

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, 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>

Jonathan Katz · Hovav Shacham (Eds.)

Advances in Cryptology – CRYPTO 2017

37th Annual International Cryptology Conference
Santa Barbara, CA, USA, August 20–24, 2017
Proceedings, Part III

Editors

Jonathan Katz
University of Maryland
College Park, MD
USA

Hovav Shacham
UC San Diego
La Jolla, CA
USA

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-319-63696-2

ISBN 978-3-319-63697-9 (eBook)

DOI 10.1007/978-3-319-63697-9

Library of Congress Control Number: 2017947035

LNCS Sublibrary: SL4 – Security and Cryptology

© International Association for Cryptologic Research 2017

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 Springer Nature

The registered company is Springer International Publishing AG

The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The 37th International Cryptology Conference (Crypto 2017) was held at the University of California, Santa Barbara, USA, during August 20–24, 2017, sponsored by the International Association for Cryptologic Research.

There were 311 submissions to Crypto 2017, a substantial increase from previous years. The Program Committee, aided by nearly 350 external reviewers, selected 72 papers to appear in the program. We are indebted to all the reviewers for their service. Their reviews and discussions, if printed out, would consume about a thousand pages.

Two papers—“Identity-Based Encryption from the Diffie-Hellman Assumption,” by Nico Döttling and Sanjam Garg, and “The first Collision for Full SHA-1,” by Marc Stevens, Elie Bursztein, Pierre Karpman, Ange Albertini, and Yarik Markov—were honored as best papers. A third paper—“Watermarking Cryptographic Functionalities from Standard Lattice Assumptions,” by Sam Kim and David J. Wu—was honored as best paper authored exclusively by young researchers.

Crypto was the venue for the 2017 IACR Distinguished Lecture, delivered by Shafi Goldwasser. Crypto also shared an invited speaker, Cédric Fournet, with the 30th IEEE Computer Security Foundations Symposium (CSF 2017), which was held jointly with Crypto.

We are grateful to Steven Myers, the Crypto general chair; to Shai Halevi, author of the IACR Web Submission and Review system; to Alfred Hofmann, Anna Kramer, and their colleagues at Springer; to Sally Vito of UCSB Conference Services; and, of course, everyone who submitted a paper to Crypto and everyone who attended the conference.

August 2017

Jonathan Katz
Hovav Shacham

Crypto 2017

The 37th IACR International Cryptology Conference

University of California, Santa Barbara, CA, USA
August 20–24, 2017

Sponsored by the *International Association for Cryptologic Research*

General Chair

Steven Myers

Indiana University, USA

Program Chairs

Jonathan Katz

University of Maryland, USA

Hovav Shacham

UC San Diego, USA

Program Committee

Masayuki Abe

NTT Secure Platform Laboratories, Japan

Shweta Agrawal

IIT Madras, India

Adi Akavia

The Academic College of Tel Aviv-Yaffo, Israel

Elena Andreeva

KU Leuven, Belgium

Mihir Bellare

UC San Diego, USA

Dan Boneh

Stanford University, USA

Elette Boyle

IDC Herzliya, Israel

Ran Canetti

Boston University, USA, and Tel Aviv University,
Israel

Jung Hee Cheon

Seoul National University, Korea

Dana Dachman-Soled

University of Maryland, USA

Ivan Damgård

Aarhus University, Denmark

Nico Döttling

UC Berkeley, USA

Orr Dunkelman

University of Haifa, Israel

Eiichiro Fujisaki

NTT Secure Platform Laboratories, Japan

Sergey Gorbunov

University of Waterloo, Canada

Vipul Goyal

Carnegie Mellon University, USA

Matthew Green

Johns Hopkins University, USA

Nadia Heninger

University of Pennsylvania, USA

Viet Tung Hoang

Florida State University, USA

Dennis Hofheinz

Karlsruhe Institute of Technology, Germany

Sorina Ionica

Université de Picardie, France

Tetsu Iwata	Nagoya University, Japan
Seny Kamara	Brown University, USA
Gaëtan Leurent	Inria, France
Rachel Lin	UC Santa Barbara, USA
Stefan Lucks	Bauhaus-Universität Weimar, Germany
Vadim Lyubashevsky	IBM Zurich, Switzerland
Mohammad Mahmoody	University of Virginia, USA
Payman Mohassel	Visa Research, USA
Claudio Orlandi	Aarhus University, Denmark
Elisabeth Oswald	University of Bristol, UK
Rafael Pass	Cornell University, USA
Gregory G. Rose	TargetProof LLC, USA
Christian Schaffner	University of Amsterdam and CWI and QuSoft, The Netherlands
Gil Segev	Hebrew University, Israel
Yannick Seurin	ANSSI, France
Douglas Stebila	McMaster University, Canada
Stefano Tessaro	UC Santa Barbara, USA
Mehdi Tibouchi	NTT Secure Platform Laboratories, Japan
Erin Tromer	Tel Aviv University, Israel, and Columbia University, USA
Dominique Unruh	University of Tartu, Estonia
Vassilis Zikas	Rensselaer Polytechnic Institute, USA

