

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 III

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 978-3-319-96877-3 ISBN 978-3-319-96878-0 (eBook)
<https://doi.org/10.1007/978-3-319-96878-0>

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	Benoit Cogliati
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
Iliia 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 III

Efficient MPC

TinyKeys: A New Approach to Efficient Multi-Party Computation	3
<i>Carmit Hazay, Emmanuela Orsini, Peter Scholl, and Eduardo Soria-Vazquez</i>	
Fast Large-Scale Honest-Majority MPC for Malicious Adversaries	34
<i>Koji Chida, Daniel Genkin, Koki Hamada, Dai Ikarashi, Ryo Kikuchi, Yehuda Lindell, and Ariel Nof</i>	

Quantum Cryptography

Quantum FHE (Almost) As Secure As Classical	67
<i>Zvika Brakerski</i>	
IND-CCA-Secure Key Encapsulation Mechanism in the Quantum Random Oracle Model, Revisited	96
<i>Haodong Jiang, Zhenfeng Zhang, Long Chen, Hong Wang, and Zhi Ma</i>	
Pseudorandom Quantum States	126
<i>Zhengfeng Ji, Yi-Kai Liu, and Fang Song</i>	
Quantum Attacks Against Indistinguishability Obfuscators Proved Secure in the Weak Multilinear Map Model	153
<i>Alice Pellet-Mary</i>	
Cryptanalyses of Branching Program Obfuscations over GGH13 Multilinear Map from the NTRU Problem	184
<i>Jung Hee Cheon, Minki Hhan, Jiseung Kim, and Changmin Lee</i>	

MPC

An Optimal Distributed Discrete Log Protocol with Applications to Homomorphic Secret Sharing	213
<i>Itai Dinur, Nathan Keller, and Ohad Klein</i>	
Must the Communication Graph of MPC Protocols be an Expander?.	243
<i>Elette Boyle, Ran Cohen, Deepesh Data, and Pavel Hubáček</i>	
Two-Round Multiparty Secure Computation Minimizing Public Key Operations.	273
<i>Sanjam Garg, Peihan Miao, and Akshayaram Srinivasan</i>	

Limits of Practical Sublinear Secure Computation	302
<i>Elette Boyle, Yuval Ishai, and Antigoni Polychroniadou</i>	

Garbling

Limits on the Power of Garbling Techniques for Public-Key Encryption	335
<i>Sanjam Garg, Mohammad Hajiabadi, Mohammad Mahmoody, and Ameer Mohammed</i>	

Optimizing Authenticated Garbling for Faster Secure Two-Party Computation	365
<i>Jonathan Katz, Samuel Ranellucci, Mike Rosulek, and Xiao Wang</i>	

Information-Theoretic MPC

Amortized Complexity of Information-Theoretically Secure MPC Revisited . . .	395
<i>Ignacio Cascudo, Ronald Cramer, Chaoping Xing, and Chen Yuan</i>	
Private Circuits: A Modular Approach	427
<i>Prabhanjan Ananth, Yuval Ishai, and Amit Sahai</i>	

Various Topics

A New Public-Key Cryptosystem via Mersenne Numbers	459
<i>Divesh Aggarwal, Antoine Joux, Anupam Prakash, and Miklos Santha</i>	
Fast Homomorphic Evaluation of Deep Discretized Neural Networks	483
<i>Florian Bourse, Michele Minelli, Matthias Minihold, and Pascal Paillier</i>	

Oblivious Transfer

Adaptive Garbled RAM from Laconic Oblivious Transfer	515
<i>Sanjam Garg, Rafail Ostrovsky, and Akshayaram Srinivasan</i>	
On the Round Complexity of OT Extension	545
<i>Sanjam Garg, Mohammad Mahmoody, Daniel Masny, and Izaak Meckler</i>	

Non-malleable Codes

Non-Malleable Codes for Partial Functions with Manipulation Detection	577
<i>Aggelos Kiayias, Feng-Hao Liu, and Yiannis Tselekounis</i>	
Continuously Non-Malleable Codes in the Split-State Model from Minimal Assumptions	608
<i>Rafail Ostrovsky, Giuseppe Persiano, Daniele Venturi, and Ivan Visconti</i>	

Zero Knowledge

Non-Interactive Zero-Knowledge Proofs for Composite Statements	643
<i>Shashank Agrawal, Chaya Ganesh, and Payman Mohassel</i>	
From Laconic Zero-Knowledge to Public-Key Cryptography: Extended Abstract	674
<i>Itay Berman, Akshay Degwekar, Ron D. Rothblum, and Prashant Nalini Vasudevan</i>	
Updatable and Universal Common Reference Strings with Applications to zk-SNARKs	698
<i>Jens Groth, Markulf Kohlweiss, Mary Maller, Sarah Meiklejohn, and Ian Miers</i>	

Obfuscation

A Simple Obfuscation Scheme for Pattern-Matching with Wildcards	731
<i>Allison Bishop, Lucas Kowalczyk, Tal Malkin, Valerio Pastro, Mariana Raykova, and Kevin Shi</i>	
On the Complexity of Compressing Obfuscation	753
<i>Gilad Asharov, Naomi Ephraim, Ilan Komargodski, and Rafael Pass</i>	

Author Index	785
-------------------------------	-----