More information about this series at http://www.springer.com/series/7410
Theory of Cryptography

14th International Conference, TCC 2016-B
Beijing, China, October 31 – November 3, 2016
Proceedings, Part II
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
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
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  
Akshay Degwekar  
Justin Holmgren
Badrinarayanan  
Itai Dinur  
Pavel Hubáček
Marshall Ball  
Léo Ducas  
Tsung-Hsuan Hung
Raef Bassily  
Tuyet Duong  
Vincenzo Iovino
Carsten Baum  
Andreas Enge  
Aayush Jain
Amos Beimel  
Antonio Faonio  
Chethan Kamath
Fabrice Benhamouda  
Oriol Farras  
Tomasz Kazana
Itay Berman  
Pooya Farshim  
Raza Ali Kazmi
Nir Bitansky  
Sebastian Faust  
Carmen Kempka
Alexander R. Block  
Omar Fawzi  
Florian Kerschbaum
Tobias Boelter  
Max Fillinger  
Dakshita Khurana
Zvika Brakerski  
Nils Fleischhacker  
Fuyuki Kitagawa
Brandon Broadnax  
Eiichiro Fujisaki  
Susumu Kiyoshima
Ran Canetti  
Peter Gaži  
Saleet Klein
Andrea Caranti  
Satrajit Ghosh  
Ilan Komargodski
Nishanth Chandran  
Alexander Golovnev  
Venkata Koppula
Yi-Hsiu Chen  
Siyao Guo  
Stephan Krenn
Yilei Chen  
Divya Gupta  
Mukul Ramesh Kulkarni
Yu-Chi Chen  
Venkatesan Guruswami  
Tancrède Lepoint
Seung Geol Choi  
Yongling Hao  
Kevin Lewi
<table>
<thead>
<tr>
<th>Wei-Kai Lin</th>
<th>Christopher Peikert</th>
<th>Aishwarya</th>
</tr>
</thead>
<tbody>
<tr>
<td>Helger Lipmaa</td>
<td>Oxana Poburinnaya</td>
<td>Thiruvengadam</td>
</tr>
<tr>
<td>Feng-Hao Liu</td>
<td>Bertram Poettering</td>
<td>Junnich Tomida</td>
</tr>
<tr>
<td>Vadim Lyubashevsky</td>
<td>Antigoni Polychroniadou</td>
<td>Rotem Tsabary</td>
</tr>
<tr>
<td>Mohammad Mahmoody</td>
<td>Christopher Portmann</td>
<td>Margarita Vald</td>
</tr>
<tr>
<td>Giulio Malavolta</td>
<td>Srini Raghuraman</td>
<td>Prashant Vasudevan</td>
</tr>
<tr>
<td>Alex J. Malozemoff</td>
<td>Samuel Ranellucci</td>
<td>Daniele Venturi</td>
</tr>
<tr>
<td>Daniel Masny</td>
<td>Vanishree Rao</td>
<td>Damien Vergnaud</td>
</tr>
<tr>
<td>Takahiro Matsuda</td>
<td>Mariana Raykova</td>
<td>Jorge L. Villar</td>
</tr>
<tr>
<td>Christian Matt</td>
<td>Joseph Renes</td>
<td>Dhinakaran</td>
</tr>
<tr>
<td>Patrick McCorry</td>
<td>Leonid Reyzin</td>
<td>Vinayagamurthy</td>
</tr>
<tr>
<td>Or Meir</td>
<td>Silas Richelson</td>
<td></td>
</tr>
<tr>
<td>Peihan Miao</td>
<td>Mike Rosulek</td>
<td>Ivan Visconti</td>
</tr>
<tr>
<td>Eric Miles</td>
<td>Guy Rothblum</td>
<td>Hoeteck Wee</td>
</tr>
<tr>
<td>Pratyush Mishra</td>
<td>Ron Rothblum</td>
<td>Eyal Widder</td>
</tr>
<tr>
<td>Ameer Mohammed</td>
<td>Sajin Sasy</td>
<td>David Wu</td>
</tr>
<tr>
<td>Payman Mohassel</td>
<td>Alessandra Scafuro</td>
<td>Keita Xagawa</td>
</tr>
<tr>
<td>Tal Moran</td>
<td>Dominique Schröder</td>
<td>Sophia Yakoubov</td>
</tr>
<tr>
<td>Kirill Morozov</td>
<td>Karn Seth</td>
<td>Takashi Yamakawa</td>
</tr>
<tr>
<td>Pratyay Mukherjee</td>
<td>Vladimir Shpilrain</td>
<td>Avishay Yanay</td>
</tr>
<tr>
<td>Hai H. Nguyen</td>
<td>Mark Simkin</td>
<td>Arkady Yerukhimovich</td>
</tr>
<tr>
<td>Ryo Nishimaki</td>
<td>Nigel Smart</td>
<td>Eylon Yogev</td>
</tr>
<tr>
<td>Maciej Obremski</td>
<td>Pratik Soni</td>
<td>Mohammad Zaheri</td>
</tr>
<tr>
<td>Miyako Ohkubo</td>
<td>Bing Sun</td>
<td>Mark Zhandry</td>
</tr>
<tr>
<td>Jiaxin Pan</td>
<td>David Sutter</td>
<td>Hong-Sheng Zhou</td>
</tr>
<tr>
<td>Omkant Pandey</td>
<td>Björn Tackmann</td>
<td></td>
</tr>
<tr>
<td>Omer Paneth</td>
<td>Stefano Tessaro</td>
<td>Juba Ziani</td>
</tr>
<tr>
<td>Valerio Pastro</td>
<td>Justin Thaler</td>
<td></td>
</tr>
</tbody>
</table>
## Contents – Part II

