

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, Zurich, 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, Chennai, 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>

Jesper Buus Nielsen · Vincent Rijmen (Eds.)

Advances in Cryptology – EUROCRYPT 2018

37th Annual International Conference on the Theory
and Applications of Cryptographic Techniques
Tel Aviv, Israel, April 29 – May 3, 2018
Proceedings, Part II

Editors

Jesper Buus Nielsen
Aarhus University
Aarhus
Denmark

Vincent Rijmen
University of Leuven
Leuven
Belgium

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-78374-1 ISBN 978-3-319-78375-8 (eBook)
<https://doi.org/10.1007/978-3-319-78375-8>

Library of Congress Control Number: 2018937382

LNCS Sublibrary: SL4 – Security and Cryptology

© International Association for Cryptologic Research 2018

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. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

This Springer imprint is published by the registered company Springer International Publishing AG
part of Springer Nature
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

Eurocrypt 2018, the 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, was held in Tel Aviv, Israel, from April 29 to May 3, 2018. The conference was sponsored by the International Association for Cryptologic Research (IACR). Orr Dunkelman (University of Haifa, Israel) was responsible for the local organization. He was supported by a local organizing team consisting of Technion's Hiroshi Fujiwara Cyber Security Research Center headed by Eli Biham, and most notably by Suzie Eid. We are deeply 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. Only the invited talks spanned over both tracks.

We received a total of 294 submissions. Each submission was anonymized for the reviewing process and was assigned to at least three of the 54 Program Committee members. Committee members were allowed to submit at most one paper, or two if both were co-authored. Submissions by committee members were held to a higher standard than normal submissions. The reviewing process included a rebuttal round for all submissions. After extensive deliberations, the Program Committee accepted 69 papers. The revised versions of these papers are included in these three-volume proceedings, organized topically within their respective track.

The committee decided to give the Best Paper Award to the papers "Simple Proofs of Sequential Work" by Bram Cohen and Krzysztof Pietrzak, "Two-Round Multiparty Secure Computation from Minimal Assumptions" by Sanjam Garg and Akshayaram Srinivasan, and "Two-Round MPC from Two-Round OT" by Fabrice Benhamouda and Huijia Lin. All three papers received invitations for the *Journal of Cryptology*.

The program also included invited talks by Anne Canteaut, titled "Desperately Seeking Sboxes", and Matthew Green, titled "Thirty Years of Digital Currency: From DigiCash to the Blockchain".

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

We are also indebted to the members of the Program Committee and all external reviewers for their voluntary work. The Program Committee work is 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 2018. We would also like to thank the many sponsors for their generous support, including the Cryptography Research Fund that supported student speakers.

