Lecture Notes in Computer Science 11692

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 I

Springer

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 978-3-030-26947-0 ISBN 978-3-030-26948-7 (eBook)
https://doi.org/10.1007/978-3-030-26948-7

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
Eran 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 Badrinarayanan	Fabrice Benhamouda
Prabhanjan Ananth	Josep Balasch	Pauline Bert
Elena Andreeva	Foteini Baldimtsi	Rishabh Bhadauria
Benny Applebaum	Marshall Ball	Olivier Blazy
Marcel Armour	Achiya Bar-On	Jeremiah Blocki
Gal Arnon		Jonathan Bootle

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













VISA
Research

Contents – Part I

Award Papers

Cryptanalysis of OCB2: Attacks on Authenticity and Confidentiality 3
Akiko Inoue, Tetsu Iwata, Kazuhiko Minematsu, and Bertram Poettering

Quantum Cryptanalysis in the RAM Model: Claw-Finding Attacks on SIKE 32
Samuel Jaques and John M. Schanck

Fully Secure Attribute-Based Encryption for *t*-CNF from LWE. 62
Rotem Tsabary

Lattice-Based ZK

Noninteractive Zero Knowledge for NP from (Plain) Learning with Errors . . . 89
Chris Peikert and Sina Shiehian

Lattice-Based Zero-Knowledge Proofs: New Techniques for Shorter and Faster Constructions and Applications 115
Muhammed F. Esgin, Ron Steinfeld, Joseph K. Liu, and Dongxi Liu

Efficient Lattice-Based Zero-Knowledge Arguments with Standard Soundness: Construction and Applications 147
Rupeng Yang, Man Ho Au, Zhenfei Zhang, Qiuliang Xu, Zuoxia Yu, and William Whyte

Algebraic Techniques for Short(er) Exact Lattice-Based Zero-Knowledge Proofs 176
Jonathan Bootle, Vadim Lyubashevsky, and Gregor Seiler

Symmetric Cryptography

Seedless Fruit Is the Sweetest: Random Number Generation, Revisited 205
Sandro Coretti, Yevgeniy Dodis, Harish Karthikeyan, and Stefano Tessaro

Nonces Are Noticed: AEAD Revisited. 235
Mihir Bellare, Ruth Ng, and Björn Tackmann

How to Build Pseudorandom Functions from Public Random Permutations . . . 266
Yu Long Chen, Eran Lambooij, and Bart Mennink

Mathematical Cryptanalysis

New Results on Modular Inversion Hidden Number Problem and Inversive Congruential Generator 297
Jun Xu, Santanu Sarkar, Lei Hu, Huaxiong Wang, and Yanbin Pan

On the Shortness of Vectors to Be Found by the Ideal-SVP Quantum Algorithm 322
Léo Ducas, Maxime Plançon, and Benjamin Wesolowski

Proofs of Storage

Proofs of Replicated Storage Without Timing Assumptions 355
Ivan Damgård, Chaya Ganesh, and Claudio Orlandi

Simple Proofs of Space-Time and Rational Proofs of Storage 381
Tal Moran and Ilan Orlov

Non-Malleable Codes

Non-malleable Codes for Decision Trees 413
Marshall Ball, Siyao Guo, and Daniel Wichs

Explicit Rate-1 Non-malleable Codes for Local Tampering. 435
Divya Gupta, Hemanta K. Maji, and Mingyuan Wang

Continuous Space-Bounded Non-malleable Codes from Stronger Proofs-of-Space 467
Binyi Chen, Yilei Chen, Kristina Hostáková, and Pratyay Mukherjee

SNARKs and Blockchains

Synchronous, with a Chance of Partition Tolerance 499
Yue Guo, Rafael Pass, and Elaine Shi

Subvector Commitments with Application to Succinct Arguments 530
Russell W. F. Lai and Giulio Malavolta

Batching Techniques for Accumulators with Applications to IOPs and Stateless Blockchains. 561
Dan Boneh, Benedikt Bünz, and Ben Fisch

Homomorphic Cryptography

On the Plausibility of Fully Homomorphic Encryption for RAMs 589
Ariel Hamlin, Justin Holmgren, Mor Weiss, and Daniel Wichs

Homomorphic Time-Lock Puzzles and Applications 620
Giulio Malavolta and Sri Aravinda Krishnan Thyagarajan

Symmetric Primitives with Structured Secrets 650
Navid Alamati, Hart Montgomery, and Sikhar Patranabis

Leakage Models and Key Reuse

Unifying Leakage Models on a Rényi Day 683
Thomas Prest, Dahmun Goudarzi, Ange Martinelli, and Alain Passelègue

Leakage Certification Revisited: Bounding Model Errors in Side-Channel Security Evaluations 713
Olivier Bronchain, Julien M. Hendrickx, Clément Massart, Alex Olshevsky, and François-Xavier Standaert

