

*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>

Amos Beimel · Stefan Dziembowski (Eds.)

# Theory of Cryptography

16th International Conference, TCC 2018  
Panaji, India, November 11–14, 2018  
Proceedings, Part I

*Editors*

Amos Beimel  
Ben Gurion University  
Beer Sheva, Israel

Stefan Dziembowski  
University of Warsaw  
Warsaw, Poland

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-030-03806-9              ISBN 978-3-030-03807-6 (eBook)  
<https://doi.org/10.1007/978-3-030-03807-6>

Library of Congress Control Number: 2018960441

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 16th Theory of Cryptography Conference (TCC 2018) was held during November 11–14, 2018, at the Cidade de Goa hotel, in Panaji, Goa, India. It was sponsored by the International Association for Cryptologic Research (IACR). The general chairs of the conference were Shweta Agrawal and Manoj Prabhakaran. We would like to thank them for their hard work in organizing the conference.

The conference received 168 submissions, of which the Program Committee (PC) selected 50 for presentation (with two pairs of papers sharing a single presentation slot per pair). Each submission was reviewed by at least three PC members, often more. The 30 PC members (including PC chairs), all top researchers in our field, were helped by 211 external reviewers, who were consulted when appropriate. These proceedings consist of the revised version of the 50 accepted papers. The revisions were not reviewed, and the authors bear full responsibility for the content of their papers.

As in previous years, we used Shai Halevi’s excellent Web-review software, and are extremely grateful to him for writing it, and for providing fast and reliable technical support whenever we had any questions. Based on the experience from previous years, we again made use of the interaction feature supported by the review software, where PC members may anonymously interact with authors. This was used to ask specific technical questions, such as suspected bugs. We felt this approach helped us prevent potential misunderstandings and improved the quality of the review process.

This was the fifth year that TCC presented the Test of Time Award to an outstanding paper that was published at TCC at least eight years ago, making a significant contribution to the theory of cryptography, preferably with influence also in other areas of cryptography, theory, and beyond. This year the Test of Time Award Committee selected the following paper, published at TCC 2005: “Evaluating 2-DNF Formulas on Ciphertexts” by Dan Boneh, Eu-Jin Goh, and Kobbi Nissim. This paper was selected for introducing compact two-operation homomorphic encryption and developing new bilinear map techniques that led to major improvements in the design of cryptographic schemes. The authors were also invited to deliver a talk at TCC 2018. A Best Student Paper Award was given to Tianren Liu for his paper “On Basing Search SIVP on NP-Hardness.”

The conference also featured two other invited talks, by Moni Naor and by Daniel Wichs.

We are greatly indebted to many people who were involved in making TCC 2018 a success. First of all, a big thanks to the most important contributors: all the authors who submitted papers to the conference. Next, we would like to thank the PC members for their hard work, dedication, and diligence in reviewing the papers, verifying the correctness, and in-depth discussion. We are also thankful to the external reviewers for their volunteered hard work and investment in reviewing papers and answering questions, often under time pressure. For running the conference itself, we are very grateful to the general chairs, Shweta Agrawal and Manoj Prabhakaran. We appreciate

the sponsorship from the IACR, Microsoft Research, IBM, and Google. We also wish to thank IIT Madras and IIT Bombay for their support. Finally, we are thankful to the TCC Steering Committee as well as the entire thriving and vibrant TCC community.

November 2018

Amos Beimel  
Stefan Dziembowski  
TCC 2018 Program Chairs

# TCC 2018

## The 16th Theory of Cryptography Conference

Goa, India

November 11–14, 2018

Sponsored by the *International Association for Cryptologic Research*

### General Chairs

Shweta Agrawal  
Manoj Prabhakaran

Indian Institute of Technology, Madras, India  
Indian Institute of Technology, Bombay, India

