were chosen for inclusion in the program. Each paper was reviewed by at least three independent reviewers, with papers from Program Committee members receiving at least five reviews. Reviewers with potential conflicts of interest for specific papers were excluded from all discussions about those papers, and this policy was extended to the program chairs as well.

The 44 members of the Program Committee were aided in this complex and time-consuming task by many external reviewers. We would like to thank them all for their service, their expert opinions, and their spirited contributions to the review process. It was a tremendously difficult task to choose the program for this conference, as the quality of the submissions was very high. It was even harder to identify a single best paper, but our congratulations go to Elette Boyle, Niv Gilboa, and Yuval Ishai from IDC Herzliya, Ben Gurion University, and the Technion, respectively, whose paper “Breaking the Circuit Size Barrier for Secure Computation Under DDH” was awarded Best Paper. Our congratulations also go to Mark Zhandry of MIT and Princeton University who won the award for the Best Student Paper “The Magic of ELFs.”

The invited speakers at Crypto 2016 were Brian Sniffen, Chief Security Architect at Akamai Technologies, Inc., and Paul Kocher, founder of Cryptography Research. Brian’s presentation cast a fascinating light on the issues of real-world cryptographic deployment while Paul’s presentation, a joint invitation from the program co-chairs of both Crypto 2016 and CHES 2016, marked 20 years since his publication of the first paper on side-channel attacks at Crypto 1996.

We are, of course, indebted to Brian LaMacchia, the general chair, as well as the local Organizing Committee, who together proved ideal liaisons for establishing the layout of the program and for supporting the speakers. Our job as program co-chairs was made much easier by the excellent tools developed by Shai Halevi; both Shai and Brian were always available at short notice to answer our queries. Finally, we would like to thank all the authors who submitted their work to Crypto 2016. Without you the conference would not exist.

August 2016

Matthew Robshaw
Jonathan Katz

Crypto 2016

The 36th IACR International Cryptology Conference

University of California, Santa Barbara, CA, USA
August 14–18, 2016

Sponsored by the *International Association for Cryptologic Research*

General Chair

Brian LaMacchia Microsoft

Program Chairs

Matthew Robshaw Impinj, USA
Jonathan Katz University of Maryland, USA

Program Committee

Alex Biryukov	University of Luxembourg, Luxembourg
Anne Canteaut	Inria, France
Dario Catalano	Università di Catania, Italy
Nishanth Chandran	Microsoft Research, India
Melissa Chase	Microsoft Research, USA
Joan Daemen	STMicroelectronics, Belgium and Radboud University, The Netherlands
Martin Van Dijk	University of Connecticut, USA
Itai Dinur	Ben-Gurion University, Israel
Pierre-Alain Fouque	Université Rennes 1, France
Steven Galbraith	Auckland University, New Zealand
Sanjam Garg	University of California, Berkeley, USA
S. Dov Gordon	George Mason University, USA
Jens Groth	University College London, UK
Sorina Ionica	Université de Picardie, France
Tetsu Iwata	Nagoya University, Japan
Angelos Kiayias	National and Kapodistrian University of Athens, Greece
Gregor Leander	Ruhr Universität Bochum, Germany
Shengli Liu	Shanghai Jiao Tong University, China
Alexander May	Ruhr Universität Bochum, Germany
Willi Meier	FHNW, Switzerland
Payman Mohassel	Visa Research, USA

Elke De Mulder	Cryptographic Research, France
Steven Myers	Indiana University, USA
Phong Nguyen	Inria, France and CNRS/JFLI and University of Tokyo, Japan
Kaisa Nyberg	Aalto University, Finland
Kenny Paterson	Royal Holloway University of London, UK
Thomas Peyrin	Nanyang Technological University, Singapore
Benny Pinkas	Bar-Ilan University, Israel
David Pointcheval	École Normale Supérieure, France
Manoj Prabhakaran	University of Illinois, USA
Bart Preneel	KU Leuven, Belgium
Mariana Raykova	Yale University, USA
Christian Rechberger	TU-Graz, Austria and DTU, Denmark
Mike Rosulek	Oregon State University, USA
Rei Safavi-Naini	University of Calgary, Canada
Alessandra Scafuro	Boston University and Northeastern University, USA
Patrick Schaumont	Virginia Tech, USA
Dominique Schröder	Saarland University, Germany
Jae Hong Seo	Myongji University, Korea
Yannick Seurin	ANSSI, France
Abhi Shelat	University of Virginia, USA
Nigel Smart	University of Bristol, UK
Ron Steinfeld	Monash University, Australia
Mehdi Tibouchi	NTT Secure Platform Laboratories, Japan

