Lecture Notes in Computer Science 10991

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 I

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 978-3-319-96883-4 ISBN 978-3-319-96884-1 (eBook)
https://doi.org/10.1007/978-3-319-96884-1

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
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	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 Alamati	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 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
foundation


INPUT | OUTPUT


JUZIX


moz://a


Protocol
Labs


Qualcomm


VISA
Research

Western Digital.


CASH


FUJITSU

IBM Research


POA


PayPal


CLOUDFLARE


IoTeX

Contents – Part I

Secure Messaging

Towards Bidirectional Ratcheted Key Exchange 3
Bertram Poettering and Paul Rösler

Optimal Channel Security Against Fine-Grained State Compromise: The Safety of Messaging 33
Joseph Jaeger and Igors Stepanovs

Out-of-Band Authentication in Group Messaging: Computational, Statistical, Optimal 63
Lior Rotem and Gil Segev

Implementations and Physical Attacks Prevention

Faster Homomorphic Linear Transformations in HElib. 93
Shai Halevi and Victor Shoup

CAPA: The Spirit of Beaver Against Physical Attacks. 121
Oscar Reparaz, Lauren De Meyer, Begül Bilgin, Victor Arribas, Svetla Nikova, Ventzislav Nikov, and Nigel Smart

Authenticated and Format-Preserving Encryption

Fast Message Franking: From Invisible Salamanders to Encryptment. 155
Yevgeniy Dodis, Paul Grubbs, Thomas Ristenpart, and Joanne Woodage

Indifferentiable Authenticated Encryption. 187
Manuel Barbosa and Pooya Farshim

The Curse of Small Domains: New Attacks on Format-Preserving Encryption 221
Viet Tung Hoang, Stefano Tessaro, and Ni Trieu

Cryptoanalysis

Cryptanalysis via Algebraic Spans. 255
Adi Ben-Zvi, Arkadius Kalka, and Boaz Tsaban

Improved Division Property Based Cube Attacks Exploiting Algebraic Properties of Superpoly 275
Qingju Wang, Yonglin Hao, Yosuke Todo, Chaoyun Li, Takanori Isobe, and Willi Meier

Generic Attacks Against Beyond-Birthday-Bound MACs 306
Gaëtan Leurent, Mridul Nandi, and Ferdinand Sibleyras

Searchable Encryption and Differential Privacy

Structured Encryption and Leakage Suppression 339
Seny Kamara, Tarik Moataz, and Olya Ohrimenko

Searchable Encryption with Optimal Locality: Achieving Sublogarithmic Read Efficiency 371
Ioannis Demertzis, Dimitrios Papadopoulos, and Charalampos Papamanthou

Tight Tradeoffs in Searchable Symmetric Encryption 407
Gilad Asharov, Gil Segev, and Ido Shahaf

Hardness of Non-interactive Differential Privacy from One-Way Functions 437
Lucas Kowalczyk, Tal Malkin, Jonathan Ullman, and Daniel Wichs

Risky Traitor Tracing and New Differential Privacy Negative Results 467
Rishab Goyal, Venkata Koppula, Andrew Russell, and Brent Waters

Secret Sharing

Non-malleable Secret Sharing for General Access Structures 501
Vipul Goyal and Ashutosh Kumar

On the Local Leakage Resilience of Linear Secret Sharing Schemes 531
Fabrice Benhamouda, Akshay Degwekar, Yuval Ishai, and Tal Rabin

Encryption

Threshold Cryptosystems from Threshold Fully Homomorphic Encryption . . . 565
Dan Boneh, Rosario Gennaro, Steven Goldfeder, Aayush Jain, Sam Kim, Peter M. R. Rasmussen, and Amit Sahai

Multi-Input Functional Encryption for Inner Products: Function-Hiding Realizations and Constructions Without Pairings 597
Michel Abdalla, Dario Catalano, Dario Fiore, Romain Gay, and Bogdan Ursu

Symmetric Cryptography

Encrypt or Decrypt? To Make a Single-Key Beyond Birthday Secure Nonce-Based MAC 631
Nilanjan Datta, Avijit Dutta, Mridul Nandi, and Kan Yasuda

Rasta: A Cipher with Low ANDdepth and Few ANDs per Bit 662
Christoph Dobraunig, Maria Eichlseder, Lorenzo Grassi, Virginie Lallemand, Gregor Leander, Eik List, Florian Mendel, and Christian Rechberger

Non-Uniform Bounds in the Random-Permutation, Ideal-Cipher, and Generic-Group Models 693
Sandro Coretti, Yevgeniy Dodis, and Siyao Guo