Additional Reviewers

Aysajan Abidin	Achiya Bar-On	Leon Groot Bruinderink
Shashank Agrawal	Razvan Barbulescu	Benedikt Bunz
Thomas Agrikola	Guy Barwell	Anne Canteaut
Ali Akhavi	Carsten Baum	Angelo de Caro
Gorjan Alagic	Amin Baumeler	Ignacio Cascudo
Martin Albrecht	Fabrice Benhamouda	David Cash
Jacob Alperin-Sheriff	Daniel J. Bernstein	Wouter Castryck
Joel Alwen	Jean-François Biasse	Nishanth Chandran
Joran van Apeldoorn	Alex Biryukov	Eshan Chattopadhyay
Daniel Apon	Nir Bitansky	Binyi Chen
Gilad Asharov	Olivier Blazy	Jie Chen
Tomer Ashur	Jeremiah Blocki	Yilei Chen
Nuttapong Attrapadung	Andrej Bogdanov	Alessandro Chiesa
Christian Badertscher	Xavier Bonnetain	Chongwon Cho
Saikrishna	Charlotte Bonte	Arka Rai Choudhuri
Badrinarayanan	Carl Bootland	Heewon Chung
Shi Bai	Christina Boura	Kai-Min Chung
Foteini Baldimtsi	Zvika Brakerski	Benoit Cogliati
Marshall Ball	Brandon Broadnax	Aloni Cohen

Ran Cohen
 Katriel Cohn-Gordon
 Henry Corrigan-Gibbs
 Geoffroy Couteau
 Alain Couvreur
 Cas Cremers
 Jan Czajkowski
 Wei Dai
 Bernardo David
 Jean Paul Degabriele
 Jeroen Delvaux
 Apoorva Deshpande
 Bogdan Adrian Dina
 Itai Dinur
 Yevgeniy Dodis
 Benjamin Dowling
 Rafael Dowsley
 Leo Ducas
 Yfke Dulek
 Tuyet Duong
 Tuyet Thi Anh Duong
 Fred Dupuis
 Frédéric Dupuis
 Alfredo Rial Duran
 Sébastien Duval
 Aner Moshe Ben Efraim
 Maria Eichlseder
 Keita Emura
 Naomi Ephraim
 Saba Eskandarian
 Thomas Espitau
 Oriol Farràs
 Pooya Farshim
 Sebastian Faust
 Prastudy Fauzi
 Nelly Fazio
 Serge Fehr
 Houda Ferradi
 Manuel Ferscht
 Dario Fiore
 Ben Fisch
 Joseph Fitzsimons
 Nils Fleischhacker
 Tore Frederiksen
 Rotem Arnon Friedman
 Georg Fuchsbauer

Marc Fyrbiak
 Tommaso Gagliardoni
 Nicolas Gama
 Juan Garay
 Sanjam Garg
 Christina Garman
 Romain Gay
 Peter Gazi
 Alexandre Gelin
 Daniel Genkin
 Marios Georgiou
 Benoit Gerard
 Essam Ghadafi
 Niv Gilboa
 Dov Gordon
 Rishab Goyal
 Vincent Grosso
 Jens Groth
 Paul Grubbs
 Siyao Guo
 Helene Haag
 Helene Haagh
 KyooHyung Han
 Marcella Hastings
 Carmit Hazay
 Ethan Heilman
 Brett Hemenway
 Minki Hhan
 Justin Holmgren
 Akinori Hosoyamada
 Yan Huang
 Pavel Hubacek
 Ilia Iliashenko
 Vincenzo Iovino
 Yuval Ishai
 Joseph Jaeger
 Zahra Jafraghli
 Tibor Jager
 Aayush Jain
 Abhishek Jain
 Chethan Kamath
 Bhavana Kanukurthi
 Angshuman Karmakar
 Pierre Karpman
 Stefan Katzenbeisser
 Xagawa Keita

