

Contents – Part III

Quantum Techniques

Quantum Homomorphic Encryption for Polynomial-Sized Circuits	3
<i>Yfke Dulek, Christian Schaffner, and Florian Speelman</i>	
Adaptive Versus Non-Adaptive Strategies in the Quantum Setting with Applications	33
<i>Frédéric Dupuis, Serge Fehr, Philippe Lamontagne, and Louis Salvail</i>	
Semantic Security and Indistinguishability in the Quantum World	60
<i>Tommaso Gagliardini, Andreas Hülsing, and Christian Schaffner</i>	

Spooky Encryption

Spooky Encryption and Its Applications.	93
<i>Yevgeniy Dodis, Shai Halevi, Ron D. Rothblum, and Daniel Wichs</i>	
Spooky Interaction and Its Discontents: Compilers for Succinct Two-Message Argument Systems	123
<i>Cynthia Dwork, Moni Naor, and Guy N. Rothblum</i>	

Secure Computation and Protocols II

Adaptively Secure Garbled Circuits from One-Way Functions	149
<i>Brett Hemenway, Zahra Jafargholi, Rafail Ostrovsky, Alessandra Scafuro, and Daniel Wichs</i>	
Rate-1, Linear Time and Additively Homomorphic UC Commitments	179
<i>Ignacio Cascudo, Ivan Damgård, Bernardo David, Nico Döttling, and Jesper Buus Nielsen</i>	
UC Commitments for Modular Protocol Design and Applications to Revocation and Attribute Tokens.	208
<i>Jan Camenisch, Maria Dubovitskaya, and Alfredo Rial</i>	
Probabilistic Termination and Composability of Cryptographic Protocols	240
<i>Ran Cohen, Sandro Coretti, Juan Garay, and Vassilis Zikas</i>	
Concurrent Non-Malleable Commitments (and More) in 3 Rounds	270
<i>Michele Ciampi, Rafail Ostrovsky, Luisa Siniscalchi, and Ivan Visconti</i>	

IBE, ABE, and Functional Encryption

Programmable Hash Functions from Lattices: Short Signatures and IBEs with Small Key Sizes	303
<i>Jiang Zhang, Yu Chen, and Zhenfeng Zhang</i>	
Fully Secure Functional Encryption for Inner Products, from Standard Assumptions.	333
<i>Shweta Agrawal, Benoît Libert, and Damien Stehlé</i>	
Circuit-ABE from LWE: Unbounded Attributes and Semi-adaptive Security . . .	363
<i>Zvika Brakerski and Vinod Vaikuntanathan</i>	

Automated Tools and Synthesis

Design in Type-I, Run in Type-III: Fast and Scalable Bilinear-Type Conversion Using Integer Programming.	387
<i>Masayuki Abe, Fumitaka Hoshino, and Miyako Ohkubo</i>	
Linicrypt: A Model for Practical Cryptography	416
<i>Brent Carmer and Mike Rosulek</i>	

Zero Knowledge

On the Relationship Between Statistical Zero-Knowledge and Statistical Randomized Encodings	449
<i>Benny Applebaum and Pavel Raykov</i>	
How to Prove Knowledge of Small Secrets	478
<i>Carsten Baum, Ivan Damgård, Kasper Green Larsen, and Michael Nielsen</i>	
Efficient Zero-Knowledge Proof of Algebraic and Non-Algebraic Statements with Applications to Privacy Preserving Credentials	499
<i>Melissa Chase, Chaya Ganesh, and Payman Mohassel</i>	

Theory

Fine-Grained Cryptography	533
<i>Akshay Degwekar, Vinod Vaikuntanathan, and Prashant Nalini Vasudevan</i>	
TWORAM: Efficient Oblivious RAM in Two Rounds with Applications to Searchable Encryption	563
<i>Sanjam Garg, Payman Mohassel, and Charalampos Papamanthou</i>	

Bounded Indistinguishability and the Complexity of Recovering Secrets	593
<i>Andrej Bogdanov, Yuval Ishai, Emanuele Viola, and Christopher Williamson</i>	
Two-Message, Oblivious Evaluation of Cryptographic Functionalities	619
<i>Nico Döttling, Nils Fleischhacker, Johannes Krupp, and Dominique Schröder</i>	
Author Index	649

<http://www.springer.com/978-3-662-53014-6>

Advances in Cryptology – CRYPTO 2016
36th Annual International Cryptology Conference, Santa
Barbara, CA, USA, August 14–18, 2016, Proceedings,
Part III
Robshaw, M.; Katz, J. (Eds.)
2016, XIII, 651 p. 77 illus., Softcover
ISBN: 978-3-662-53014-6