Additional Reviewers

Michel Abdalla	Foteini Baldimtsi	Dan Boneh
Masayuki Abe	Paulo Barreto	Jonathan Bootle
Arash Afshar	Gilles Barthe	Raphael Bost
Shashank Agrawal	Lejla Batina	Christina Boura
Shweta Agrawal	Christof Beierle	Florian Bourse
Ayo Akinyele	Mihir Bellare	Cyril Bouvier
Martin Albrecht	Fabrice Benhamouda	Elette Boyle
Gergely Alpar	Sanjay Bhattacharjee	Zvika Brakerski
Jacob Alperin-Sheriff	Jean-Francois Biasse	Lus Brandão
Elena Andreeva	Begul Bilgin	Anne Broadbent
Daniel Apon	Gaetan Bisson	Christina Brzuska
Gilad Asharov	Nir Bitansky	Christian Cachin
Gilles Van Assche	Simon Blackburn	Ran Canetti
Nuttapong Attrapadung	Olivier Blazy	Angelo De Caro
Saikrishna	Matthieu Bloch	Guilhem Castagnos
Badrinarayanan	Céline Blondeau	Andrea Cerulli
Josep Balasch	Andrej Bogdanov	Pyrros Chaidos

André Chailloux
Jie Chen
Céline Chevalier
Chongwon Cho
Seung Geol Choi
Ashish Choudhury
Sherman Chow
Kai-Min Chung
Michele Ciampi
Michael Clear
Ran Cohen
Geoffroy Couteau
Dana Dachman-Soled
Deepesh Data
Jean Paul Degabriele
David Derler
Daniel Dinu
Christoph Dobraunig
Yevgeniy Dodis
Nico Döttling
Natnatee Dokmai
Leo Ducas
Tuyet Duong
Keita Emura
Frederic Ezerman
Pooya Farshim
Sebastian Faust
Dario Fiore
Marc Fischlin
Joe Fitzsimons
Nils Fleischhacker
Emmanuel Fouotsa
Georg Fuchsbauer
Eiichiro Fujisaki
Martin Gagne
François Le Gall
Chaya Ganesh
Juan Garay
Christina Garman
Romain Gay
Essam Ghadafi
Benedikt Gierlichs
Niv Gilboa
Vipul Goyal
Frédéric Grosshans
Aurore Guillevic

Divya Gupta
Felix Günther
Shai Halevi
Mike Hamburg
Shuai Han
Helena Handschuh
Christian Hanser
Carmit Hazay
Ethan Heilman
Ryan Henry
Gottfried Herold
Felix Heuer
Viet Tung Hoang
Dennis Hofheinz
Ziyuan Hu
Yan Huang
Michael Hutter
Malika Izabachene
Håkon Jacobsen
Mahavir Jhawar
Dingding Jia
Keting Jia
Thomas Johansson
Aaron Johnson
Kimmo Järvinen
Yael Tauman Kalai
Bhavana Kanukurthi
Petteri Kaski
Marcel Keller
Nathan Keller
Carmen Kempka
Iordanis Kerenidis
Dmitry Khovratovich
Dakshita Khurana
Eike Kiltz
Jinsu Kim
Taechan Kim
Paul Kirchner
Elena Kirshanova
Susumu Kiyoshima
Simon Knellwolf
Stefan Koelbl
Vlad Kolesnikov
Takeshi Koshihara
Luke Kowalczyk
Thorsten Kranz

