

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 I

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 978-3-319-63687-0 ISBN 978-3-319-63688-7 (eBook)
DOI 10.1007/978-3-319-63688-7

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 Dötting	UC Berkeley, USA
Orr Dunkelman	University of Haifa, Israel
Eiichi 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
Erhan 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	Marc Fyrbiak	Marcel Keller
Katriel Cohn-Gordon	Tommaso Gagliardoni	Nathan Keller
Henry Corrigan-Gibbs	Nicolas Gama	Iordanis Kerenidis
Geoffroy Couteau	Juan Garay	Dakshita Khurana
Alain Couvreur	Sanjam Garg	Andrey Kim
Cas Cremers	Christina Garman	Dongwoo Kim
Jan Czajkowski	Romain Gay	Duhyeong Kim
Wei Dai	Peter Gazi	Eunhyung Kim
Bernardo David	Alexandre Gelin	Jae-yun Kim
Jean Paul Degabriele	Daniel Genkin	Jihye Kim
Jeroen Delvaux	Marios Georgiou	Jinsu Kim
Apoorva Deshpande	Benoit Gerard	Jiseung Kim
Bogdan Adrian Dina	Essam Ghadafi	Sam Kim
Itai Dinur	Niv Gilboa	Taechan Kim
Yevgeniy Dodis	Dov Gordon	Fuyuki Kitagawa
Benjamin Dowling	Rishab Goyal	Susumu Kiyoshima
Rafael Dowsley	Vincent Grosso	Dima Kogan
Leo Ducas	Jens Groth	Vlad Kolesnikov
Yfke Dulek	Paul Grubbs	Ilan Komargodski
Tuyet Duong	Siyao Guo	Venkata Koppula
Tuyet Thi Anh Duong	Helene Haag	Venkata Kopulla
Fred Dupuis	Helene Haagh	Evgenios Kornaropoulos
Frédéric Dupuis	Kyoohyung Han	Juliane Kraemer
Alfredo Rial Duran	Marcella Hastings	Mukul Kulkarni
Sébastien Duval	Carmit Hazay	Ashutosh Kumar
Aner Moshe Ben Efraim	Ethan Heilman	Ranjit Kumaresan
Maria Eichlseder	Brett Hemenway	Alptekin Küpçü
Keita Emura	Minki Hhan	Lakshmi Kuppusamy
Naomi Ephraim	Justin Holmgren	Thijs Laarhoven
Saba Eskandarian	Akinori Hosoyamada	Changmin Lee
Thomas Espitau	Yan Huang	Joohee Lee
Oriol Farràs	Pavel Hubacek	Younho Lee
Pooya Farshim	Iliia Iliashenko	Nikos Leonardos
Sebastian Faust	Vincenzo Iovino	Tancrede Lepoint
Prastudy Fauzi	Yuval Ishai	Baiyu Li
Nelly Fazio	Joseph Jaeger	Benoit Libert
Serge Fehr	Zahra Jafragholi	Eik List
Houda Ferradi	Tibor Jager	Yi-Kai Liu
Manuel Ferscht	Aayush Jain	Steve Lu
Dario Fiore	Abhishek Jain	Yun Lu
Ben Fisch	Chethan Kamath	Atul Luykx
Joseph Fitzsimons	Bhavana Kanukurthi	Saeed Mahloujifar
Nils Fleischhacker	Angshuman Karmakar	Giulio Malavolta
Tore Frederiksen	Pierre Karpman	Alex Malozemoff
Rotem Arnon Friedman	Stefan Katzenbeisser	Antonio Marcedone
Georg Fuchsbauer	Xagawa Keita	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 Terner
Pratyay Mukherjee	Silas Richelson	Aishwarya
Muhammad Naveed	Matt Robshaw	Thiruvengadam
María 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	Venkitasubramaniam
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 Shibusaki	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