Provable Security of (Tweakable) Block Ciphers Based on Substitution-Permutation Networks 722
Benoît Cogliati, Yevgeniy Dodis, Jonathan Katz, Jooyoung Lee, John Steinberger, Aishwarya Thiruvengadam, and Zhe Zhang

Proofs of Work and Proofs of Stake

Verifiable Delay Functions 757
Dan Boneh, Joseph Bonneau, Benedikt Bünz, and Ben Fisch

Proofs of Work From Worst-Case Assumptions 789
Marshall Ball, Alon Rosen, Manuel Sabin, and Prashant Nalini Vasudevan

Author Index 821

Contents – Part II

Proof Tools

Simplifying Game-Based Definitions: Indistinguishability up to Correctness and Its Application to Stateful AE 3
Phillip Rogaway and Yusi Zhang

The Algebraic Group Model and its Applications 33
Georg Fuchsbauer, Eike Kiltz, and Julian Loss

Key Exchange

On Tightly Secure Non-Interactive Key Exchange 65
Julia Hesse, Dennis Hofheinz, and Lisa Kohl

Practical and Tightly-Secure Digital Signatures and Authenticated Key Exchange 95
Kristian Gjøsteen and Tibor Jager

Symmetric Cryptoanalysis

Fast Correlation Attack Revisited: Cryptanalysis on Full Grain-128a, Grain-128, and Grain-v1 129
Yosuke Todo, Takanori Isobe, Willi Meier, Kazumaro Aoki, and Bin Zhang

A Key-Recovery Attack on 855-round Trivium 160
Ximing Fu, Xiaoyun Wang, Xiaoyang Dong, and Willi Meier

Improved Key Recovery Attacks on Reduced-Round AES with Practical Data and Memory Complexities 185
Achiya Bar-On, Orr Dunkelman, Nathan Keller, Eyal Ronen, and Adi Shamir

Bernstein Bound on WCS is Tight: Repairing Luykx-Preneel Optimal Forgeries 213
Mridul Nandi

Hashes and Random Oracles

Correcting Subverted Random Oracles 241
Alexander Russell, Qiang Tang, Moti Yung, and Hong-Sheng Zhou

Combiners for Backdoored Random Oracles 272
Balthazar Bauer, Pooya Farshim, and Sogol Mazaheri

On Distributional Collision Resistant Hashing 303
Ilan Komargodski and Eylon Yogev

Trapdoor Functions

Fast Distributed RSA Key Generation for Semi-honest and Malicious Adversaries 331
Tore Kasper Frederiksen, Yehuda Lindell, Valery Osheter, and Benny Pinkas

Trapdoor Functions from the Computational Diffie-Hellman Assumption 362
Sanjam Garg and Mohammad Hajiabadi

Round Optimal MPC

Round-Optimal Secure Multiparty Computation with Honest Majority 395
Prabhanjan Ananth, Arka Rai Choudhuri, Aarushi Goel, and Abhishek Jain

On the Exact Round Complexity of Secure Three-Party Computation 425
Arpita Patra and Divya Ravi

Promise Zero Knowledge and Its Applications to Round Optimal MPC 459
Saikrishna Badrinarayanan, Vipul Goyal, Abhishek Jain, Yael Tauman Kalai, Dakshita Khurana, and Amit Sahai

Round-Optimal Secure Multi-Party Computation 488
Shai Halevi, Carmit Hazay, Antigoni Polychroniadou, and Muthuramakrishnan Venkitasubramaniam

Foundations

Yes, There is an Oblivious RAM Lower Bound! 523
Kasper Green Larsen and Jesper Buus Nielsen

Constrained PRFs for NC^1 in Traditional Groups 543
Nuttapong Attrapadung, Takahiro Matsuda, Ryo Nishimaki, Shota Yamada, and Takashi Yamakawa

Lattices

GGH15 Beyond Permutation Branching Programs: Proofs, Attacks, and Candidates 577
Yilei Chen, Vinod Vaikuntanathan, and Hoeteck Wee

Lower Bounds on Lattice Enumeration with Extreme Pruning 608
Yoshinori Aono, Phong Q. Nguyen, Takenobu Seito, and Junji Shikata

Dissection-BKW 638
Andre Esser, Felix Heuer, Robert Kübler, Alexander May, and Christian Sohler

Lattice-Based ZK

Sub-linear Lattice-Based Zero-Knowledge Arguments for Arithmetic Circuits 669
Carsten Baum, Jonathan Bootle, Andrea Cerulli, Rafael del Pino, Jens Groth, and Vadim Lyubashevsky

Lattice-Based Zero-Knowledge Arguments for Integer Relations 700
Benoît Libert, San Ling, Khoa Nguyen, and Huaxiong Wang

