

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>

Hovav Shacham · Alexandra Boldyreva (Eds.)

Advances in Cryptology – CRYPTO 2018

38th Annual International Cryptology Conference
Santa Barbara, CA, USA, August 19–23, 2018
Proceedings, Part II

Editors

Hovav Shacham
The University of Texas at Austin
Austin, TX
USA

Alexandra Boldyreva
Georgia Institute of Technology
Atlanta, GA
USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-96880-3 ISBN 978-3-319-96881-0 (eBook)
<https://doi.org/10.1007/978-3-319-96881-0>

Library of Congress Control Number: 2018949031

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.

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

Preface

The 38th International Cryptology Conference (Crypto 2018) was held at the University of California, Santa Barbara, California, USA, during August 19–23, 2018. It was sponsored by the International Association for Cryptologic Research (IACR). For 2018, the conference was preceded by three days of workshops on various topics. And, of course, there was the awesome Beach BBQ at Goleta Beach.

Crypto continues to grow, year after year, and Crypto 2018 was no exception. The conference set new records for both submissions and publications, with a whopping 351 papers submitted for consideration. It took a Program Committee of 46 cryptography experts working with 272 external reviewers almost 2.5 months to select the 79 papers which were accepted for the conference. It also took one program chair about 30 minutes to dig up all those stats.

In order to minimize intentional and/or subconscious bias, papers were reviewed in the usual double-blind fashion. Program Committee members were limited to two submissions, and their submissions were scrutinized more closely and held to higher standards. The two program chairs were not allowed to submit papers. Of course, they were fine with that restriction since they were way too busy to actually write any papers.

The Program Committee recognized two papers and their authors for standing out among the rest. “Yes, There Is an Oblivious RAM Lower Bound!”, by Kasper Green Larsen and Jesper Buus Nielsen, was voted best paper of the conference. Additionally, “Multi-Theorem Preprocessing NIZKs from Lattices,” by Sam Kim and David J. Wu, was voted Best Paper Authored Exclusively By Young Researchers. There was no award for Best Paper Authored Exclusively by Old Researchers.

Crypto 2018 played host for the IACR Distinguished Lecture, delivered by Shafi Goldwasser. Crypto also welcomed Lea Kissner as an invited speaker from Google.

We would like to express our sincere gratitude to all the reviewers for volunteering their time and knowledge in order to select a great program for 2018. Additionally, we are very appreciative of the following individuals and organizations for helping make Crypto 2018 a success:

Tal Rabin - Crypto 2018 General Chair and Workshops Organizer
Elette Boyle - Workshops Chair
Fabrice Benhamouda - Workshops Organizer
Shafi Goldwasser - IACR Distinguished Lecturer
Lea Kissner - Invited Speaker from Google
Shai Halevi - Author of the IACR Web Submission and Review System
Anna Kramer and her colleagues at Springer
Sally Vito and UCSB Conference Services

We would also like to say thank you to our numerous sponsors, everyone who submitted papers, the session chairs, the rump session chair, and the presenters.

Lastly, a big thanks to everyone who attended the conference at UCSB. Without you, we would have had a lot of leftover potato salad at the Beach BBQ.

