

Founding Editors

Gerhard Goos

Karlsruhe Institute of Technology, Karlsruhe, Germany

Juris Hartmanis

Cornell University, Ithaca, NY, USA

Editorial Board Members

Elisa Bertino

Purdue University, West Lafayette, IN, USA

Wen Gao

Peking University, Beijing, China

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Gerhard Woeginger

RWTH Aachen, Aachen, Germany

Moti Yung

Columbia University, New York, NY, USA

More information about this series at <http://www.springer.com/series/7410>

Alexandra Boldyreva · Daniele Micciancio (Eds.)

Advances in Cryptology – CRYPTO 2019

39th Annual International Cryptology Conference
Santa Barbara, CA, USA, August 18–22, 2019
Proceedings, Part II

Editors

Alexandra Boldyreva
Georgia Institute of Technology
Atlanta, GA, USA

Daniele Micciancio
University of California at San Diego
La Jolla, CA, USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-030-26950-0 ISBN 978-3-030-26951-7 (eBook)

<https://doi.org/10.1007/978-3-030-26951-7>

LNCS Sublibrary: SL4 – Security and Cryptology

© International Association for Cryptologic Research 2019

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, expressed 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 39th International Cryptology Conference (Crypto 2019) was held at the University of California, Santa Barbara, California, USA, during August 18–22, 2019. It was sponsored by the International Association for Cryptologic Research (IACR). As in the previous year, a number of workshops took place on the days (August 17 and August 18, 2019) immediately before the conference. This year, the list of affiliated events included a Workshop on Attacks in Cryptography organized by Juraj Somorovsky (Ruhr University Bochum); a Blockchain Workshop organized by Rafael Pass (Cornell Tech) and Elaine Shi (Cornell); a Workshop on Advanced Cryptography Standardization organized by Daniel Benarroch (QEDIT) and Tancrède Lepoint (Google); a workshop on New Roads to Cryptopia organized by Amit Sahai (UCLA); a Privacy Preserving Machine Learning Workshop organized by Gilad Asharov (JP Morgan AI Research), Rafail Ostrovsky (UCLA) and Antigoni Polychroniadou (JP Morgan AI Research); and the Mathcrypt Workshop organized by Kristin Lauter (Microsoft Research), Yongsoo Song (Microsoft Research) and Jung Hee Cheon (Seoul National University).

Crypto continues to grow, year after year, and Crypto 2019 was no exception. The conference set new records for both submissions and publications, with a whopping 378 papers submitted for consideration. It took a Program Committee (PC) of 51 cryptography experts working with 333 external reviewers for over two months to select the 81 papers which were accepted for the conference.

As usual, papers were reviewed in the double-blind fashion, with each paper assigned to three PC members. Initially, papers received independent reviews, without any communication between PC members. After the initial review stage, authors were given the opportunity to comment on all available preliminary reviews. Finally, the PC discussed each submission, taking all reviews and author comments into account, and selecting the list of papers to be included in the conference program. PC members were limited to two submissions, and their submissions were held to higher standards. The two Program Chairs were not allowed to submit papers.

The PC recognized three papers and their authors for standing out amongst the rest. “Cryptanalysis of OCB2: Attacks on Authenticity and Confidentiality”, by Akiko Inoue, Tetsu Iwata, Kazuhiko Minematsu and Bertram Poettering was voted Best Paper of the conference. Additionally, the papers “Quantum cryptanalysis in the RAM model: Claw-finding attacks on SIKE” by Samuel Jaques and John M. Schanck, and “Fully Secure Attribute-Based Encryption for t-CNF from LWE” by Rotem Tsabary, were voted Best Papers Authored Exclusively By Young Researchers.

Beside the technical presentations, Crypto 2019 featured a Rump session, and two invited talks by Jonathan Katz from University of Maryland, and Helen Nissenbaum from Cornell Tech.

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 2019. Additionally, we are very appreciative of the following individuals and organizations for helping make Crypto 2019 a success:

- Muthu Venkitasubramaniam (University of Rochester) - Crypto 2019 General Chair
- Carmit Hazay (Bar-Ilan University) - Workshop Chair
- Jonathan Katz (University of Maryland) - Invited Speaker
- Helen Nissenbaum (Cornell Tech) - Invited Speaker
- Shai Halevi - Author of the IACR Web Submission and Review System
- Anna Kramer and her colleagues at Springer
- Whitney Morris and UCSB Conference Services

We would also like to say thank you to our numerous sponsors, the workshop organizers, everyone who submitted papers, the session chairs, and the presenters. Lastly, a big thanks to everyone who attended the conference at UCSB.