Marcel Keller
 Nathan Keller
 Iordanis Kerenidis
 Dakshita Khurana
 Andrey Kim
 Dongwoo Kim
 Duhyeong Kim
 Eunkyung Kim
 Jae-yun Kim
 Jihye Kim
 Jinsu Kim
 Jiseung Kim
 Sam Kim
 Taechan Kim
 Fuyuki Kitagawa
 Susumu Kiyoshima
 Dima Kogan
 Vlad Kolesnikov
 Ilan Komargodski
 Venkata Koppula
 Venkata Kopulla
 Evgenios Kornaropoulos
 Juliane Kraemer
 Mukul Kulkarni
 Ashutosh Kumar
 Ranjit Kumaresan
 Alptekin Küpçü
 Lakshmi Kuppasamy
 Thijs Laarhoven
 Changmin Lee
 Joohee Lee
 Younho Lee
 Nikos Leonardos
 Tancrede Lepoint
 Baiyu Li
 Benoit Libert
 Eik List
 Yi-Kai Liu
 Steve Lu
 Yun Lu
 Atul Luykx
 Saeed Mahloujifar
 Giulio Malavolta
 Alex Malozemoff
 Antonio Marcedone
 Daniel P. Martin

Marco Martinoli	Rafael del Pino	Yongsoo Song
Daniel Masny	Oxana Poburinnaya	Pratik Soni
Takahiro Matsuda	David Pointcheval	Florian Speelman
Florian Mendel	Antigoni Polychroniadou	Akshayaram Srinivasan
Bart Mennink	Raluca Ada Popa	Martijn Stam
Peihan Miao	Bart Preneel	François-Xavier Standaert
Daniele Micciancio	Thomas Prest	John Steinberger
Gabrielle De Micheli	Emmanuel Prouff	Igors Stepanovs
Ian Miers	Carla Rafols	Noah
Andrew Miller	Srinivasan Raghuraman	Stephens-Davidowitz
Kazuhiko Minematsu	Samuel Ranellucci	Valentin Suder
Tarik Moataz	Mariana Raykova	Koutarou Suzuki
Ameer Mohammed	Oded Regev	Björn Tackmann
Hart Montgomery	Ling Ren	Alain Tapp
Andrew Morgan	Oscar Reparaz	Isamu Teranishi
Nicky Mouha	Leo Reyzin	Benjamin Turner
Pratyay Mukherjee	Silas Richelson	Aishwarya
Muhammad Naveed	Matt Robshaw	Thiruvengadam
Maria Naya-Plasencia	Mike Rosulek	Sri Aravinda Krishnan
Kartik Nayak	Yann Rotella	Thyagarajan
Gregory Neven	Lior Rotem	Yosuke Todo
Ruth Ng	Ron Rothblum	Junichi Tomida
Michael Nielsen	Arnab Roy	Luca Trevisan
Tobias Nilges	Sujoy Sinha Roy	Roberto Trifiletti
Ryo Nishimaki	Olivier Ruatta	Daniel Tschudi
Ariel Nof	Ulrich Rührmair	Nik Unger
Kaisa Nyberg	Yusuke Sakai	Salil Vadhan
Adam O'Neill	Olivier Sanders	Margarita Vald
Maciej Obremski	Yu Sasaki	Luke Valenta
Sabine Oechsner	Sajin Sasy	Kerem Varici
Miyako Ohkubo	Alessandra Scafuro	Srinivas Vivek Venkatesh
Rafail Ostrovsky	Patrick Schaumont	Muthuramakrishnan
Daniel Page	Thomas Schneider	Venkatasubramaniam
Jiaxin Pan	Peter Scholl	Daniele Venturi
Omer Paneth	Gregor Seiler	Damien Vergnaud
Dimitris Papadopoulos	Ido Shahaf	Jorge Villar
Sunno Park	abhi shelat	Dhinakaran
Anat Paskin-Cherniavsky	Timothy Sherwood	Vinayagamurthy
Kenny Paterson	Kyoji Shibutani	Ivan Visconti
Arpita Patra	Sina Shiehian	Damian Vizar
Filip Pawlega	Mark Simkin	Christine van Vreedendal
Chris Peikert	Leonie Simpson	Michael Walter
Josef Pieprzyk	Maciej Skorski	Mingyuan Wang
Cécile Pierrot	Nigel Smart	Xiao Wang
Krzysztof Pietrzak	Yongha Son	Yuyu Wang
Benny Pinkas	Fang Song	Yohei Watanabe

Hoeteck Wee
Avi Weinstock
Mor Weiss
Jakob Wenzel
Daniel Wichs
David Wu
Keita Xagawa
Sophia Yakoubov

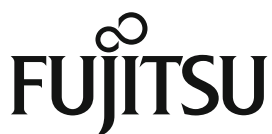
Avishay Yanay
Kan Yasuda
Donggeon Yhee
Chen Yilei
Eylon Yogev
Kazuki Yoneyama
Lanqing Yu
Thomas Zacharias

