Lecture Notes in Computer Science 10821

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

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

Springer

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

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

Philip Vejre
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

Symmetric Cryptanalysis