August 2018

Alexandra Boldyreva
Hovav Shacham

Crypto 2018

The 38th IACR International Cryptology Conference

University of California, Santa Barbara, CA, USA

August 19–23, 2018

Sponsored by the *International Association for Cryptologic Research*

General Chair

Tal Rabin

IBM T.J. Watson Research Center, USA

Program Chairs

Hovav Shacham

University of Texas at Austin, USA

Alexandra Boldyreva

Georgia Institute of Technology, USA

Program Committee

Shweta Agrawal

Indian Institute of Technology, Madras, India

Benny Applebaum

Tel Aviv University, Israel

Foteini Baldimtsi

George Mason University, USA

Gilles Barthe

IMDEA Software Institute, Spain

Fabrice Benhamouda

IBM Research, USA

Alex Biryukov

University of Luxembourg, Luxembourg

Jeremiah Blocki

Purdue University, USA

Anne Broadbent

University of Ottawa, Canada

Chris Brzuska

Aalto University, Finland

Chitchanok Chuengsatiansup

Inria and ENS de Lyon, France

Dana Dachman-Soled

University of Maryland, USA

Léoucas

Centrum Wiskunde & Informatica, The Netherlands

Pooya Farshim

CNRS and ENS, France

Dario Fiore

IMDEA Software Institute, Spain

Marc Fischlin

Darmstadt University of Technology, Germany

Georg Fuchsbauer

Inria and ENS, France

Steven D. Galbraith

University of Auckland, New Zealand

Christina Garman

Purdue University, USA

Daniel Genkin

University of Pennsylvania and University
of Maryland, USA

Dov Gordon

George Mason University, USA

Viet Tung Hoang

Florida State University, USA

Tetsu Iwata	Nagoya University, Japan
Stanislaw Jarecki	University of California, Irvine, USA
Seny Kamara	Brown University, USA
Markulf Kohlweiss	University of Edinburgh, UK
Farinaz Koushanfar	University of California, San Diego, USA
Xuejia Lai	Shanghai Jiao Tong University, China
Tancrède Lepoint	SRI International, USA
Anna Lysyanskaya	Brown University, USA
Alex J. Malozemoff	Galois, USA
Sarah Meiklejohn	University College London, UK
Daniele Micciancio	University of California, San Diego, USA
María Naya-Plasencia	Inria, France
Kenneth G. Paterson	Royal Holloway, University of London, UK
Ananth Raghunathan	Google, USA
Mike Rosulek	Oregon State University, USA
Ron Rothblum	MIT and Northeastern University, USA
Alessandra Scafuro	North Carolina State University, USA
abhi shelat	Northeastern University, USA
Nigel P. Smart	Katholieke Universiteit Leuven, Belgium
Martijn Stam	University of Bristol, UK
Noah Stephens-Davidowitz	Princeton University, USA
Aishwarya Thiruvengadam	University of California, Santa Barbara, USA
Hoeteck Wee	CNRS and ENS, France
Daniel Wichs	Northeastern University, USA
Mark Zhandry	Princeton University, USA

Additional Reviewers

Aydin Abadi	Balthazar Bauer	Zvika Brakerski
Archita Agarwal	Carsten Baum	Jacqueline Brendel
Divesh Aggarwal	Amos Beimel	David Butler
Shashank Agrawal	Itay Berman	Matteo Campanelli
Adi Akavia	Marc Beunardeau	Brent Carmer
Navid Alapati	Sai Lakshmi Bhavana	Ignacio Cascudo
Martin Albrecht	Simon Blackburn	Wouter Castryck
Miguel Ambrona	Estuardo Alpirez Bock	Andrea Cerulli
Ghous Amjad	Andrej Bogdanov	André Chailloux
Megumi Ando	André Schrottenloher	Nishanth Chandran
Ralph Ankele	Xavier Bonnetain	Panagiotis Chatzigiannis
Gilad Asharov	Charlotte Bonte	Stephen Checkoway
Achiya Bar-On	Carl Bootland	Binyi Chen
Manuel Barbosa	Jonathan Bootle	Michele Ciampi
Paulo Barreto	Christina Boura	Benoitogliati
James Bartusek	Florian Bourse	Gil Cohen
Guy Barwell	Elette Boyle	Ran Cohen

Aisling Connolly
 Sandro Coretti
 Henry Corrigan-Gibbs
 Geoffroy Couteau
 Shujie Cui
 Ting Cui
 Joan Daemen
 Wei Dai
 Yuanxi Dai
 Alex Davidson
 Jean Paul Degabriele
 Akshay Degwekar
 Ioannis Demertzis
 Itai Dinur
 Jack Doerner
 Nico Döttling
 Benjamin Dowling
 Tuyet Thi Anh Duong
 Frédéric Dupuis
 Betul Durak
 Lior Eldar
 Karim Eldefrawy
 Lucas Enloe
 Andre Esser
 Antonio Faonio
 Prastudy Fauzi
 Daniel Feher
 Serge Fehr
 Nils Fleischhacker
 Benjamin Fuller
 Tommaso Gagliardoni
 Martin Gagné
 Adria Gascon
 Pierrick Gaudry
 Romain Gay
 Nicholas Genise
 Marilyn George
 Ethan Gertler
 Vlad Gheorghiu
 Esha Ghosh
 Brian Goncalves
 Junqing Gong
 Adam Groce
 Johann Großschädl
 Paul Grubbs
 Jiaxin Guan