August 2019

Alexandra Boldyreva
Daniele Micciancio

CRYPTO 2019

The 39th International Cryptology Conference

University of California, Santa Barbara, CA, USA
August 18–22, 2019

Sponsored by the *International Association for Cryptologic Research*

General Chair

Muthu Venkitasubramaniam University of Rochester, USA

Program Chairs

Alexandra Boldyreva Georgia Institute of Technology, USA
Daniele Micciancio University of California at San Diego, USA

Program Committee

Manuel Barbosa	INESC TEC, University of Porto, Portugal
Zvika Brakerski	Weizmann Institute of Science, Israel
Mark Bun	Simons Institute, Boston University, USA
Ran Canetti	Tel Aviv University, Israel, and Boston University, USA
Dario Catalano	University of Catania, Italy
Alessandro Chiesa	UC Berkeley, USA
Sherman S. M. Chow	Chinese University of Hong Kong, SAR China
Kai-Min Chung	Academia Sinica, Taiwan
Jean-Sebastien Coron	Luxembourg University, Luxembourg
Jean Paul Degabriele	TU Darmstadt, Germany
Nico Döttling	Cispa Helmholtz Center (i.G.), Germany
Orr Dunkelman	University of Haifa, Israel
Rosario Gennaro	City College, CUNY, USA
Tim Güneysu	Ruhr University Bochum, DFKI, Germany
Felix Günther	UC San Diego, USA
Siyao Guo	NYU Shanghai, China
Sean Hallgren	Pennsylvania State University, USA
Carmit Hazay	Bar-Ilan University, Israel
Susan Hohenberger	Johns Hopkins University, USA
Sorina Ionica	Université de Picardie, France
Bhavana Kanukurthi	Indian Institute of Science, India
Vladimir Kolesnikov	Georgia Institute of Technology, USA

Anja Lehmann	IBM Research Zurich, Switzerland
Vadim Lyubashevsky	IBM Research Zurich, Switzerland
Ilya Mironov	Google
Michael Naehrig	Microsoft Research
Svetla Nikova	KU Leuven, Belgium
Ryo Nishimaki	NTT Secure Platform Labs, Japan
Omer Paneth	MIT, USA
Charalampos Papamanthou	University of Maryland, USA
Chris Peikert	University of Michigan, USA
Giuseppe Persiano	University of Salerno, Italy
Christophe Petit	University of Birmingham, UK
Thomas Peyrin	Nanyang Technological University, Singapore
Benny Pinkas	Bar Ilan University, Israel
Bertram Poettering	Royal Holloway, University of London, UK
Mariana Raykova	Yale University, USA
Silas Richelson	UC Riverside, USA
Adeline Roux-Langlois	University Rennes, CNRS, IRISA, France
Peter Scholl	Aarhus University, Denmark
Dominique Schröder	Friedrich-Alexander-Universität, Germany
Thomas Shrimpton	University of Florida, USA
Damien Stehlé	ENS Lyon, France
Björn Tackmann	IBM Research Zurich, Switzerland
Keisuke Tanaka	Tokyo Institute of Technology, Japan
Erin Tromer	Tel Aviv University, Israel, and Columbia University, USA
Daniele Venturi	Sapienza, University of Rome, Italy
Xiao Wang	MIT, Boston University, USA
Xiaoyun Wang	Tsinghua University, China
Bogdan Warinschi	University of Bristol, UK
Mor Weiss	IDC Herzliya, Israel

Additional Reviewers

Ittai Abraham	Vivek Arte	Paulo S. L. M. Barreto
Shweta Agrawal	Gilad Asharov	James Bartusek
Gorjan Alagic	Tomer Ashur	Carsten Baum
Navid Alamati	Nuttapong Attrapadung	Gabrielle Beck
Younes Talibi Alaoui	Benedikt Auerbach	Amos Beimel
Martin Albrecht	Roberto Avanzi	Sonia Belaid
Joel Alwen	Saikrishna	Fabrice Benhamouda
Prabhanjan Ananth	Badrinarayanan	Pauline Bert
Elena Andreeva	Josep Balasch	Rishabh Bhaduria
Benny Applebaum	Foteini Baldimtsi	Olivier Blazy
Marcel Armour	Marshall Ball	Jeremiah Blocki
Gal Arnon	Achiya Bar-On	Jonathan Bootle