Samee Zahur
Greg Zaverucha
Mark Zhandry
Ren Zhang
Yupeng Zhang
Hong-Sheng Zhou

Platinum Sponsor



Silver Sponsors



Western Digital®

Contents – Part III

Authenticated Encryption

Boosting Authenticated Encryption Robustness with Minimal Modifications	3
<i>Tomer Ashur, Orr Dunkelman, and Atul Luykx</i>	
ZMAC: A Fast Tweakable Block Cipher Mode for Highly Secure Message Authentication	34
<i>Tetsu Iwata, Kazuhiko Minematsu, Thomas Peyrin, and Yannick Seurin</i>	
Message Franking via Committing Authenticated Encryption	66
<i>Paul Grubbs, Jiahui Lu, and Thomas Ristenpart</i>	
Key Rotation for Authenticated Encryption	98
<i>Adam Everspaugh, Kenneth Paterson, Thomas Ristenpart, and Sam Scott</i>	

Public-Key Encryption

Kurosawa-Desmedt Meets Tight Security	133
<i>Romain Gay, Dennis Hofheinz, and Lisa Kohl</i>	
Asymptotically Compact Adaptively Secure Lattice IBEs and Verifiable Random Functions via Generalized Partitioning Techniques	161
<i>Shota Yamada</i>	
Identity-Based Encryption from Codes with Rank Metric	194
<i>Philippe Gaborit, Adrien Hauteville, Duong Hieu Phan, and Jean-Pierre Tillich</i>	

Stream Ciphers

Degree Evaluation of NFSR-Based Cryptosystems	227
<i>Meicheng Liu</i>	
Cube Attacks on Non-Blackbox Polynomials Based on Division Property . . .	250
<i>Yosuke Todo, Takanori Isobe, Yonglin Hao, and Willi Meier</i>	

Lattice Crypto

Middle-Product Learning with Errors	283
<i>Miruna Roşca, Amin Sakzad, Damien Stehlé, and Ron Steinfeld</i>	

All-But-Many Lossy Trapdoor Functions from Lattices and Applications	298
<i>Xavier Boyen and Qinyi Li</i>	
All-But-Many Lossy Trapdoor Functions and Selective Opening Chosen-Ciphertext Security from LWE	332
<i>Benoît Libert, Amin Sakzad, Damien Stehlé, and Ron Steinfeld</i>	
Amortization with Fewer Equations for Proving Knowledge of Small Secrets	365
<i>Rafael del Pino and Vadim Lyubashevsky</i>	
Leakage and Subversion	
Private Multiplication over Finite Fields.	397
<i>Sonia Belaïd, Fabrice Benhamouda, Alain Passelègue, Emmanuel Prouff, Adrian Thillard, and Damien Vergnaud</i>	
Anonymous Attestation with Subverted TPMs	427
<i>Jan Camenisch, Manu Drijvers, and Anja Lehmann</i>	
Hedging Public-Key Encryption in the Real World	462
<i>Alexandra Boldyreva, Christopher Patton, and Thomas Shrimpton</i>	
Symmetric-Key Crypto	
Information-Theoretic Indistinguishability via the Chi-Squared Method	497
<i>Wei Dai, Viet Tung Hoang, and Stefano Tessaro</i>	
Indifferentiability of Iterated Even-Mansour Ciphers with Non-idealized Key-Schedules: Five Rounds Are Necessary and Sufficient	524
<i>Yuanxi Dai, Yannick Seurin, John Steinberger, and Aishwarya Thiruvengadam</i>	
Encrypted Davies-Meyer and Its Dual: Towards Optimal Security Using Mirror Theory	556
<i>Bart Mennink and Samuel Neves</i>	
Real-World Crypto	
A Formal Treatment of Multi-key Channels	587
<i>Felix Günther and Sogol Mazaheri</i>	
Ratcheted Encryption and Key Exchange: The Security of Messaging	619
<i>Mihir Bellare, Asha Camper Singh, Joseph Jaeger, Maya Nyayapati, and Igors Stepanovs</i>	

PRF-ODH: Relations, Instantiations, and Impossibility Results	651
<i>Jacqueline Brendel, Marc Fischlin, Felix Günther, and Christian Janson</i>	
A New Distribution-Sensitive Secure Sketch and Popularity-Proportional Hashing	682
<i>Joanne Woodage, Rahul Chatterjee, Yevgeniy Dodis, Ari Juels, and Thomas Ristenpart</i>	
Author Index	711