Security in the Presence of Key Reuse: Context-Separable Interfaces and Their Applications. 738
Christopher Patton and Thomas Shrimpton

Author Index 769

Contents – Part II

MPC Communication Complexity

The Communication Complexity of Threshold Private Set Intersection 3
Satrajit Ghosh and Mark Simkin

Adaptively Secure MPC with Sublinear Communication Complexity 30
Ran Cohen, Abhi Shelat, and Daniel Wichs

Communication Lower Bounds for Statistically Secure MPC, With or Without Preprocessing 61
Ivan Damgård, Kasper Green Larsen, and Jesper Buus Nielsen

Communication-Efficient Unconditional MPC with Guaranteed Output Delivery 85
Vipul Goyal, Yanyi Liu, and Yifan Song

Symmetric Cryptanalysis

Efficient Collision Attack Frameworks for RIPEMD-160 117
Fukang Liu, Christoph Dobraunig, Florian Mendel, Takanori Isobe, Gaoli Wang, and Zhenfu Cao

Improving Attacks on Round-Reduced Speck32/64 Using Deep Learning . . . 150
Aron Gohr

Correlation of Quadratic Boolean Functions: Cryptanalysis of All Versions of Full MORUS 180
Danping Shi, Siwei Sun, Yu Sasaki, Chaoyun Li, and Lei Hu

Low-Memory Attacks Against Two-Round Even-Mansour Using the 3-XOR Problem 210
Gaëtan Leurent and Ferdinand Sibleyras

(Post) Quantum Cryptography

How to Record Quantum Queries, and Applications to Quantum Indifferentiability 239
Mark Zhandry

Quantum Security Proofs Using Semi-classical Oracles 269
Andris Ambainis, Mike Hamburg, and Dominique Unruh

Quantum Indistinguishability of Random Sponges 296
Jan Czajkowski, Andreas Hülsing, and Christian Schaffner

Revisiting Post-quantum Fiat-Shamir 326
Qipeng Liu and Mark Zhandry

Security of the Fiat-Shamir Transformation in the Quantum Random-Oracle Model 356
Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner

Leakage Resilience

Unconditionally Secure Computation Against Low-Complexity Leakage 387
Andrej Bogdanov, Yuval Ishai, and Akshayaram Srinivasan

Tight Leakage-Resilient CCA-Security from Quasi-Adaptive Hash Proof System 417
Shuai Han, Shengli Liu, Lin Lyu, and Dawu Gu

Non-malleable Secret Sharing in the Computational Setting: Adaptive Tampering, Noisy-Leakage Resilience, and Improved Rate 448
Antonio Faonio and Daniele Venturi

Leakage Resilient Secret Sharing and Applications 480
Akshayaram Srinivasan and Prashant Nalini Vasudevan

Stronger Leakage-Resilient and Non-Malleable Secret Sharing Schemes for General Access Structures 510
Divesh Aggarwal, Ivan Damgård, Jesper Buus Nielsen, Maciej Obremski, Erick Purwanto, João Ribeiro, and Mark Simkin

Memory Hard Functions and Privacy Amplification

Memory-Hard Functions from Cryptographic Primitives 543
Binyi Chen and Stefano Tessaro

Data-Independent Memory Hard Functions: New Attacks and Stronger Constructions 573
Jeremiah Blocki, Ben Harsha, Siteng Kang, Seunghoon Lee, Lu Xing, and Samson Zhou

Simultaneous Amplification: The Case of Non-interactive Zero-Knowledge . . . 608
Vipul Goyal, Aayush Jain, and Amit Sahai

The Privacy Blanket of the Shuffle Model 638
Borja Balle, James Bell, Adrià Gascón, and Kobbi Nissim

Attribute Based Encryption

Realizing Chosen Ciphertext Security Generically in Attribute-Based Encryption and Predicate Encryption 671
Venkata Koppula and Brent Waters

Match Me if You Can: Matchmaking Encryption and Its Applications 701
Giuseppe Ateniese, Danilo Francati, David Nuñez, and Daniele Venturi

ABE for DFA from *k*-Lin 732
Junqing Gong, Brent Waters, and Hoeteck Wee

Attribute Based Encryption (and more) for Nondeterministic Finite Automata from LWE 765
Shweta Agrawal, Monosij Maitra, and Shota Yamada

Foundations

The Distinction Between Fixed and Random Generators in Group-Based Assumptions 801
James Bartusek, Fermi Ma, and Mark Zhandry

Unifying Computational Entropies via Kullback–Leibler Divergence 831
Rohit Agrawal, Yi-Hsiu Chen, Thibaut Horel, and Salil Vadhan