### Program Committee

Masayuki Abe	NTT and Kyoto University, Japan
Divesh Aggarwal	National University of Singapore, Singapore
Shweta Agrawal	Indian Institute of Technology, Madras, India
Gilad Asharov	Cornell Tech, USA
Amos Beimel (Co-chair)	Ben-Gurion University, Israel
Andrej Bogdanov	The Chinese University of Hong Kong, SAR China
Zvika Brakerski	Weizmann Institute of Science, Israel
Nishanth Chandran	Microsoft Research, India
Stefan Dziembowski (Co-chair)	University of Warsaw, Poland
Sebastian Faust	TU Darmstadt, Germany
Marc Fischlin	TU Darmstadt, Germany
Iftach Haitner	Tel Aviv University, Israel
Martin Hirt	ETH Zurich, Switzerland
Pavel Hubáček	Charles University in Prague, Czech Republic
Aggelos Kiayias	University of Edinburgh, UK
Eyal Kushilevitz	Technion, Israel
Anna Lysyanskaya	Brown University, USA
Tal Malkin	Columbia University, USA
Eran Omri	Ariel University, Israel
Chris Peikert	University of Michigan – Ann Arbor, USA
Krzysztof Pietrzak	IST Austria, Austria
Antigoni Polychroniadou	Cornell University, USA
Alon Rosen	IDC Herzliya, Israel
Mike Rosulek	Oregon State University, USA
Vinod Vaikuntanathan	MIT, USA
Ivan Visconti	University of Salerno, Italy
Hoeteck Wee	CNRS and ENS, France

Mor Weiss	Northeastern University, USA
Stefan Wolf	University of Lugano, Switzerland
Vassilis Zikas	University of Edinburgh, UK

## TCC Steering Committee

Ivan Damgård	Aarhus University, Denmark
Shai Halevi (Chair)	IBM Research, USA
Huijia (Rachel) Lin	UCSB, USA
Tal Malkin	Columbia University, USA
Ueli Maurer	ETH, Switzerland
Moni Naor	Weizmann Institute of Science, Israel
Manoj Prabhakaran	Indian Institute of Technology, Bombay, India

## Additional Reviewers

Aydin Abadi	David Cash	Romain Gay
Shashank Agrawal	Anrin Chakraborti	Peter Gazi
Adi Akavia	Yilei Chen	Ran Gelles
Navid Alamati	Ilaria Chillotti	Badih Ghazi
Ghada Almashaqbeh	Wutichai Chongchitmate	Satrajit Ghosh
Bar Alon	Michele Ciampi	Irene Giacomelli
Joel Alwen	Ran Cohen	Junqing Gong
Prabhanjan Ananth	Xavier Coiteux-Roy	Dov Gordon
Megumi Ando	Sandro Coretti	Paul Grubbs
Benny Applebaum	Geoffroy Couteau	Cyprien de Saint Guilhem
Frederik Armknecht	Dana Dachman-Soled	Siyao Guo
Christian Badertscher	Pratish Datta	Divya Gupta
Saikrishna	Bernardo David	Arne Hansen
Badrinarayanan	Jean Paul Degabriele	Patrick Harasser
Karim Baghery	Akshay Degwekar	Prahladh Harsha
Marshall Ball	Apoorva Deshpande	Julia Hesse
Fabio Banfi	Nico Döttling	Minki Hhan
Laasya Bangalore	Lisa Eckey	Ryo Hiromasa
Carsten Baum	Naomi Ephraim	Justin Holmgren
Aner Ben-Efraim	Omar Fawzi	Kristina Hostakova
Fabrice Benhamouda	Serge Fehr	Yuval Ishai
Nir Bitansky	Matthias Fitzi	Muhammad Ishaq
Jonathan Bootle	Nils Fleischhacker	Zahra Jafargholi
Cecilia Boschini	Georg Fuchsbauer	Tibor Jager
Florian Bourse	Eiichiro Fujisaki	Aayush Jain
Elette Boyle	Steven Galbreith	Abhishek Jain
Anne Broadbent	Chaya Ganesh	Daniel Jost
Brent Carmer	Adria Gascon	Bruce Kapron



