

# Contents – Part I

## Functional Encryption

Stronger Security for Reusable Garbled Circuits, General Definitions and Attacks . . . . .	3
<i>Shweta Agrawal</i>	
Generic Transformations of Predicate Encodings: Constructions and Applications . . . . .	36
<i>Miguel Ambrona, Gilles Barthe, and Benedikt Schmidt</i>	
Practical Functional Encryption for Quadratic Functions with Applications to Predicate Encryption . . . . .	67
<i>Carmen Elisabetta Zaira Baltico, Dario Catalano, Dario Fiore, and Romain Gay</i>	

## Foundations I

Memory-Tight Reductions . . . . .	101
<i>Benedikt Auerbach, David Cash, Manuel Fersch, and Eike Kiltz</i>	
Be Adaptive, Avoid Overcommitting . . . . .	133
<i>Zahra Jafargholi, Chethan Kamath, Karen Klein, Ilan Komargodski, Krzysztof Pietrzak, and Daniel Wichs</i>	

## Two-Party Computation

The TinyTable Protocol for 2-Party Secure Computation, or: Gate-Scrambling Revisited . . . . .	167
<i>Ivan Damgård, Jesper Buus Nielsen, Michael Nielsen, and Samuel Ranellucci</i>	
Privacy-Free Garbled Circuits for Formulas: Size Zero and Information-Theoretic . . . . .	188
<i>Yashvanth Kondi and Arpita Patra</i>	
Secure Arithmetic Computation with Constant Computational Overhead . . . .	223
<i>Benny Applebaum, Ivan Damgård, Yuval Ishai, Michael Nielsen, and Lior Zichron</i>	
Encryption Switching Protocols Revisited: Switching Modulo $p$ . . . . .	255
<i>Guilhem Castagnos, Laurent Imbert, and Fabien Laguillaumie</i>	

## Bitcoin

The Bitcoin Backbone Protocol with Chains of Variable Difficulty . . . . .	291
<i>Juan Garay, Aggelos Kiayias, and Nikos Leonardos</i>	
Bitcoin as a Transaction Ledger: A Composable Treatment . . . . .	324
<i>Christian Badertscher, Ueli Maurer, Daniel Tschudi, and Vassilis Zikas</i>	
Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol . . . . .	357
<i>Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov</i>	

## Multiparty Computation

Robust Non-interactive Multiparty Computation Against Constant-Size Collusion . . . . .	391
<i>Fabrice Benhamouda, Hugo Krawczyk, and Tal Rabin</i>	
The Price of Low Communication in Secure Multi-party Computation . . . . .	420
<i>Juan Garay, Yuval Ishai, Rafail Ostrovsky, and Vassilis Zikas</i>	
Topology-Hiding Computation on All Graphs . . . . .	447
<i>Adi Akavia, Rio LaVigne, and Tal Moran</i>	
A New Approach to Round-Optimal Secure Multiparty Computation . . . . .	468
<i>Prabhanjan Ananth, Arka Rai Choudhuri, and Abhishek Jain</i>	

## Award Papers

Watermarking Cryptographic Functionalities from Standard Lattice Assumptions . . . . .	503
<i>Sam Kim and David J. Wu</i>	
Identity-Based Encryption from the Diffie-Hellman Assumption . . . . .	537
<i>Nico Döttling and Sanjam Garg</i>	
The First Collision for Full SHA-1 . . . . .	570
<i>Marc Stevens, Elie Bursztein, Pierre Karpman, Ange Albertini, and Yarik Markov</i>	

## Obfuscation I

Indistinguishability Obfuscation from SXDH on 5-Linear Maps and Locality-5 PRGs . . . . .	599
<i>Huijia Lin</i>	

Indistinguishability Obfuscation from Trilinear Maps and Block-Wise Local PRGs . . . . .	630
<i>Huijia Lin and Stefano Tessaro</i>	
Lower Bounds on Obfuscation from All-or-Nothing Encryption Primitives. . .	661
<i>Sanjam Garg, Mohammad Mahmoody, and Ameer Mohammed</i>	
Structure vs. Hardness Through the Obfuscation Lens . . . . .	696
<i>Nir Bitansky, Akshay Degwekar, and Vinod Vaikuntanathan</i>	
<b>Conditional Disclosure of Secrets</b>	
Conditional Disclosure of Secrets: Amplification, Closure, Amortization, Lower-Bounds, and Separations . . . . .	727
<i>Benny Applebaum, Barak Arkis, Pavel Raykov, and Prashant Nalini Vasudevan</i>	
Conditional Disclosure of Secrets via Non-linear Reconstruction . . . . .	758
<i>Tianren Liu, Vinod Vaikuntanathan, and Hoeteck Wee</i>	
<b>Author Index</b> . . . . .	791

Advances in Cryptology - CRYPTO 2017  
37th Annual International Cryptology Conference, Santa  
Barbara, CA, USA, August 20-24, 2017, Proceedings,  
Part I  
Katz, J.; Shacham, H. (Eds.)  
2017, XV, 793 p. 120 illus., Softcover  
ISBN: 978-3-319-63687-0