Daniel Kraschewski
Anna Krasnova
Hugo Krawczyk
Fernando Krell
Stephan Krenn
Ranjit Kumaresan
Alptekin Kupcu
Fabien Laguillaumie
Virginie Lallemand
Enrique Larraia
Changmin Lee
Hyung Tae Lee
Kwangsu Lee
Nikos Leonardos
Tancrede Lepoint
Anthony Leverrier
Benoit Libert
Fuchun Lin
Rachel Lin
Yehuda Lindell
Feng-Hao Liu
Yi-Kai Liu
Patrick Longa
Steve Lu
Stefan Lucks
Atul Luykx
Anna Lysyanskaya
Lin Lyu
Vadim Lyubashevsky
Mohammad Mahmoody
Hemanta Maji
Giulio Malavolta
Tal Malkin
Alex Malozemoff
Mark Marson
Daniel Masny
Takahiro Matsuda
Florian Mendel
Bart Mennink
Thyla van der Merwe
Peihan Miao
Christof Michel
Ian Miers
Andrew Miller
Brice Minaud
Kazuhiko Minematsu

Ilya Mironov	Carla Rafols	Jean-Pierre Tillich
Ameer Mohammad	Srinivasan Raghuraman	Yosuke Todo
Amir Moradi	Vanishree Rao	Yiannis Tselekounis
Tal Moran	Manuel Reinert	Michael Tunstall
Nicky Mouha	Oscar Reparaz	Himanshu Tyagi
Pratyay Mukherjee	Silas Richelson	Aleksei Udovenko
Jörn Müller-Quade	Thomas Ristenpart	Jon Ullman
Valérie Nachev	Damien Robert	Dominique Unruh
Michael Naehrig	Alon Rosen	Prashant Vasudevan
Maria Naya-Plasencia	Adeline Roux-Langlois	Vesselin Velichkov
Soheil Nemati	Arnab Roy	Muthu
Khoa Nguyen	Tim Ruffing	Venkitasubramaniam
Ivica Nikolic	Hansol Ryu	Frederik Vercauteren
Ventzi Nikov	Sondre Rønjom	Damien Vergnaud
Ryo Nishimaki	Akshayaram Srinivasan	Jorge Villar
Anca Nitulescu	Amin Sakzad	Dhinakaran
Adam O'Neill	Katerina Samari	Vinayagamurthy
Miyako Ohkubo	Ruediger Schack	Ivan Visconti
Go Ohtake	Christian Schaffner	Michael Walter
Tatsuaki Okamoto	John Schanck	Pengwei Wang
Ozgur Oksuz	Thomas Schneider	Qingju Wang
Cristina Onete	Peter Scholl	Xiao Wang
Claudio Orlandi	Peter Schwabe	Hoeteck Wee
Elisabeth Oswald	Sven Schäge	Mor Weiss
Léo Paul Perrin	Adam Sealfon	Yunhua Wen
Jiaxin Pan	Setareh Sharifian	Carolyn Whinnall
Giorgos Panagiotakos	Tom Shrimpton	Daniel Wichs
Omkant Pandey	Sandeep Shukla	Xiaodi Wu
Kostas	Siang Meng Sim	Keita Xagawa
Pappagiannopoulos	Luisa Siniscalchi	Sophia Yakubov
Anat Paskin-Cherniavsky	Daniel Slamanig	Shota Yamada
Rafael Pass	Yongsoo Song	Kan Yasuda
Valerio Pastro	Kannan Srinathan	Arkady Yerukhimovich
Arpita Patra	Akshayaram Srinivasan	Ouyang Yingkai
Souradyuti Paul	Douglas Stebila	Thomas Zacharias
Christopher Peikert	Damien Stehlé	Mark Zhandry
Rene Peralta	John Steinberger	Bingsheng Zhang
Trevor Perrin	Marc Stevens	Liang Feng Zhang
Giuseppe Persiano	Valentin Suder	Xiao Zhang
Christophe Petit	Willy Susilo	Yupeng Zhang
Rafael Del Pino	Björn Tackmann	Hong-Sheng Zhou
Oxana Poburinnaya	Katsuyuki Takashima	Vassilis Zikas
Antigoni Polychroniadou	Qiang Tang	Dionysis Zindros
Orazio Puglisi	Stefano Tessaro	
Baodong Qin	Aishwarya	
Max Rabkin	Thiruvengadam	