Author Index 859

Contents – Part III

Trapdoor Functions

Trapdoor Hash Functions and Their Applications 3
Nico Döttling, Sanjam Garg, Yuval Ishai, Giulio Malavolta, Tamer Mour, and Rafail Ostrovsky

CCA Security and Trapdoor Functions via Key-Dependent-Message Security 33
Fuyuki Kitagawa, Takahiro Matsuda, and Keisuke Tanaka

Zero Knowledge I

Zero-Knowledge Proofs on Secret-Shared Data via Fully Linear PCPs 67
Dan Boneh, Elette Boyle, Henry Corrigan-Gibbs, Niv Gilboa, and Yuval Ishai

Non-Uniformly Sound Certificates with Applications to Concurrent Zero-Knowledge 98
Cody Freitag, Ilan Komargodski, and Rafael Pass

On Round Optimal Statistical Zero Knowledge Arguments 128
Nir Bitansky and Omer Paneth

Signatures and Messaging

It Wasn't Me! Repudiability and Claimability of Ring Signatures 159
Sunoo Park and Adam Sealfon

Two-Party ECDSA from Hash Proof Systems and Efficient Instantiations . . . 191
Guilhem Castagnos, Dario Catalano, Fabien Laguillaumie, Federico Savasta, and Ida Tucker

Asymmetric Message Franking: Content Moderation for Metadata-Private End-to-End Encryption 222
Nirvan Tyagi, Paul Grubbs, Julia Len, Ian Miers, and Thomas Ristenpart

Obfuscation

Statistical Zeroizing Attack: Cryptanalysis of Candidates of BP Obfuscation over GGH15 Multilinear Map 253
Jung Hee Cheon, Wonhee Cho, Minki Hhan, Jiseung Kim, and Changmin Lee

Indistinguishability Obfuscation Without Multilinear Maps: New Paradigms via Low Degree Weak Pseudorandomness and Security Amplification 284
Prabhanjan Ananth, Aayush Jain, Huijia Lin, Christian Matt, and Amit Sahai

Watermarking

Watermarking PRFs from Lattices: Stronger Security via Extractable PRFs. . . . 335
Sam Kim and David J. Wu

Watermarking Public-Key Cryptographic Primitives 367
Rishab Goyal, Sam Kim, Nathan Manohar, Brent Waters, and David J. Wu

Secure Computation

SpOT-Light: Lightweight Private Set Intersection from Sparse OT Extension 401
Benny Pinkas, Mike Rosulek, Ni Trieu, and Avishay Yanai

Universally Composable Secure Computation with Corrupted Tokens 432
Nishanth Chandran, Wutichai Chongchitmate, Rafail Ostrovsky, and Ivan Visconti

Reusable Non-Interactive Secure Computation 462
Melissa Chase, Yevgeniy Dodis, Yuval Ishai, Daniel Kraschewski, Tianren Liu, Rafail Ostrovsky, and Vinod Vaikuntanathan

Efficient Pseudorandom Correlation Generators: Silent OT Extension and More 489
Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, and Peter Scholl

Various Topics

Adaptively Secure and Succinct Functional Encryption: Improving Security and Efficiency, Simultaneously 521
Fuyuki Kitagawa, Ryo Nishimaki, Keisuke Tanaka, and Takashi Yamakawa

Non-interactive Non-malleability from Quantum Supremacy 552
Yael Tauman Kalai and Dakshita Khurana

Cryptographic Sensing 583
Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai

Public-Key Cryptography in the Fine-Grained Setting 605
Rio LaVigne, Andrea Lincoln, and Virginia Vassilevska Williams

Zero Knowledge II

Exploring Constructions of Compact NIZKs from Various Assumptions 639
Shuichi Katsumata, Ryo Nishimaki, Shota Yamada, and Takashi Yamakawa

New Constructions of Reusable Designated-Verifier NIZKs 670
Alex Lombardi, Willy Quach, Ron D. Rothblum, Daniel Wichs, and David J. Wu

Scalable Zero Knowledge with No Trusted Setup 701
Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev

Libra: Succinct Zero-Knowledge Proofs with Optimal Prover Computation. . . . 733
Tiacheng Xie, Jiaheng Zhang, Yupeng Zhang, Charalampos Papamanthou, and Dawn Song

Key Exchange and Broadcast Encryption

Highly Efficient Key Exchange Protocols with Optimal Tightness. 767
Katriel Cohn-Gordon, Cas Cremers, Kristian Gjøsteen, Håkon Jacobsen, and Tibor Jager

Strong Asymmetric PAKE Based on Trapdoor CKEM. 798
Tatiana Bradley, Stanislaw Jarecki, and Jiayu Xu

Broadcast and Trace with N^{ε} Ciphertext Size from Standard Assumptions . . . 826
Rishab Goyal, Willy Quach, Brent Waters, and Daniel Wichs

Author Index 857