Lecture Notes in Computer Science 10992

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

Springer

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

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
Léo Ducas	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
Archita Agarwal
Divesh Aggarwal
Shashank Agrawal
Adi Akavia
Navid Alamati
Martin Albrecht
Miguel Ambrona
Ghous Amjad
Megumi Ando
Ralph Ankele
Gilad Asharov
Achiya Bar-On
Manuel Barbosa
Paulo Barreto
James Bartusek
Guy Barwell
Balthazar Bauer
Carsten Baum
Amos Beimel
Itay Berman
Marc Beunardeau
Sai Lakshmi Bhavana
Simon Blackburn
Estuardo Alpirez Bock
Andrej Bogdanov
André Schrottenloher
Xavier Bonnetain
Charlotte Bonte
Carl Bootland
Jonathan Bootle
Christina Boura
Florian Bourse
Elette Boyle
Zvika Brakerski
Jacqueline Brendel
David Butler
Matteo Campanelli
Brent Carmer
Ignacio Cascudo
Wouter Castryck
Andrea Cerulli
André Chailloux
Nishanth Chandran
Panagiotis Chatzigiannis
Stephen Checkoway
Binyi Chen
Michele Ciampi
Benoit Cogliati
Gil Cohen
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 Hébant
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
Edoardo Persichetti
Duong-Hieu Phan
Krzysztof Pietrzak
Bertram Poettering
David Pointcheval
Antigoni Polychroniadou
Eamonn Postlethwaite
Willy Quach
Elizabeth Quaglia
Samuel Ranellucci
Mariana Raykova
Christian Rechberger
Oded Regev
Nicolas Resch
Leo Reyzin
M. Sadegh Riazi
Silas Richelson
Peter Rindal
Phillip Rogaway
Miruna Rosca
Dragos Rotaru
Yann Rotella
Arnab Roy
Manuel Sabin
Sruthi Sekar
Amin Sakzad
Katerina Samari
Pedro Moreno Sanchez
Sven Schaege
Adam Sealfon
Yannick Seurin
Aria Shahverdi
Tom Shrimpton
Luisa Siniscalchi
Kit Smeets
Fang Song
Pratik Soni
Jessica Sorrell
Florian Speelman
Douglas Stebila
Marc Stevens
Bing Sun
Shifeng Sun
Siwei Sun
Qiang Tang
Seth Terashima
Tian Tian
Mehdi Tibouchi
Yosuke Todo
Aleksei Udovenko
Dominique Unruh
Bogdan Ursu
María Isabel González Vasco
Muthuramakrishnan Venkitasubramaniam
Fre Vercauteren
Fernando Virdia
Alexandre Wallet
Michael Walter
Meiqin Wang
Qingju Wang
Boyang Wei
Mor Weiss
Jan Winkelmann
Tim Wood
David Wu
Hong Xu
Shota Yamada
Hailun Yan
LeCorre Yann
Kan Yasuda
Arkady Yerukhimovich
Eylon Yogev
Yang Yu
Yu Yu
Thomas Zacharias
Wentao Zhang
Hong-Sheng Zhou
Linfeng Zhou
Vassilis Zikas
Giorgos Zirdelis
Lukas Zobernig
Adi Ben Zvi

Sponsors

NSF

aws

ethereum foundatior

INPUT | OUTPUT

JUZIX

moz://a

Protocol Labs

Qualcomm

VISA Research

Western Digital.

ZCASH

FUJITSU

IBM Research

POA

PayPal

CLOUDFLARE

IoTeX

Contents – Part II

Proof Tools

Key Exchange

Symmetric Cryptoanalysis

Hashes and Random Oracles

Trapdoor Functions

Round Optimal MPC

Foundations

Lattices

Lattice-Based ZK

Efficient MPC