Cecilia Boschini
 Katharina Boudgoust
 Florian Bourse
 Elette Boyle
 Jacqueline Brendel
 Anne Broadbent
 Wouter Castryck
 Andrea Cerulli
 Yilei Chen
 Nai-Hui Chia
 Iliaria Chillotti
 Arka Rai Choudhuri
 Michele Ciampi
 Benoitogliati
 Ran Cohen
 Sandro Coretti
 Craig Costello
 Geoffroy Couteau
 Jan Czakowski
 Dana Dachaman-Soled
 Wei Dai
 Anders Dalskov
 Hannah Davis
 Akshay Degwekar
 Ioannis Demertzis
 Patrick Derbez
 David Derler
 Itai Dinur
 Mario Di Raimondo
 Benjamin Dowling
 Minxin Du
 Léo Lucas
 Yfke Dulek
 Francois Dupressoir
 Frédéric Dupuis
 Stefan Dziembowski
 Gautier Eberhart
 Christoph Egger
 Maria Eichlseder
 Daniel Escudero
 Antonio Faonio
 Franz Aguirre Farro
 Pooya Farshim
 Omar Fawzi
 Katharina Fech
 Ben Fisch

Marc Fischlin
 Emmanuel Fouotsa
 Danilo Francati
 Daniele Friolo
 Ariel Gabizon
 Tommaso Gagliardoni
 Steven Galbraith
 Chaya Ganesh
 Lydia Garms
 Romain Gay
 Ran Gelles
 Adela Georgescu
 David Gerault
 Essam Ghadafi
 Satrajit Ghosh
 Federico Giacon
 Aarushi Goel
 Junqing Gong
 Alonso Gonzalez
 Rishab Goyal
 Vipul Goyal
 Nicola Greco
 Daniel Grosse
 Zichen Gui
 Tim Güneysu
 Chethan Kamath Hosdurg
 Mohammad Hajiabadi
 Lucjan Hanzlik
 Patrick Harasser
 Carmit Hazay
 Julia Hesse
 Minki Hhan
 Kuan-Yi Ho
 Justin Holmgren
 Akinori Hosoyamada
 Patrick Hough
 James Howe
 Pavel Hubáček
 Shih-Han Hung
 Kathrin Hövelmanns
 Takanori Isobe
 Mitsugu Iwamoto
 Malika Izabachène
 Joseph Jaeger
 Christian Janson
 Dirmanto Jap

Stas Jarecki
 Zhengzhong Jin
 Charanjit Jutla
 Guillaume Kaim
 Mustafa Kairallah
 Yael Kalai
 Chethan Kamath
 Marc Kaplan
 Shuichi Katsumata
 Shinagawa Kazumasa
 Mojtaba Khalili
 Dmitry Khovratovich
 Ryo Kikuchi
 Sam Kim
 Elena Kirshanova
 Fuyuki Kitagawa
 Susumu Kiyoshima
 Karen Klein
 Michael Klooss
 Kamil Klucznik
 Markulf Kohlweiss
 Ilan Komargodski
 Venkata Koppula
 Evgenios Kornaropoulos
 Takeshi Koshiba
 Luke Kowalczyk
 Stephan Krenn
 Mukul Kulkarni
 Ranjit Kumaresan
 Gijs Van Laer
 Russell W. F. Lai
 Thalia Laing
 Changmin Lee
 Eysa Lee
 Moon Sung Lee
 Tancrede Lepoint
 Jyun-Jie Liao
 Han-Hsuan Lin
 Huijia (Rachel) Lin
 Helger Lipmaa
 Qipeng Liu
 Tianren Liu
 Alex Lombardi
 Patrick Longa
 Julian Loss
 Atul Luykx