Contents – Part I

Functional Encryption

Stronger Security for Reusable Garbled Circuits, General Definitions and Attacks	3
<i>Shweta Agrawal</i>	
Generic Transformations of Predicate Encodings: Constructions and Applications	36
<i>Miguel Ambrona, Gilles Barthe, and Benedikt Schmidt</i>	
Practical Functional Encryption for Quadratic Functions with Applications to Predicate Encryption	67
<i>Carmen Elisabetta Zaira Baltico, Dario Catalano, Dario Fiore, and Romain Gay</i>	

Foundations I

Memory-Tight Reductions	101
<i>Benedikt Auerbach, David Cash, Manuel Fersch, and Eike Kiltz</i>	
Be Adaptive, Avoid Overcommitting	133
<i>Zahra Jafargholi, Chethan Kamath, Karen Klein, Ilan Komargodski, Krzysztof Pietrzak, and Daniel Wichs</i>	

Two-Party Computation

The TinyTable Protocol for 2-Party Secure Computation, or: Gate-Scrambling Revisited	167
<i>Ivan Damgård, Jesper Buus Nielsen, Michael Nielsen, and Samuel Ranellucci</i>	
Privacy-Free Garbled Circuits for Formulas: Size Zero and Information-Theoretic	188
<i>Yashvanth Kondi and Arpita Patra</i>	
Secure Arithmetic Computation with Constant Computational Overhead	223
<i>Benny Applebaum, Ivan Damgård, Yuval Ishai, Michael Nielsen, and Lior Zichron</i>	
Encryption Switching Protocols Revisited: Switching Modulo p	255
<i>Guilhem Castagnos, Laurent Imbert, and Fabien Laguillaumie</i>	

Bitcoin

The Bitcoin Backbone Protocol with Chains of Variable Difficulty 291
Juan Garay, Aggelos Kiayias, and Nikos Leonardos

Bitcoin as a Transaction Ledger: A Composable Treatment 324
Christian Badertscher, Ueli Maurer, Daniel Tschudi, and Vassilis Zikas

Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol 357
*Aggelos Kiayias, Alexander Russell, Bernardo David,
 and Roman Oliynykov*

Multiparty Computation

Robust Non-interactive Multiparty Computation Against
 Constant-Size Collusion 391
Fabrice Benhamouda, Hugo Krawczyk, and Tal Rabin

The Price of Low Communication in Secure Multi-party Computation 420
Juan Garay, Yuval Ishai, Rafail Ostrovsky, and Vassilis Zikas

Topology-Hiding Computation on All Graphs 447
Adi Akavia, Rio LaVigne, and Tal Moran

A New Approach to Round-Optimal Secure Multiparty Computation 468
Prabhanjan Ananth, Arka Rai Choudhuri, and Abhishek Jain

Award Papers

Watermarking Cryptographic Functionalities from Standard
 Lattice Assumptions 503
Sam Kim and David J. Wu

Identity-Based Encryption from the Diffie-Hellman Assumption 537
Nico Döttling and Sanjam Garg

The First Collision for Full SHA-1 570
*Marc Stevens, Elie Bursztein, Pierre Karpman, Ange Albertini,
 and Yarik Markov*

Obfuscation I

Indistinguishability Obfuscation from SXDH on 5-Linear Maps
 and Locality-5 PRGs 599
Huijia Lin

Indistinguishability Obfuscation from Trilinear Maps and Block-Wise Local PRGs <i>Huijia Lin and Stefano Tessaro</i>	630
Lower Bounds on Obfuscation from All-or-Nothing Encryption Primitives. <i>Sanjam Garg, Mohammad Mahmoody, and Ameer Mohammed</i>	661
Structure vs. Hardness Through the Obfuscation Lens <i>Nir Bitansky, Akshay Degwekar, and Vinod Vaikuntanathan</i>	696
Conditional Disclosure of Secrets	
Conditional Disclosure of Secrets: Amplification, Closure, Amortization, Lower-Bounds, and Separations <i>Benny Applebaum, Barak Arkis, Pavel Raykov, and Prashant Nalini Vasudevan</i>	727
Conditional Disclosure of Secrets via Non-linear Reconstruction. <i>Tianren Liu, Vinod Vaikuntanathan, and Hoeteck Wee</i>	758
Author Index	791