Tomasz Kazana	Daniele Micciancio	Adam Sealfon
Dakshita Khurana	Michele Minelli	Sruthi Sekar
Jiseung Kim	Konstantinos Mitropoulos	Yannick Seurin
Sam Kim	Tarik Moataz	Sina Shiehian
Fuyuki Kitagawa	Fabrice Mouhartem	Tom Shrimpton
Susumu Kiyoshima	Tamer Mour	Luisa Siniscalchi
Karen Klein	Pratyay Mukherjee	Veronika Slivova
Ilan Komargodski	Priyanka Mukhopadhyay	Pratik Soni
Orestis Konstantinidis	Marta Mularczyk	Nick Spooner
Venkata Koppula	Jörn Müller-Quade	Akshayaram Srinivasan
Lucas Kowalczyk	Kartik Nayak	Martjin Stam
Daniel Kraschewski	Tobias Nilges	John Steinberger
Mukul Kulkarni	Chinmay Nirkhe	Noah
Ashutosh Kumar	Ryo Nishimaki	Stephens-Davidowitz
Rajendra Kumar	Sai Lakshmi Bhavana	Qiang Tang
Benjamin Kuykendall	Obbattu	Stefano Tessaro
Rio LaVinge	Maciej Obremski	Ni Trieu
Changmin Lee	Miyako Ohkubo	Rotem Tsabary
Moon Sung Lee	Georgios Panagiotakos	Yiannis Tselekounis
Nikos Leonardos	Omer Paneth	Margarita Vald
Xiao Liang	Anat Paskin-Cherniavsky	Prashant Vasudevan
Jyun-Jie Liao	Valerio Pastro	Muthuramakrishnan
Chengyu Lin	Serdar Pehlivanoglu	Venkitasubramaniam
Huijia (Rachel) Lin	Renen Perlman	Daniele Venturi
Feng-Hao Liu	Giuseppe Persiano	Satyantarayana Vusirikala
Qipeng Liu	Thomas Peters	Hendrik Waldner
Tianren Liu	Christopher Portmann	Petros Wallden
Yi-Kai Liu	Srinivasan Raghuraman	Michael Walter
Chen-Da Liu Zhang	Govind Ramnarayan	Xiao Wang
Alex Lombardi	Samuel Ranellucci	Christopher Williamson
Julian Loss	Michael Raskin	David Wu
Steve Lu	Michael Riabzev	Keita Xagawa
Yun Lu	João Ribeiro	Yu Yu
Vadim Lyubashevsky	Silas Richelson	Shota Yamada
Urmila Mahadev	Felix Rohrbach	Takashi Yamakawa
Mohammad Mahmoody	Lior Rotem	Kevin Yeo
Subhamoy Maitra	Paul Rösler	Eylon Yogev
Nikolaos Makriyannis	Manuel Sabin	Thomas Zacharias
Takahiro Matsuda	Katerina Samari	Mark Zhandry
Christian Matt	Alessandra Scafuro	Jiamin Zhu
Jeremias Mechler	Giannicola Scarpa	Dionysis Zindros
Peihan Miao	Peter Scholl	Giorgos Zirdelis

# Contents – Part I

## Memory-Hard Functions and Complexity Theory

Provable Time-Memory Trade-Offs: Symmetric Cryptography Against Memory-Bounded Adversaries . . . . .	3
<i>Stefano Tessaro and Aishwarya Thiruvengadam</i>	
Static-Memory-Hard Functions, and Modeling the Cost of Space vs. Time . . .	33
<i>Thaddeus Dryja, Quanquan C. Liu, and Sunoo Park</i>	
No-signaling Linear PCPs . . . . .	67
<i>Susumu Kiyoshima</i>	
On Basing Search SIVP on NP-Hardness . . . . .	98
<i>Tianren Liu</i>	

## Two-Round MPC Protocols

Two-Round MPC: Information-Theoretic and Black-Box . . . . .	123
<i>Sanjam Garg, Yuval Ishai, and Akshayaram Srinivasan</i>	
Perfect Secure Computation in Two Rounds . . . . .	152
<i>Benny Applebaum, Zvika Brakerski, and Rotem Tsabary</i>	
Two-Round Adaptively Secure Multiparty Computation from Standard Assumptions . . . . .	175
<i>Fabrice Benhamouda, Huijia Lin, Antigoni Polychroniadou, and Muthuramakrishnan Venkatasubramanian</i>	

