

*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, 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>

Martin Hirt · Adam Smith (Eds.)

# Theory of Cryptography

14th International Conference, TCC 2016-B  
Beijing, China, October 31 – November 3, 2016  
Proceedings, Part II

*Editors*

Martin Hirt  
Department of Computer Science  
ETH Zurich  
Zurich  
Switzerland

Adam Smith  
Pennsylvania State University  
University Park, PA  
USA

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-662-53643-8              ISBN 978-3-662-53644-5 (eBook)  
DOI 10.1007/978-3-662-53644-5

Library of Congress Control Number: 2016954934

LNCS Sublibrary: SL4 – Security and Cryptology

© International Association for Cryptologic Research 2016

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.

Printed on acid-free paper

This Springer imprint is published by Springer Nature  
The registered company is Springer-Verlag GmbH Germany  
The registered company address is: Heidelberger Platz 3, 14197 Berlin, Germany

# Preface

The 14th Theory of Cryptography Conference (TCC 2016-B) was held October 31 to November 3, 2016, at the Beijing Friendship Hotel in Beijing, China. It was sponsored by the International Association for Cryptographic Research (IACR) and organized in cooperation with State Key Laboratory of Information Security at the Institute of Information Engineering of the Chinese Academy of Sciences. The general chair was Dongdai Lin, and the honorary chair was Andrew Chi-Chih Yao.

The conference received 113 submissions, of which the Program Committee (PC) selected 45 for presentation (with three pairs of papers sharing a single presentation slot per pair). Of these, there were four whose authors were all students at the time of submission. The committee selected “Simulating Auxiliary Inputs, Revisited” by Maciej Skórski for the Best Student Paper award. Each submission was reviewed by at least three PC members, often more. The 25 PC members, all top researchers in our field, were helped by 154 external reviewers, who were consulted when appropriate. These proceedings consist of the revised version of the 45 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 the last two years, we used the interaction feature supported by the review software, where PC members may directly and anonymously interact with authors. The feature allowed the PC to ask specific technical questions that arose during the review process, for example, about suspected bugs. Authors were prompt and extremely helpful in their replies. We hope that it will continue to be used in the future.

This was the third year where 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. The Test of Time Award Committee consisted of Tal Rabin (chair), Yuval Ishai, Daniele Micciancio, and Jesper Nielsen. They selected “Indifferentiability, Impossibility Results on Reductions, and Applications to the Random Oracle Methodology” by Ueli Maurer, Renato Renner, and Clemens Holenstein—which appeared in TCC 2004, the first edition of the conference—for introducing indifferentiability, a security notion that had “significant impact on both the theory of cryptography and the design of practical cryptosystems.” Sadly, Clemens Holenstein passed away in 2012. He is survived by his wife and two sons. Maurer and Renner accepted the award on his behalf. The authors delivered a talk in a special session at TCC 2016-B. An invited paper by them, which was not reviewed, is included in these proceedings.

The conference featured two other invited talks, by Allison Bishop and Srini Devadas. In addition to regular papers and invited events, there was a rump session featuring short talks by attendees.

We are greatly indebted to many people who were involved in making TCC 2016-B a success. First of all, our sincere thanks to the most important contributors: all the authors who submitted papers to the conference. There were many more good submissions than we had space to accept. We would like to thank the PC members for their hard work, dedication, and diligence in reviewing the papers, verifying their correctness, and discussing their merits in depth. We are also thankful to the external reviewers for their volunteered hard work in reviewing papers and providing valuable expert feedback in response to specific queries. For running the conference itself, we are very grateful to Dongdai and the rest of the local Organizing Committee. Finally, we are grateful to the TCC Steering Committee, and especially Shai Halevi, for guidance and advice, as well as to the entire thriving and vibrant theoretical cryptography community. TCC exists for and because of that community, and we are proud to be a part of it.

November 2016

Martin Hirt  
Adam Smith

# TCC 2016-B

## Theory of Cryptography Conference

Beijing, China

October 31 – November 3, 2016

Sponsored by the International Association for Cryptologic Research and organized in cooperation with the State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences.