Multi-Theorem Preprocessing NIZKs from Lattices 733
Sam Kim and David J. Wu

Efficient MPC

SPD$\mathbb{Z}_{2^k}$: Efficient MPC mod 2^k for Dishonest Majority 769
Ronald Cramer, Ivan Damgård, Daniel Escudero, Peter Scholl, and Chaoping Xing

Yet Another Compiler for Active Security or: Efficient MPC Over Arbitrary Rings 799
Ivan Damgård, Claudio Orlandi, and Mark Simkin

Author Index 831

Contents – Part III

Efficient MPC

TinyKeys: A New Approach to Efficient Multi-Party Computation 3
Carmit Hazay, Emmanuela Orsini, Peter Scholl, and Eduardo Soria-Vazquez

Fast Large-Scale Honest-Majority MPC for Malicious Adversaries 34
Koji Chida, Daniel Genkin, Koki Hamada, Dai Ikarashi, Ryo Kikuchi, Yehuda Lindell, and Ariel Nof

Quantum Cryptography

Quantum FHE (Almost) As Secure As Classical 67
Zvika Brakerski

IND-CCA-Secure Key Encapsulation Mechanism in the Quantum Random Oracle Model, Revisited 96
Haodong Jiang, Zhenfeng Zhang, Long Chen, Hong Wang, and Zhi Ma

Pseudorandom Quantum States 126
Zhengfeng Ji, Yi-Kai Liu, and Fang Song

Quantum Attacks Against Indistinguishablility Obfuscators Proved Secure in the Weak Multilinear Map Model 153
Alice Pellet-Mary

Cryptanalyses of Branching Program Obfuscations over GGH13 Multilinear Map from the NTRU Problem 184
Jung Hee Cheon, Minki Hhan, Jiseung Kim, and Changmin Lee

MPC

An Optimal Distributed Discrete Log Protocol with Applications to Homomorphic Secret Sharing 213
Itai Dinur, Nathan Keller, and Ohad Klein

Must the Communication Graph of MPC Protocols be an Expander?. 243
Elette Boyle, Ran Cohen, Deepesh Data, and Pavel Hubáček

Two-Round Multiparty Secure Computation Minimizing Public Key Operations. 273
Sanjam Garg, Peihan Miao, and Akshayaram Srinivasan

Limits of Practical Sublinear Secure Computation 302
Elette Boyle, Yuval Ishai, and Antigoni Polychroniadou

Garbling

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

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

Information-Theoretic MPC

Amortized Complexity of Information-Theoretically Secure MPC Revisited . . . 395
Ignacio Cascudo, Ronald Cramer, Chaoping Xing, and Chen Yuan

Private Circuits: A Modular Approach 427
Prabhanjan Ananth, Yuval Ishai, and Amit Sahai

Various Topics

A New Public-Key Cryptosystem via Mersenne Numbers 459
Divesh Aggarwal, Antoine Joux, Anupam Prakash, and Miklos Santha

Fast Homomorphic Evaluation of Deep Discretized Neural Networks 483
Florian Bourse, Michele Minelli, Matthias Minihold, and Pascal Paillier

Oblivious Transfer

Adaptive Garbled RAM from Laconic Oblivious Transfer 515
Sanjam Garg, Rafail Ostrovsky, and Akshayaram Srinivasan

On the Round Complexity of OT Extension 545
Sanjam Garg, Mohammad Mahmoody, Daniel Masny, and Izaak Meckler

Non-malleable Codes

Non-Malleable Codes for Partial Functions with Manipulation Detection 577
Aggelos Kiayias, Feng-Hao Liu, and Yiannis Tselekounis

Continuously Non-Malleable Codes in the Split-State Model from Minimal Assumptions 608
Rafail Ostrovsky, Giuseppe Persiano, Daniele Venturi, and Ivan Visconti

Zero Knowledge

Non-Interactive Zero-Knowledge Proofs for Composite Statements 643
Shashank Agrawal, Chaya Ganesh, and Payman Mohassel

From Laconic Zero-Knowledge to Public-Key Cryptography:
Extended Abstract 674
Itay Berman, Akshay Degwekar, Ron D. Rothblum,
and Prashant Nalini Vasudevan

Updatable and Universal Common Reference Strings with Applications
to zk-SNARKs 698
Jens Groth, Markulf Kohlweiss, Mary Maller, Sarah Meiklejohn,
and Ian Miers

Obfuscation

A Simple Obfuscation Scheme for Pattern-Matching with Wildcards 731
Allison Bishop, Lucas Kowalczyk, Tal Malkin, Valerio Pastro,
Mariana Raykova, and Kevin Shi

On the Complexity of Compressing Obfuscation 753
Gilad Asharov, Naomi Ephraim, Ilan Komargodski, and Rafael Pass

Author Index 785