## Zero Knowledge

One-Message Zero Knowledge and Non-malleable Commitments . . . . .	209
<i>Nir Bitansky and Huijia Lin</i>	
Smooth NIZK Arguments . . . . .	235
<i>Charanjit S. Jutla and Arnab Roy</i>	
Round-Optimal Fully Black-Box Zero-Knowledge Arguments from One-Way Permutations . . . . .	263
<i>Carmit Hazay and Muthuramakrishnan Venkatasubramanian</i>	
Round Optimal Black-Box “Commit-and-Prove” . . . . .	286
<i>Dakshita Khurana, Rafail Ostrovsky, and Akshayaram Srinivasan</i>	

**Information-Theoretic Cryptography**

On the Power of Amortization in Secret Sharing:  $d$ -Uniform Secret Sharing  
and CDS with Constant Information Rate. . . . . 317  
*Benny Applebaum and Barak Arkis*

Information-Theoretic Secret-Key Agreement: The Asymptotically Tight  
Relation Between the Secret-Key Rate and the Channel Quality Ratio . . . . . 345  
*Daniel Jost, Ueli Maurer, and João L. Ribeiro*

Information-Theoretic Broadcast with Dishonest Majority  
for Long Messages . . . . . 370  
*Wutichai Chongchitmate and Rafail Ostrovsky*

Oblivious Transfer in Incomplete Networks . . . . . 389  
*Varun Narayanan and Vinod M. Prabahakaran*

**Trapdoor Permutations and Signatures**

Injective Trapdoor Functions via Derandomization: How Strong  
is Rudich’s Black-Box Barrier?. . . . . 421  
*Lior Rotem and Gil Segev*

Enhancements are Blackbox Non-trivial: Impossibility of Enhanced  
Trapdoor Permutations from Standard Trapdoor Permutations. . . . . 448  
*Mohammad Hajiabadi*

Certifying Trapdoor Permutations, Revisited. . . . . 476  
*Ran Canetti and Amit Lichtenberg*

On the Security Loss of Unique Signatures . . . . . 507  
*Andrew Morgan and Rafael Pass*

**Coin-Tossing and Fairness**

On the Complexity of Fair Coin Flipping. . . . . 539  
*Iftach Haitner, Nikolaos Makriyannis, and Eran Omri*

Game Theoretic Notions of Fairness in Multi-party Coin Toss . . . . . 563  
*Kai-Min Chung, Yue Guo, Wei-Kai Lin, Rafael Pass,  
and Elaine Shi*

Achieving Fair Treatment in Algorithmic Classification . . . . . 597  
*Andrew Morgan and Rafael Pass*

**Functional and Identity-Based Encryption**

Upgrading to Functional Encryption . . . . . 629  
*Saikrishna Badrinarayanan, Dakshita Khurana, Amit Sahai,  
and Brent Waters*

Impossibility of Simulation Secure Functional Encryption Even with  
Random Oracles . . . . . 659  
*Shashank Agrawal, Venkata Koppula, and Brent Waters*

Registration-Based Encryption: Removing Private-Key Generator  
from IBE . . . . . 689  
*Sanjam Garg, Mohammad Hajiabadi, Mohammad Mahmoody,  
and Ahmadreza Rahimi*

**Author Index** . . . . . 719

## Contents – Part II

### MPC Protocols

Topology-Hiding Computation Beyond Semi-Honest Adversaries . . . . .	3
<i>Rio LaVigne, Chen-Da Liu-Zhang, Ueli Maurer, Tal Moran, Marta Mularczyk, and Daniel Tschudi</i>	
Secure Computation Using Leaky Correlations (Asymptotically Optimal Constructions) . . . . .	36
<i>Alexander R. Block, Divya Gupta, Hemanta K. Maji, and Hai H. Nguyen</i>	
Fine-Grained Secure Computation . . . . .	66
<i>Matteo Campanelli and Rosario Gennaro</i>	
On the Structure of Unconditional UC Hybrid Protocols . . . . .	98
<i>Mike Rosulek and Morgan Shirley</i>	