May 2018

Jesper Buus Nielsen
Vincent Rijmen

Eurocrypt 2018

The 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques

Sponsored by *the International Association for Cryptologic Research*

April 29 – May 3, 2018
Tel Aviv, Israel

General Chair

Orr Dunkelman

University of Haifa, Israel

Program Co-chairs

Jesper Buus Nielsen

Aarhus University, Denmark

Vincent Rijmen

University of Leuven, Belgium

Program Committee

Martin Albrecht

Royal Holloway, UK

Joël Alwen

IST Austria, Austria, and Wickr, USA

Gilles Van Assche

STMicroelectronics, Belgium

Paulo S. L. M. Barreto

University of Washington Tacoma, USA

Nir Bitansky

Tel Aviv University, Israel

Céline Blondeau

Aalto University, Finland

Andrey Bogdanov

DTU, Denmark

Chris Brzuska

TU Hamburg, Germany, and Aalto University, Finland

Jan Camenisch

IBM Research – Zurich, Switzerland

Ignacio Cascudo

Aalborg University, Denmark

Melissa Chase

Microsoft Research, USA

Alessandro Chiesa

UC Berkeley, USA

Joan Daemen

Radboud University, The Netherlands,
and STMicroelectronics, Belgium

Yevgeniy Dodis

New York University, USA

Nico Döttling

Friedrich Alexander University Erlangen-Nürnberg,
Germany

Sebastian Faust

TU Darmstadt, Germany

Serge Fehr

CWI Amsterdam, The Netherlands

Georg Fuchsbauer

Inria and ENS, France

Jens Groth

University College London, UK

Jian Guo

Nanyang Technological University, Singapore

Martin Hirt	ETH Zurich, Switzerland
Dennis Hofheinz	KIT, Germany
Yuval Ishai	Technion, Israel, and UCLA, USA
Nathan Keller	Bar-Ilan University, Israel
Eike Kiltz	Ruhr-Universität Bochum, Germany
Gregor Leander	Ruhr-Universität Bochum, Germany
Yehuda Lindell	Bar-Ilan University, Israel
Mohammad Mahmoody	University of Virginia, USA
Willi Meier	FHNW, Windisch, Switzerland
Florian Mendel	Infineon Technologies, Germany
Bart Mennink	Radboud University, The Netherlands
Maria Naya-Plasencia	Inria, France
Svetla Nikova	KU Leuven, Belgium
Eran Omri	Ariel University, Israel
Arpita Patra	Indian Institute of Science, India
David Pointcheval	ENS/CNRS, France
Bart Preneel	KU Leuven, Belgium
Thomas Ristenpart	Cornell Tech, USA
Alon Rosen	IDC Herzliya, Israel
Mike Rosulek	Oregon State University, USA
Louis Salvail	Université de Montréal, Canada
Yu Sasaki	NTT Secure Platform Laboratories, Japan
Thomas Schneider	TU Darmstadt, Germany
Jacob C. N. Schuldt	AIST, Japan
Nigel P. Smart	KU Leuven, Belgium, and University of Bristol, UK
Adam Smith	Boston University, USA
Damien Stehlé	ENS de Lyon, France
Björn Tackmann	IBM Research – Zurich, Switzerland
Dominique Unruh	University of Tartu, Estonia
Vinod Vaikuntanathan	MIT, USA
Muthuramakrishnan Venkitasubramaniam	University of Rochester, USA
Frederik Vercauteren	KU Leuven, Belgium
Damien Vergnaud	Sorbonne Université, France
Ivan Visconti	University of Salerno, Italy
Moti Yung	Columbia University and Snap Inc., USA

Additional Reviewers

Masayuki Abe	Divesh Aggarwal	Bar Alon
Aysajan Abidin	Shashank Agrawal	Abdel Aly
Ittai Abraham	Shweta Agrawal	Prabhanjan Ananth
Hamza Abusalah	Thomas Agrikola	Elena Andreeva

Daniel Apon
 Gilad Asharov
 Nuttapong Attrapadung
 Benedikt Auerbach
 Daniel Augot
 Christian Badertscher
 Saikrishna
 Badrinarayanan
 Shi Bai
 Josep Balasch
 Marshall Ball
 Valentina Banciu
 Subhadeep Banik
 Zhenzhen Bao
 Gilles Barthe
 Lejla Batina
 Balthazar Bauer
 Carsten Baum
 Christof Beierle
 Amos Beimel
 Sonia Belaid
 Aner Ben-Efraim
 Fabrice Benhamouda
 Iddo Bentov
 Itay Berman
 Kavun Elif Bilge
 Olivier Blazy
 Jeremiah Blocki
 Andrey Bogdanov
 Carl Bootland
 Jonathan Bootle
 Raphael Bost
 Leif Both
 Florian Bourse
 Elette Boyle
 Zvika Brakerski
 Christian Cachin
 Ran Canetti
 Anne Canteaut
 Brent Carmer
 Wouter Castryck
 Andrea Cerulli
 André Chailloux
 Avik Chakraborti
 Yilei Chen
 Ashish Choudhury