### General Chair

Dongdai Lin                      Chinese Academy of Sciences, China

### Honorary Chair

Andrew Chi-Chih Yao          Tsinghua University, China

### Program Committee

Masayuki Abe	NTT, Japan
Divesh Aggarwal	NUS, Singapore
Andrej Bogdanov	Chinese University of Hong Kong, Hong Kong
Elette Boyle	IDC Herzliya, Israel
Anne Broadbent	University of Ottawa, Canada
Chris Brzuska	TU Hamburg, Germany
David Cash	Rutgers University, USA
Alessandro Chiesa	University of California, Berkeley, USA
Kai-Min Chung	Academia Sinica, Taiwan
Nico Döttling	University of California, Berkeley, USA
Sergey Gorbunov	University of Waterloo, Canada
Martin Hirt (Co-chair)	ETH Zurich, Switzerland
Abhishek Jain	Johns Hopkins University, USA
Huijia Lin	University of California, Santa Barbara, USA
Hemanta K. Maji	Purdue University, USA
Adam O'Neill	Georgetown University, USA
Rafael Pass	Cornell University, USA
Krzysztof Pietrzak	IST Austria, Austria
Manoj Prabhakaran	IIT Bombay, India
Renato Renner	ETH Zurich, Switzerland
Alon Rosen	IDC Herzliya, Israel
abhi shelat	Northeastern University, USA
Adam Smith (Co-chair)	Pennsylvania State University, USA

John Steinberger	Tsinghua University, China
Jonathan Ullman	Northeastern University, USA
Vinod Vaikuntanathan	MIT, USA
Muthuramakrishnan Venkitasubramaniam	University of Rochester, USA

## TCC Steering Committee

Mihir Bellare	UCSD, USA
Ivan Damgård	Aarhus University, Denmark
Shafi Goldwasser	MIT, USA
Shai Halevi (Chair)	IBM Research, USA
Russell Impagliazzo	UCSD, USA
Ueli Maurer	ETH, Switzerland
Silvio Micali	MIT, USA
Moni Naor	Weizmann Institute, Israel
Tatsuaki Okamoto	NTT, Japan

## External Reviewers

Hamza Abusalah	Michele Ciampi	Carmit Hazay
Shashank Agrawal	Aloni Cohen	Brett Hemenway
Shweta Agrawal	Ran Cohen	Felix Heuer
Joël Alwen	Angelo DeCaro	Ryo Hiromasa
Prabhanjan Ananth	Jean Paul Degabriele	Dennis Hofheinz
Saikrishna Badrinarayanan	Akshay Degwekar	Justin Holmgren
Marshall Ball	Itai Dinur	Pavel Hubáček
Raef Bassily	Léo Ducas	Tsung-Hsuan Hung
Carsten Baum	Tuyet Duong	Vincenzo Iovino
Amos Beimel	Andreas Enge	Aayush Jain
Fabrice Benhamouda	Antonio Faonio	Chethan Kamath
Itay Berman	Oriol Farras	Tomasz Kazana
Nir Bitansky	Pooya Farshim	Raza Ali Kazmi
Alexander R. Block	Sebastian Faust	Carmen Kempka
Tobias Boelter	Omar Fawzi	Florian Kerschbaum
Zvika Brakerski	Max Fillinger	Dakshita Khurana
Brandon Broadnax	Nils Fleischhacker	Fuyuki Kitagawa
Ran Canetti	Eiichiro Fujisaki	Susumu Kiyoshima
Andrea Caranti	Peter Gaži	Saleet Klein
Nishanth Chandran	Satrajit Ghosh	Ilan Komargodski
Yi-Hsiu Chen	Alexander Golovnev	Venkata Koppula
Yilei Chen	Siyao Guo	Stephan Krenn
Yu-Chi Chen	Divya Gupta	Mukul Ramesh Kulkarni
Seung Geol Choi	Venkatesan Guruswami	Tancrede Lepoint
	Yongling Hao	Kevin Lewi



Wei-Kai Lin	Christopher Peikert	Aishwarya
Helger Lipmaa	Oxana Poburinnaya	Thiruvengadam
Feng-Hao Liu	Bertram Poettering	Junnichi Tomida
Vadim Lyubashevsky	Antigoni Polychroniadou	Rotem Tsabary
Mohammad Mahmoody	Christopher Portmann	Margarita Vald
Giulio Malavolta	Srini Raghuraman	Prashant Vasudevan
Alex J. Malozemoff	Samuel Ranellucci	Daniele Venturi
Daniel Masny	Vanishree Rao	Damien Vergnaud
Takahiro Matsuda	Mariana Raykova	Jorge L. Villar
Christian Matt	Joseph Renes	Dhinakaran
Patrick McCorry	Leonid Reyzin	Vinayagamurthy
Or Meir	Silas Richelson	Madars Virza
Peihan Miao	Mike Rosulek	Ivan Visconti
Eric Miles	Guy Rothblum	Hoeteck Wee
Pratyush Mishra	Ron Rothblum	Eyal Widder
Ameer Mohammed	Sajin Sasy	David Wu
Payman Mohassel	Alessandra Scafuro	Keita Xagawa
Tal Moran	Dominique Schröder	Sophia Yakoubov
Kirill Morozov	Karn Seth	Takashi Yamakawa
Pratyay Mukherjee	Vladimir Shpilrain	Avishay Yanay
Hai H. Nguyen	Mark Simkin	Arkady Yerukhimovich
Ryo Nishimaki	Nigel Smart	Eylon Yogev
Maciej Obremski	Pratik Soni	Mohammad Zaheri
Miyako Ohkubo	Bing Sun	Mark Zhandry
Jiaxin Pan	David Sutter	Hong-Sheng Zhou
Omkant Pandey	Björn Tackmann	Juba Ziani
Omer Paneth	Stefano Tessaro	
Valerio Pastro	Justin Thaler	