Jian Guo
 Siyao Guo
 Joanne Hall
 Ariel Hamlin
 Abida Haque
 Patrick Harasser
 Gottfried Herold
 Naofumi Homma
 Akinori Hosoyamada
 Jialin Huang
 Siam Umar Hussain
 Chloé Héban
 Yuval Ishai
 Ilia Iliashenko
 Yuval Ishai
 Håkon Jacobsen
 Christian Janson
 Ashwin Jha
 Thomas Johansson
 Chethan Kamath
 Bhavana Kanukurthi
 Marc Kaplan
 Pierre Karpman
 Sriram Keelveedhi
 Dmitry Khovratovich
 Franziskus Kiefer
 Eike Kiltz
 Sam Kim
 Elena Kirshanova
 Konrad Kohbrok
 Lisa Maria Kohl
 Ilan Komargodski
 Yashvanth Kondi
 Venkata Koppula
 Lucas Kowalczyk
 Hugo Krawczyk
 Thijs Laarhoven
 Marie-Sarah Lacharite
 Virginie Lallemand
 Esteban Landerreche
 Phi Hung Le
 Eysa Lee
 Jooyoung Lee
 Gaëtan Leurent
 Baiyu Li
 Benoit Libert

Fuchun Lin
 Huijia Lin
 Tingting Lin
 Feng-Hao Liu
 Qipeng Liu
 Tianren Liu
 Zhiqiang Liu
 Alex Lombardi
 Sébastien Lord
 Steve Lu
 Yiyuan Luo
 Atul Luykx
 Vadim Lyubashevsky
 Fermi Ma
 Varun Madathil
 Mohammad Mahmoody
 Mary Maller
 Giorgia Azzurra Marson
 Daniel P. Martin
 Samiha Marwan
 Christian Matt
 Alexander May
 Sogol Mazaheri
 Bart Mennink
 Carl Alexander Miller
 Brice Minaud
 Ilya Mironov
 Tarik Moataz
 Nicky Mouha
 Fabrice Mouhartem
 Pratyay Mukherjee
 Mridul Nandi
 Samuel Neves
 Anca Nitulescu
 Kaisa Nyberg
 Adam O'Neill
 Maciej Obremski
 Olya Ohrimenko
 Igor Carboni Oliveira
 Claudio Orlandi
 Michele Orrù
 Emmanuela Orsini
 Dag Arne Osvald
 Elisabeth Oswald
 Elena Pagnin
 Chris Peikert

Léo Perrin	Sven Schaege	Fernando Virdia
Edoardo Persichetti	Adam Sealfon	Alexandre Wallet
Duong-Hieu Phan	Yannick Seurin	Michael Walter
Krzysztof Pietrzak	Aria Shahverdi	Meiqin Wang
Bertram Poettering	Tom Shrimpton	Qingju Wang
David Pointcheval	Luisa Siniscalchi	Boyang Wei
Antigoni Polychroniadou	Kit Smeets	Mor Weiss
Eamonn Postlethwaite	Fang Song	Jan Winkelmann
Willy Quach	Pratik Soni	Tim Wood
Elizabeth Quaglia	Jessica Sorrell	David Wu
Samuel Ranellucci	Florian Speelman	Hong Xu
Mariana Raykova	Douglas Stebila	Shota Yamada
Christian Rechberger	Marc Stevens	Hailun Yan
Oded Regev	Bing Sun	LeCorre Yann
Nicolas Resch	Shifeng Sun	Kan Yasuda
Leo Reyzin	Siwei Sun	Arkady Yerukhimovich
M. Sadegh Riazi	Qiang Tang	Eylon Yogev
Silas Richelson	Seth Terashima	Yang Yu
Peter Rindal	Tian Tian	Yu Yu
Phillip Rogaway	Mehdi Tibouchi	Thomas Zacharias
Miruna Rosca	Yosuke Todo	Wentao Zhang
Dragos Rotaru	Aleksei Udovenko	Hong-Sheng Zhou
Yann Rotella	Dominique Unruh	Linfeng Zhou
Arnab Roy	Bogdan Ursu	Vassilis Zikas
Manuel Sabin	María Isabel González	Giorgos Zirdelis
Sruthi Sekar	Vasco	Lukas Zoernig
Amin Sakzad	Muthuramakrishnan	Adi Ben Zvi
Katerina Samari	Venkatasubramaniam	
Pedro Moreno Sanchez	Fre Vercauteren	

Sponsors



Western Digital.