### Delegation and IP

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

### Public-Key Encryption

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

### Obfuscation and Multilinear Maps

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Obfuscation in a Weak Multilinear Map Model</td>
<td>241</td>
</tr>
<tr>
<td><em>Sanjam Garg,</em> <em>Eric Miles,</em> <em>Pratyay Mukherjee,</em> <em>Amit Sahai,</em> <em>Akshayaram Srinivasan,</em> and <em>Mark Zhandry</em></td>
<td></td>
</tr>
</tbody>
</table>
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  
*Ueli Maurer and Renato Renner*

**Foundations**

Fast Pseudorandom Functions Based on Expander Graphs ....................... 27  
*Benny Applebaum and Pavel Raykov*

3-Message Zero Knowledge Against Human Ignorance ................................. 57  
*Nir Bitansky, Zvika Brakerski, Yael Kalai, Omer Paneth,  and Vinod Vaikuntanathan*

The GGM Function Family Is a Weakly One-Way Family of Functions ........ 84  
*Aloni Cohen and Saleet Klein*

On the (In)Security of SNARKs in the Presence of Oracles .................... 108  
*Dario Fiore and Anca Nitulescu*

Leakage Resilient One-Way Functions: The Auxiliary-Input Setting .......... 139  
*Ilan Komargodski*

Simulating Auxiliary Inputs, Revisited ........................................... 159  
*Maciej Skórski*

**Unconditional Security**

Pseudoentropy: Lower-Bounds for Chain Rules and Transformations .......... 183  
*Krzysztof Pietrzak and Maciej Skórski*

Oblivious Transfer from Any Non-trivial Elastic Noisy Channel via Secret Key Agreement ................................................................. 204  
*Ignacio Cascudo, Ivan Damgård, Felipe Lacerda,  and Samuel Ranellucci*

Simultaneous Secrecy and Reliability Amplification for a General Channel Model ................................................................. 235  
*Russell Impagliazzo, Ragesh Jaiswal, Valentine Kabanets,  Bruce M. Kapron, Valerie King,  and Stefano Tessaro*
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 Venkitasubramaniam

Composable Adaptive Secure Protocols Without Setup Under Polytime Assumptions 400
   Carmit Hazay and Muthuramakrishnan Venkitasubramaniam

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