Contents – Part II

Asymmetric Cryptography

Adversary-Dependent Lossy Trapdoor Function from Hardness of Factoring Semi-smooth RSA Subgroup Moduli.	3
<i>Takashi Yamakawa, Shota Yamada, Goichiro Hanaoka, and Noboru Kunihiro</i>	
Optimal Security Proofs for Signatures from Identification Schemes	33
<i>Eike Kiltz, Daniel Masny, and Jiaxin Pan</i>	
FHE Circuit Privacy Almost for Free.	62
<i>Florian Bourse, Rafaël Del Pino, Michele Minelli, and Hoeteck Wee</i>	

Symmetric Cryptography

Cryptanalysis of a Theorem: Decomposing the Only Known Solution to the Big APN Problem	93
<i>Léo Perrin, Aleksei Udovenko, and Alex Biryukov</i>	
The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS.	123
<i>Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim</i>	

Cryptanalytic Tools

Automatic Search of Meet-in-the-Middle and Impossible Differential Attacks	157
<i>Patrick Derbez and Pierre-Alain Fouque</i>	
Memory-Efficient Algorithms for Finding Needles in Haystacks	185
<i>Itai Dinur, Orr Dunkelman, Nathan Keller, and Adi Shamir</i>	
Breaking Symmetric Cryptosystems Using Quantum Period Finding	207
<i>Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia</i>	

Hardware-Oriented Cryptography

Efficiently Computing Data-Independent Memory-Hard Functions.	241
<i>Joël Alwen and Jeremiah Blocki</i>	

Towards Sound Fresh Re-keying with Hard (Physical) Learning Problems . . .	272
<i>Stefan Dziembowski, Sebastian Faust, Gottfried Herold,</i> <i>Anthony Journault, Daniel Masny, and François-Xavier Standaert</i>	

ParII – Towards Combined Hardware Countermeasures Against Side-Channel and Fault-Injection Attacks	302
<i>Tobias Schneider, Amir Moradi, and Tim Güneysu</i>	

Secure Computation and Protocols I

Network-Hiding Communication and Applications to Multi-party Protocols . . .	335
<i>Martin Hirt, Ueli Maurer, Daniel Tschudi, and Vassilis Zikas</i>	

Network Oblivious Transfer	366
<i>Ranjit Kumaresan, Srinivasan Raghuraman, and Adam Sealfon</i>	

On the Power of Secure Two-Party Computation	397
<i>Carmit Hazay and Muthuramakrishnan Venkatasubramanian</i>	

Secure Protocol Transformations	430
<i>Yuval Ishai, Eyal Kushilevitz, Manoj Prabhakaran, Amit Sahai,</i> <i>and Ching-Hua Yu</i>	

On the Communication Required for Unconditionally Secure Multiplication . . .	459
<i>Ivan Damgård, Jesper Buus Nielsen, Antigoni Polychroniadou,</i> <i>and Michael Raskin</i>	

Obfuscation

Universal Constructions and Robust Combiners for Indistinguishability Obfuscation and Witness Encryption	491
<i>Prabhanjan Ananth, Aayush Jain, Moni Naor, Amit Sahai,</i> <i>and Eylon Yogev</i>	

Obfuscation Combiners	521
<i>Marc Fischlin, Amir Herzberg, Hod Bin-Noon, and Haya Shulman</i>	

On Statistically Secure Obfuscation with Approximate Correctness	551
<i>Zvika Brakerski, Christina Brzuska, and Nils Fleischhacker</i>	

Revisiting the Cryptographic Hardness of Finding a Nash Equilibrium.	579
<i>Sanjam Garg, Omkant Pandey, and Akshayaram Srinivasan</i>	

Asymmetric Cryptography and Cryptanalysis II

Cryptanalysis of GGH15 Multilinear Maps.	607
<i>Jean-Sébastien Coron, Moon Sung Lee, Tancrede Lepoint,</i> <i>and Mehdi Tibouchi</i>	

Annihilation Attacks for Multilinear Maps: Cryptanalysis of Indistinguishability Obfuscation over GGH13	629
<i>Eric Miles, Amit Sahai, and Mark Zhandry</i>	
Three’s Compromised Too: Circular Insecurity for Any Cycle Length from (Ring-)LWE	659
<i>Navid Alamati and Chris Peikert</i>	
Circular Security Separations for Arbitrary Length Cycles from LWE	681
<i>Venkata Koppula and Brent Waters</i>	
Author Index	701