## Contents – Part II

### Delegation and IP

Delegating RAM Computations with Adaptive Soundness and Privacy . . . . .	3
<i>Prabhanjan Ananth, Yu-Chi Chen, Kai-Min Chung, Huijia Lin, and Wei-Kai Lin</i>	
Interactive Oracle Proofs . . . . .	31
<i>Eli Ben-Sasson, Alessandro Chiesa, and Nicholas Spooner</i>	
Adaptive Succinct Garbled RAM or: How to Delegate Your Database. . . . .	61
<i>Ran Canetti, Yilei Chen, Justin Holmgren, and Mariana Raykova</i>	
Delegating RAM Computations . . . . .	91
<i>Yael Kalai and Omer Paneth</i>	

### Public-Key Encryption

Standard Security Does Not Imply Indistinguishability Under Selective Opening. . . . .	121
<i>Dennis Hofheinz, Vanishree Rao, and Daniel Wichs</i>	
Public-Key Encryption with Simulation-Based Selective-Opening Security and Compact Ciphertexts . . . . .	146
<i>Dennis Hofheinz, Tibor Jager, and Andy Rupp</i>	
Towards Non-Black-Box Separations of Public Key Encryption and One Way Function. . . . .	169
<i>Dana Dachman-Soled</i>	
Post-Quantum Security of the Fujisaki-Okamoto and OAEP Transforms . . . .	192
<i>Ehsan Ebrahimi Targhi and Dominique Unruh</i>	
Multi-key FHE from LWE, Revisited . . . . .	217
<i>Chris Peikert and Sina Shiehian</i>	

### Obfuscation and Multilinear Maps

Secure Obfuscation in a Weak Multilinear Map Model . . . . .	241
<i>Sanjam Garg, Eric Miles, Pratyay Mukherjee, Amit Sahai, Akshayaram Srinivasan, and Mark Zhandry</i>	

Virtual Grey-Boxes Beyond Obfuscation: A Statistical Security Notion  
for Cryptographic Agents . . . . . 269  
*Shashank Agrawal, Manoj Prabhakaran, and Ching-Hua Yu*

**Attribute-Based Encryption**

Deniable Attribute Based Encryption for Branching Programs from LWE . . . 299  
*Daniel Apon, Xiong Fan, and Feng-Hao Liu*

Targeted Homomorphic Attribute-Based Encryption . . . . . 330  
*Zvika Brakerski, David Cash, Rotem Tsabary, and Hoeteck Wee*

Semi-adaptive Security and Bundling Functionalities Made Generic  
and Easy . . . . . 361  
*Rishab Goyal, Venkata Koppula, and Brent Waters*

**Functional Encryption**

From Cryptomania to Obfustopia Through Secret-Key Functional  
Encryption . . . . . 391  
*Nir Bitansky, Ryo Nishimaki, Alain Passelègue, and Daniel Wichs*

Single-Key to Multi-Key Functional Encryption with Polynomial Loss . . . . . 419  
*Sanjam Garg and Akshayaram Srinivasan*

Compactness vs Collusion Resistance in Functional Encryption . . . . . 443  
*Baiyu Li and Daniele Micciancio*

**Secret Sharing**

Threshold Secret Sharing Requires a Linear Size Alphabet . . . . . 471  
*Andrej Bogdanov, Siyao Guo, and Ilan Komargodski*

How to Share a Secret, Infinitely . . . . . 485  
*Ilan Komargodski, Moni Naor, and Eylon Yogev*

**New Models**

Designing Proof of Human-Work Puzzles for Cryptocurrency and Beyond . . . 517  
*Jeremiah Blocki and Hong-Sheng Zhou*