FUJITSU

IBM Research



Contents – Part II

Proof Tools

Simplifying Game-Based Definitions: Indistinguishability up to Correctness and Its Application to Stateful AE	3
<i>Phillip Rogaway and Yusi Zhang</i>	
The Algebraic Group Model and its Applications	33
<i>Georg Fuchsbauer, Eike Kiltz, and Julian Loss</i>	

Key Exchange

On Tightly Secure Non-Interactive Key Exchange.	65
<i>Julia Hesse, Dennis Hofheinz, and Lisa Kohl</i>	
Practical and Tightly-Secure Digital Signatures and Authenticated Key Exchange	95
<i>Kristian Gjøsteen and Tibor Jager</i>	

Symmetric Cryptoanalysis

Fast Correlation Attack Revisited: Cryptanalysis on Full Grain-128a, Grain-128, and Grain-v1	129
<i>Yosuke Todo, Takanori Isobe, Willi Meier, Kazumaro Aoki, and Bin Zhang</i>	
A Key-Recovery Attack on 855-round Trivium.	160
<i>Ximing Fu, Xiaoyun Wang, Xiaoyang Dong, and Willi Meier</i>	
Improved Key Recovery Attacks on Reduced-Round AES with Practical Data and Memory Complexities	185
<i>Achiya Bar-On, Orr Dunkelman, Nathan Keller, Eyal Ronen, and Adi Shamir</i>	
Bernstein Bound on WCS is Tight: Repairing Luykx-Preneel Optimal Forgeries	213
<i>Mridul Nandi</i>	

Hashes and Random Oracles

Correcting Subverted Random Oracles.	241
<i>Alexander Russell, Qiang Tang, Moti Yung, and Hong-Sheng Zhou</i>	

Combiners for Backdoored Random Oracles.	272
<i>Balthazar Bauer, Pooya Farshim, and Sogol Mazaheri</i>	
On Distributional Collision Resistant Hashing.	303
<i>Ilan Komargodski and Eylon Yogev</i>	

Trapdoor Functions

Fast Distributed RSA Key Generation for Semi-honest and Malicious Adversaries	331
<i>Tore Kasper Frederiksen, Yehuda Lindell, Valery Osheter, and Benny Pinkas</i>	
Trapdoor Functions from the Computational Diffie-Hellman Assumption	362
<i>Sanjam Garg and Mohammad Hajiabadi</i>	

Round Optimal MPC

Round-Optimal Secure Multiparty Computation with Honest Majority	395
<i>Prabhanjan Ananth, Arka Rai Choudhuri, Aarushi Goel, and Abhishek Jain</i>	
On the Exact Round Complexity of Secure Three-Party Computation	425
<i>Arpita Patra and Divya Ravi</i>	
Promise Zero Knowledge and Its Applications to Round Optimal MPC	459
<i>Saikrishna Badrinarayanan, Vipul Goyal, Abhishek Jain, Yael Tauman Kalai, Dakshita Khurana, and Amit Sahai</i>	
Round-Optimal Secure Multi-Party Computation.	488
<i>Shai Halevi, Carmit Hazay, Antigoni Polychroniadou, and Muthuramakrishnan Venkitasubramaniam</i>	

Foundations

Yes, There is an Oblivious RAM Lower Bound!.	523
<i>Kasper Green Larsen and Jesper Buus Nielsen</i>	
Constrained PRFs for NC^1 in Traditional Groups	543
<i>Nuttapong Attrapadung, Takahiro Matsuda, Ryo Nishimaki, Shota Yamada, and Takashi Yamakawa</i>	

Lattices

GGH15 Beyond Permutation Branching Programs: Proofs, Attacks, and Candidates.	577
<i>Yilei Chen, Vinod Vaikuntanathan, and Hoeteck Wee</i>	

Lower Bounds on Lattice Enumeration with Extreme Pruning	608
<i>Yoshinori Aono, Phong Q. Nguyen, Takenobu Seito, and Junji Shikata</i>	
Dissection-BKW	638
<i>Andre Esser, Felix Heuer, Robert Kübler, Alexander May, and Christian Sohler</i>	
Lattice-Based ZK	
Sub-linear Lattice-Based Zero-Knowledge Arguments for Arithmetic Circuits	669
<i>Carsten Baum, Jonathan Bootle, Andrea Cerulli, Rafael del Pino, Jens Groth, and Vadim Lyubashevsky</i>	
Lattice-Based Zero-Knowledge Arguments for Integer Relations	700
<i>Benoît Libert, San Ling, Khoa Nguyen, and Huaxiong Wang</i>	
Multi-Theorem Preprocessing NIZKs from Lattices	733
<i>Sam Kim and David J. Wu</i>	
Efficient MPC	
SPD \mathbb{Z}_{2^k} : Efficient MPC mod 2^k for Dishonest Majority	769
<i>Ronald Cramer, Ivan Damgård, Daniel Escudero, Peter Scholl, and Chaoping Xing</i>	
Yet Another Compiler for Active Security or: Efficient MPC Over Arbitrary Rings	799
<i>Ivan Damgård, Claudio Orlandi, and Mark Simkin</i>	
Author Index	831