Chitchanok
 Chuengsatiansup
 Michele Ciampi
 Thomas De Cnudde
 Ran Cohen
 Sandro Coretti
 Jean-Sebastien Coron
 Henry Corrigan-Gibbs
 Ana Costache
 Geoffroy Couteau
 Claude Crépeau
 Ben Curtis
 Dana Dachman-Soled
 Yuanxi Dai
 Bernardo David
 Alex Davidson
 Jean Paul Degabriele
 Akshay Degwekar
 Daniel Demmler
 Amit Deo
 Apoorvaa Deshpande
 Itai Dinur
 Christoph Dobraunig
 Manu Drijvers
 Maria Dubovitskaya
 Léo Ducas
 Yfke Dulek
 Pierre-Alain Dupont
 François Dupressoir
 Avijit Dutta
 Lisa Ekey
 Maria Eichlseder
 Maximilian Ernst
 Mohammad Etemad
 Antonio Faonio
 Oriol Farràs
 Pooya Farshim
 Manuel Ferscht
 Dario Fiore
 Viktor Fischer
 Nils Fleischhacker
 Christian Forler
 Tommaso Gagliardoni
 Chaya Ganesh
 Juan Garay
 Sanjam Garg

Romain Gay
 Peter Gaži
 Rosario Gennaro
 Satrajit Ghosh
 Irene Giacomelli
 Federico Giacon
 Benedikt Gierlichs
 Junqing Gong
 Dov Gordon
 Divya Gupta
 Lorenzo Grassi
 Hannes Gross
 Vincent Grosso
 Paul Grubbs
 Chun Guo
 Siyao Guo
 Mohammad Hajiabadi
 Carmit Hazay
 Gottfried Herold
 Felix Heuer
 Thang Hoang
 Viet Tung Hoang
 Akinori Hosoyamada
 Kristina Hostáková
 Andreas Hülsing
 Ilia Iliashenko
 Roi Inbar
 Vincenzo Iovino
 Tetsu Iwata
 Abhishek Jain
 Martin Jepsen
 Daniel Jost
 Chiraag Juvekar
 Seny Kamara
 Chethan Kamath
 Bhavana Kanukurthi
 Harish Karthikeyan
 Suichi Katsumata
 Jonathan Katz
 John Kelsey
 Dakshita Khurana
 Eunkyung Kim
 Taechan Kim
 Elena Kirshanova
 Ágnes Kiss
 Susumu Kiyoshima

Ilya Kizhvatov	Marta Mularczyk	Ron Rothblum
Alexander Koch	Mridul Nandi	David Roubinet
Konrad Kohbrok	Ventzislav Nikov	Adeline Roux-Langlois
Lisa Kohl	Tobias Nilges	Vladimir Rozic
Stefan Kölbl	Ryo Nishimaki	Andy Rupp
Ilan Komargodski	Anca Nitulescu	Yusuke Sakai
Yashvanth Kondi	Ariel Nof	Simona Samardjiska
Venkata Koppula	Achiya Bar On	Niels Samwel
Thorsten Kranz	Claudio Orlandi	Olivier Sanders
Hugo Krawczyk	Michele Orrù	Pratik Sarkar
Marie-Sarah Lacharite	Clara Paglialonga	Alessandra Scafuro
Kim Laine	Giorgos Panagiotakos	Martin Schläffer
Virginie Lallemand	Omer Paneth	Dominique Schröder
Gaëtan Leurent	Louiza Papachristodoulou	Sven Schäge
Anthony Leverrier	Kostas Papagiannopoulos	Adam Sealton
Xin Li	Sunoo Park	Yannick Seurin
Pierre-Yvan Liardet	Anat Paskin-Cherniavsky	abhi shelat
Benoît Libert	Alain Passelègue	Kazumasa Shinagawa
Huijia Lin	Kenny Paterson	Luisa Siniscalchi
Guozhen Liu	Michaël Peeters	Maciej Skórski
Jian Liu	Chris Peikert	Fang Song
Chen-Da Liu-Zhang	Alice Pellet-Mary	Ling Song
Alex Lombardi	Geovandro C. C. F. Pereira	Katerina Sotiraki
Julian Loss	Leo Perrin	Florian Speelman
Steve Lu	Giuseppe Persiano	Gabriele Spini
Atul Luykx	Thomas Peters	Kannan Srinathan
Vadim Lyubashevsky	Krzysztof Pietrzak	Thomas Steinke
Saeed Mahloujifar	Benny Pinkas	Uri Stemmer
Hemanta Maji	Oxana Poburinnaya	Igor Stepanovs
Mary Maller	Bertram Poettering	Noah
Umberto Martínez-Peñas	Antigoni Polychroniadou	Stephens-Davidowitz
Daniel Masny	Christopher Portmann	Alan Szepieniec
Takahiro Matsuda	Manoj Prabhakaran	Seth Terashima
Christian Matt	Emmanuel Prouff	Cihangir Tezcan
Patrick McCorry	Carla Ràfols	Mehdi Tibouchi
Pierrick Méaux	Somindu C. Ramanna	Elmar Tischhauser
Lauren De Meyer	Samuel Ranellucci	Radu Titiu
Peihan Miao	Shahram Rasoolzadeh	Yosuke Todo
Brice Minaud	Divya Ravi	Junichi Tomida
Esfandiar Mohammadi	Ling Ren	Patrick Towa
Ameer Mohammed	Oscar Reparaz	Boaz Tsaban
Maria Chiara Molteni	Silas Richelson	Daniel Tschudi
Tal Moran	Peter Rindal	Thomas Unterluggauer
Fabrice Mouhartem	Michal Rolinek	Margarita Vald
Amir Moradi	Miruna Rosca	Kerem Varici
Pratyay Mukherjee		Prashant Vasudevan