Access Control Encryption: Enforcing Information Flow  
with Cryptography . . . . . 547  
*Ivan Damgård, Helene Haagh, and Claudio Orlandi*

**Author Index** . . . . . 577

# Contents – Part I

## TCC Test-of-Time Award

From Indifferentiability to Constructive Cryptography (and Back) . . . . .	3
<i>Ueli Maurer and Renato Renner</i>	

## Foundations

Fast Pseudorandom Functions Based on Expander Graphs . . . . .	27
<i>Benny Applebaum and Pavel Raykov</i>	
3-Message Zero Knowledge Against Human Ignorance . . . . .	57
<i>Nir Bitansky, Zvika Brakerski, Yael Kalai, Omer Paneth, and Vinod Vaikuntanathan</i>	
The GGM Function Family Is a Weakly One-Way Family of Functions . . . .	84
<i>Aloni Cohen and Saleet Klein</i>	
On the (In)Security of SNARKs in the Presence of Oracles . . . . .	108
<i>Dario Fiore and Anca Nitulescu</i>	
Leakage Resilient One-Way Functions: The Auxiliary-Input Setting . . . . .	139
<i>Ilan Komargodski</i>	
Simulating Auxiliary Inputs, Revisited . . . . .	159
<i>Maciej Skórski</i>	

## Unconditional Security

Pseudoentropy: Lower-Bounds for Chain Rules and Transformations. . . . .	183
<i>Krzysztof Pietrzak and Maciej Skórski</i>	
Oblivious Transfer from Any Non-trivial Elastic Noisy Channel via Secret Key Agreement. . . . .	204
<i>Ignacio Cascudo, Ivan Damgård, Felipe Lacerda, and Samuel Ranellucci</i>	
Simultaneous Secrecy and Reliability Amplification for a General Channel Model . . . . .	235
<i>Russell Impagliazzo, Ragesh Jaiswal, Valentine Kabanets, Bruce M. Kapron, Valerie King, and Stefano Tessaro</i>	

Proof of Space from Stacked Expanders. . . . . 262  
*Ling Ren and Srinivas Devadas*

Perfectly Secure Message Transmission in Two Rounds. . . . . 286  
*Gabriele Spini and Gilles Zémor*

**Foundations of Multi-Party Protocols**

Almost-Optimally Fair Multiparty Coin-Tossing with Nearly  
 Three-Quarters Malicious. . . . . 307  
*Bar Alon and Eran Omri*

Binary AMD Circuits from Secure Multiparty Computation . . . . . 336  
*Daniel Genkin, Yuval Ishai, and Mor Weiss*

Composable Security in the Tamper-Proof Hardware Model Under Minimal  
 Complexity . . . . . 367  
*Carmit Hazay, Antigoni Polychroniadou,  
 and Muthuramakrishnan Venkatasubramaniam*

Composable Adaptive Secure Protocols Without Setup Under Polytime  
 Assumptions. . . . . 400  
*Carmit Hazay and Muthuramakrishnan Venkatasubramaniam*

Adaptive Security of Yao’s Garbled Circuits . . . . . 433  
*Zahra Jafargholi and Daniel Wichs*

**Round Complexity and Efficiency of Multi-party Computation**

Efficient Secure Multiparty Computation with Identifiable Abort. . . . . 461  
*Carsten Baum, Emmanuela Orsini, and Peter Scholl*

Secure Multiparty RAM Computation in Constant Rounds . . . . . 491  
*Sanjam Garg, Divya Gupta, Peihan Miao, and Omkant Pandey*

Constant-Round Maliciously Secure Two-Party Computation in the RAM  
 Model . . . . . 521  
*Carmit Hazay and Avishay Yanai*

More Efficient Constant-Round Multi-party Computation from BMR  
 and SHE . . . . . 554  
*Yehuda Lindell, Nigel P. Smart, and Eduardo Soria-Vazquez*

Cross and Clean: Amortized Garbled Circuits with Constant Overhead . . . . . 582  
*Jesper Buus Nielsen and Claudio Orlandi*

**Differential Privacy**

Separating Computational and Statistical Differential Privacy  
in the Client-Server Model . . . . . 607  
*Mark Bun, Yi-Hsiu Chen, and Salil Vadhan*

Concentrated Differential Privacy: Simplifications, Extensions,  
and Lower Bounds . . . . . 635  
*Mark Bun and Thomas Steinke*

Strong Hardness of Privacy from Weak Traitor Tracing . . . . . 659  
*Lucas Kowalczyk, Tal Malkin, Jonathan Ullman, and Mark Zhandry*

**Author Index** . . . . . 691