### Order-Revealing Encryption and Symmetric Encryption

Impossibility of Order-Revealing Encryption in Idealized Models . . . . .	129
<i>Mark Zhandry and Cong Zhang</i>	
A Ciphertext-Size Lower Bound for Order-Preserving Encryption with Limited Leakage . . . . .	159
<i>David Cash and Cong Zhang</i>	
Ciphertext Expansion in Limited-Leakage Order-Preserving Encryption: A Tight Computational Lower Bound . . . . .	177
<i>Gil Segev and Ido Shahaf</i>	
Towards Tight Security of Cascaded LRW2 . . . . .	192
<i>Bart Mennink</i>	

### Information-Theoretic Cryptography II and Quantum Cryptography

Continuous NMC Secure Against Permutations and Overwrites, with Applications to CCA Secure Commitments . . . . .	225
<i>Ivan Damgård, Tomasz Kazana, Maciej Obremski, Varun Raj, and Luisa Siniscalchi</i>	
Best Possible Information-Theoretic MPC . . . . .	255
<i>Shai Halevi, Yuval Ishai, Eyal Kushilevitz, and Tal Rabin</i>	

Secure Certification of Mixed Quantum States with Application to Two-Party Randomness Generation . . . . .	282
<i>Frédéric Dupuis, Serge Fehr, Philippe Lamontagne, and Louis Salvail</i>	
Classical Proofs for the Quantum Collapsing Property of Classical Hash Functions . . . . .	315
<i>Serge Fehr</i>	
<b>LWE-Based Cryptography</b>	
Traitor-Tracing from LWE Made Simple and Attribute-Based. . . . .	341
<i>Yilei Chen, Vinod Vaikuntanathan, Brent Waters, Hoeteck Wee, and Daniel Wichs</i>	
Two-Message Statistically Sender-Private OT from LWE. . . . .	370
<i>Zvika Brakerski and Nico Döttling</i>	
Adaptively Secure Distributed PRFs from LWE . . . . .	391
<i>Benoît Libert, Damien Stehlé, and Radu Titu</i>	
<b>iO and Authentication</b>	
A Simple Construction of iO for Turing Machines . . . . .	425
<i>Sanjam Garg and Akshayaram Srinivasan</i>	
Succinct Garbling Schemes from Functional Encryption Through a Local Simulation Paradigm . . . . .	455
<i>Prabhanjan Ananth and Alex Lombardi</i>	
FE and iO for Turing Machines from Minimal Assumptions. . . . .	473
<i>Shweta Agrawal and Monosij Maitra</i>	
The MMap Strikes Back: Obfuscation and New Multilinear Maps Immune to CLT13 Zeroizing Attacks. . . . .	513
<i>Fermi Ma and Mark Zhandry</i>	
Return of GGH15: Provable Security Against Zeroizing Attacks . . . . .	544
<i>James Bartusek, Jiaxin Guan, Fermi Ma, and Mark Zhandry</i>	
The Security of Lazy Users in Out-of-Band Authentication . . . . .	575
<i>Moni Naor, Lior Rotem, and Gil Segev</i>	
<b>ORAM and PRF</b>	
Is There an Oblivious RAM Lower Bound for Online Reads? . . . . .	603
<i>Mor Weiss and Daniel Wichs</i>	

<p>Perfectly Secure Oblivious Parallel RAM. . . . .</p> <p style="padding-left: 2em;"><i>T.-H. Hubert Chan, Kartik Nayak, and Elaine Shi</i></p>	<p>636</p>
<p>Watermarking PRFs Under Standard Assumptions: Public Marking and Security with Extraction Queries. . . . .</p> <p style="padding-left: 2em;"><i>Willy Quach, Daniel Wichs, and Giorgos Zirdelis</i></p>	<p>669</p>
<p>Exploring Crypto Dark Matter: New Simple PRF Candidates and Their Applications. . . . .</p> <p style="padding-left: 2em;"><i>Dan Boneh, Yuval Ishai, Alain Passelègue, Amit Sahai, and David J. Wu</i></p>	<p>699</p>
<p><b>Author Index</b> . . . . .</p>	<p>731</p>