Philip Vejrè
Daniele Venturi
Benoît Viguier
Fernando Virdia
Damian Vizár
Alexandre Wallet
Michael Walter
Haoyang Wang
Qingju Wang

Hoeteck Wee
Felix Wegener
Christian Weinert
Erich Wenger
Daniel Wichs
Friedrich Wiemer
David Wu
Thomas Wunderer
Sophia Yakoubov

Shota Yamada
Takashi Yamakawa
Kan Yasuda
Attila Yavuz
Scott Yilek
Eylon Yogev
Greg Zaverucha
Mark Zhandry
Ren Zhang

Abstract of Invited Talks

Desperately Seeking Sboxes

Anne Canteaut

Inria, Paris, France

`anne.canteaut@inria.fr`

Abstract. Twenty-five years ago, the definition of security criteria associated to the resistance to linear and differential cryptanalysis has initiated a long line of research in the quest for Sboxes with optimal nonlinearity and differential uniformity. Although these optimal Sboxes have been studied by many cryptographers and mathematicians, many questions remain open. The most prominent open problem is probably the determination of the optimal values of the nonlinearity and of the differential uniformity for a permutation depending on an even number of variables.

Besides those classical properties, various attacks have motivated several other criteria. Higher-order differential attacks, cube distinguishers and the more recent division property exploit some specific properties of the representation of the whole cipher as a collection of multivariate polynomials, typically the fact that some given monomials do not appear in these polynomials. This type of property is often inherited from some algebraic property of the Sbox. Similarly, the invariant subspace attack and its nonlinear counterpart also originate from specific algebraic structure in the Sbox.

Thirty Years of Digital Currency: From DigiCash to the Blockchain

Matthew Green

Johns Hopkins University
mgreen@cs.jhu.edu

Abstract. More than thirty years ago a researcher named David Chaum presented his vision for a cryptographic financial system. In the past ten years this vision has been realized. Yet despite a vast amount of popular excitement, it remains to be seen whether the development of cryptocurrencies (and their associated consensus technologies) will have a lasting positive impact—both on society and on our research community. In this talk I will examine that question. Specifically, I will review several important contributions that research cryptography has made to this field; survey the most promising deployed (or developing) technologies; and discuss the many challenges ahead.