Julio López	Lorenz Panny	Siang Meng Sim
Fermi Ma	Dimitris Papadopoulos	Mark Simkin
Jack P. K. Ma	Anat Paskin-Cherniavsky	Luisa Siniscalchi
Bernardo Magri	Christopher Patton	Fang Song
Mohammad Mahmoody	Alice Pellet-Mary	Pratik Soni
Christian Majenz	Zack Pepin	Katerina Sotiraki
Hemanta Maji	Jeroen Pijnenburg	Nicholas Spooner
Giulio Malavolta	Oxana Poburinnaya	Caleb Springer
Mary Maller	Antigoni Polychroniadou	Akshayaram Srinivasan
Nathan Manohar	Bart Preneel	François-Xavier Standaert
Peter Manohar	Ben Pring	Douglas Stebila
Daniel Masny	Emmanuel Prouff	Damien Stehlé
Takahiro Matsuda	Chen Qian	Ron Steinfeld
Alexander May	Luowen Qian	Noah
Sogol Mazaheri	Willy Quach	Stephens-Davidowitz
Jeremias Mechler	Srinivasan Raghuraman	Christoph Striecks
Simon-Philipp Merz	Adrián Ranea	Patrick Struck
Peihan Miao	Divya Ravi	Banik Subhadeep
Romy Minko	Vincent Rijmen	Gelo Noel Tabia
Takaaki Mizuki	Peter Rindal	Stefano Tessaro
Amir Moradi	Felix Rohrbach	Sri Aravinda Krishnan
Kirill Morozov	Razvan Rosie	Thyagarajan
Travis Morrison	Dragos Rotaru	Mehdi Tibouchi
Nicky Mouha	Ron Rothblum	Elmar W. Tischhauser
Tamer Mour	Arnab Roy	Yosuke Todo
Pratyay Mukherjee	Paul Rösler	Junichi Tomida
Jörn Müller-Quade	Luisa Siniscalchi	Patrick Towa
Kartik Nayak	Mohamed Sabt	Monika Trimoska
Gregory Neven	Rajeev Anand Sahu	Itay Tsabary
Ka-Lok Ng	Cyprien de Saint Guilhem	Rotem Tsabary
Ruth Ng	Kazuo Sakiyama	Sulamithe Tsakou
Ngoc Khanh Nguyen	Pratik Sarkar	Ida Tucker
Ventzislav Nikov	Pascal Sasdrich	Dominique Unruh
Ariel Nof	Alessandra Scafuro	Bogdan Ursu
Sai Lakshmi Bhavana	Falk Schellenberg	Vinod Vaikuntanathan
Obbattu	Thomas Schneider	Kerem Varici
Maciej Obremski	Tobias Schneider	Prashant Vasudevan
Tobias Oder	Jacob Schuldts	Muthu
Sabine Oechsner	Gregor Seiler	Venkatasubramaniam
Wakaha Ogata	Sruthi Sekar	Fernando Virdia
Miyako Ohkubo	Karn Seth	Madars Virza
Cristina Onete	Yannick Seurin	Ivan Visconti
Claudio Orlandi	Aria Shahverdi	Satyanarayana Vusirikala
Emmanuela Orsini	Abhishek Shetty	Riad Wahby
Carles Padro	Sina Shiehian	Adrian Waller
Jiaxin Pan	Javier Silva	Alexandre Wallet

Michael Walter
 Haoyang Wang
 Jiafan Wang
 Meiqin Wang
 Xiuhua Wang
 Yuyu Wang
 Gaven Watson
 Hoeteck Wee
 Weiqiang Wen

Harry W. H. Wong
 Tim Wood
 Joanne Woodage
 Huangting Wu
 Keita Xagawa
 Shota Yamada
 Takashi Yamakawa
 Avishay Yanai
 Kenji Yasunaga

Kevin Yeo
 Eylon Yogev
 Yu Yu
 Mark Zhandry
 Jiapeng Zhang
 Yupeng Zhang
 Yongjun Zhao
 Yu Zheng

Sponsors





PlatON



Contents – Part II

MPC Communication Complexity

The Communication Complexity of Threshold Private Set Intersection.	3
<i>Satrajit Ghosh and Mark Simkin</i>	
Adaptively Secure MPC with Sublinear Communication Complexity.	30
<i>Ran Cohen, Abhi Shelat, and Daniel Wichs</i>	
Communication Lower Bounds for Statistically Secure MPC, With or Without Preprocessing.	61
<i>Ivan Damgård, Kasper Green Larsen, and Jesper Buus Nielsen</i>	
Communication-Efficient Unconditional MPC with Guaranteed Output Delivery.	85
<i>Vipul Goyal, Yanyi Liu, and Yifan Song</i>	