Contents – Part II

Blockchain

Thunderella: Blockchains with Optimistic Instant Confirmation	3
<i>Rafael Pass and Elaine Shi</i>	
But Why Does It Work? A Rational Protocol Design Treatment of Bitcoin.	34
<i>Christian Badertscher, Juan Garay, Ueli Maurer, Daniel Tschudi, and Vassilis Zikas</i>	
Ouroboros Praos: An Adaptively-Secure, Semi-synchronous Proof-of-Stake Blockchain	66
<i>Bernardo David, Peter Gazi, Aggelos Kiayias, and Alexander Russell</i>	
Sustained Space Complexity.	99
<i>Joël Alwen, Jeremiah Blocki, and Krzysztof Pietrzak</i>	

Multi-collision Resistance

Multi-Collision Resistant Hash Functions and Their Applications	133
<i>Itay Berman, Akshay Degwekar, Ron D. Rothblum, and Prashant Nalini Vasudevan</i>	
Collision Resistant Hashing for Paranoids: Dealing with Multiple Collisions.	162
<i>Ilan Komargodski, Moni Naor, and Eylon Yogev</i>	

Signatures

Synchronized Aggregate Signatures from the RSA Assumption.	197
<i>Susan Hohenberger and Brent Waters</i>	
More Efficient (Almost) Tightly Secure Structure-Preserving Signatures.	230
<i>Romain Gay, Dennis Hofheinz, Lisa Kohl, and Jiaxin Pan</i>	

Private Simultaneous Messages

The Communication Complexity of Private Simultaneous Messages, Revisited	261
<i>Benny Applebaum, Thomas Holenstein, Manoj Mishra, and Ofer Shayevitz</i>	

The Complexity of Multiparty PSM Protocols and Related Models	287
<i>Amos Beimel, Eyal Kushilevitz, and Phina Nissim</i>	

Masking

Formal Verification of Masked Hardware Implementations in the Presence of Glitches	321
<i>Roderick Bloem, Hannes Gross, Rinat Iusupov, Bettina Könighofer, Stefan Mangard, and Johannes Winter</i>	
Masking the GLP Lattice-Based Signature Scheme at Any Order	354
<i>Gilles Barthe, Sonia Belaïd, Thomas Espitau, Pierre-Alain Fouque, Benjamin Grégoire, Mélissa Rossi, and Mehdi Tibouchi</i>	
Masking Proofs Are Tight and How to Exploit it in Security Evaluations. . .	385
<i>Vincent Grosso and François-Xavier Standaert</i>	

Best Young Researcher Paper Award

The Discrete-Logarithm Problem with Preprocessing	415
<i>Henry Corrigan-Gibbs and Dmitry Kogan</i>	

Best Paper Awards

Simple Proofs of Sequential Work.	451
<i>Bram Cohen and Krzysztof Pietrzak</i>	
Two-Round Multiparty Secure Computation from Minimal Assumptions . . .	468
<i>Sanjam Garg and Akshayaram Srinivasan</i>	
k -Round Multiparty Computation from k -Round Oblivious Transfer via Garbled Interactive Circuits.	500
<i>Fabrice Benhamouda and Huijia Lin</i>	

Theoretical Multiparty Computation

Adaptively Secure Garbling with Near Optimal Online Complexity	535
<i>Sanjam Garg and Akshayaram Srinivasan</i>	
A New Approach to Black-Box Concurrent Secure Computation	566
<i>Sanjam Garg, Susumu Kiyoshima, and Omkant Pandey</i>	

Obfuscation

Obfustopia Built on Secret-Key Functional Encryption.	603
<i>Fuyuki Kitagawa, Ryo Nishimaki, and Keisuke Tanaka</i>	

Limits on Low-Degree Pseudorandom Generators (Or: Sum-of-Squares Meets Program Obfuscation)	649
<i>Boaz Barak, Zvika Brakerski, Ilan Komargodski, and Pravesh K. Kothari</i>	
 Symmetric Cryptanalysis	
Boomerang Connectivity Table: A New Cryptanalysis Tool	683
<i>Carlos Cid, Tao Huang, Thomas Peyrin, Yu Sasaki, and Ling Song</i>	
Correlation Cube Attacks: From Weak-Key Distinguisher to Key Recovery	715
<i>Meicheng Liu, Jingchun Yang, Wenhao Wang, and Dongdai Lin</i>	
The Missing Difference Problem, and Its Applications to Counter Mode Encryption	745
<i>Gaëtan Leurent and Ferdinand Sibleyras</i>	
Fast Near Collision Attack on the Grain v1 Stream Cipher	771
<i>Bin Zhang, Chao Xu, and Willi Meier</i>	
Author Index	803