Symmetric Cryptanalysis

Efficient Collision Attack Frameworks for RIPEMD-160.	117
<i>Fukang Liu, Christoph Dobraunig, Florian Mendel, Takanori Isobe, Gaoli Wang, and Zhenfu Cao</i>	
Improving Attacks on Round-Reduced Speck32/64 Using Deep Learning . . .	150
<i>Aron Gohr</i>	
Correlation of Quadratic Boolean Functions: Cryptanalysis of All Versions of Full MORUS.	180
<i>Danping Shi, Siwei Sun, Yu Sasaki, Chaoyun Li, and Lei Hu</i>	
Low-Memory Attacks Against Two-Round Even-Mansour Using the 3-XOR Problem.	210
<i>Gaëtan Leurent and Ferdinand Sibleyras</i>	

(Post) Quantum Cryptography

How to Record Quantum Queries, and Applications to Quantum Indifferentiability.	239
<i>Mark Zhandry</i>	
Quantum Security Proofs Using Semi-classical Oracles.	269
<i>Andris Ambainis, Mike Hamburg, and Dominique Unruh</i>	

Quantum Indistinguishability of Random Sponges	296
<i>Jan Czajkowski, Andreas Hülsing, and Christian Schaffner</i>	
Revisiting Post-quantum Fiat-Shamir	326
<i>Qipeng Liu and Mark Zhandry</i>	
Security of the Fiat-Shamir Transformation in the Quantum Random-Oracle Model	356
<i>Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner</i>	
Leakage Resilience	
Unconditionally Secure Computation Against Low-Complexity Leakage	387
<i>Andrej Bogdanov, Yuval Ishai, and Akshayaram Srinivasan</i>	
Tight Leakage-Resilient CCA-Security from Quasi-Adaptive Hash Proof System	417
<i>Shuai Han, Shengli Liu, Lin Lyu, and Dawu Gu</i>	
Non-malleable Secret Sharing in the Computational Setting: Adaptive Tampering, Noisy-Leakage Resilience, and Improved Rate	448
<i>Antonio Faonio and Daniele Venturi</i>	
Leakage Resilient Secret Sharing and Applications	480
<i>Akshayaram Srinivasan and Prashant Nalini Vasudevan</i>	
Stronger Leakage-Resilient and Non-Malleable Secret Sharing Schemes for General Access Structures	510
<i>Divesh Aggarwal, Ivan Damgård, Jesper Buus Nielsen, Maciej Obremski, Erick Purwanto, João Ribeiro, and Mark Simkin</i>	
Memory Hard Functions and Privacy Amplification	
Memory-Hard Functions from Cryptographic Primitives	543
<i>Binyi Chen and Stefano Tessaro</i>	
Data-Independent Memory Hard Functions: New Attacks and Stronger Constructions	573
<i>Jeremiah Blocki, Ben Harsha, Siteng Kang, Seunghoon Lee, Lu Xing, and Samson Zhou</i>	
Simultaneous Amplification: The Case of Non-interactive Zero-Knowledge . . .	608
<i>Vipul Goyal, Aayush Jain, and Amit Sahai</i>	
The Privacy Blanket of the Shuffle Model	638
<i>Borja Balle, James Bell, Adrià Gascón, and Kobbi Nissim</i>	

Attribute Based Encryption

Realizing Chosen Ciphertext Security Generically in Attribute-Based Encryption and Predicate Encryption	671
<i>Venkata Koppula and Brent Waters</i>	
Match Me if You Can: Matchmaking Encryption and Its Applications.	701
<i>Giuseppe Ateniese, Danilo Francati, David Nuñez, and Daniele Venturi</i>	
ABE for DFA from k -Lin	732
<i>Junqing Gong, Brent Waters, and Hoeteck Wee</i>	
Attribute Based Encryption (and more) for Nondeterministic Finite Automata from LWE	765
<i>Shweta Agrawal, Monosij Maitra, and Shota Yamada</i>	

Foundations

The Distinction Between Fixed and Random Generators in Group-Based Assumptions	801
<i>James Bartusek, Fermi Ma, and Mark Zhandry</i>	
Unifying Computational Entropies via Kullback–Leibler Divergence	831
<i>Rohit Agrawal, Yi-Hsiu Chen, Thibaut Horel, and Salil Vadhan</i>	
Author Index	859