

Table of Contents

Secure Computation

Computing on Authenticated Data	1
<i>Jae Hyun Ahn, Dan Boneh, Jan Camenisch, Susan Hohenberger, abhi shelat, and Brent Waters</i>	
Identifying Cheaters without an Honest Majority	21
<i>Yuval Ishai, Rafail Ostrovsky, and Hakan Seyalioglu</i>	
On the Security of the “Free-XOR” Technique	39
<i>Seung Geol Choi, Jonathan Katz, Ranjit Kumaresan, and Hong-Sheng Zhou</i>	
Secure Two-Party Computation with Low Communication	54
<i>Ivan Damgård, Sebastian Faust, and Carmit Hazay</i>	

(Blind) Signatures and Threshold Encryption

Non-interactive CCA-Secure Threshold Cryptosystems with Adaptive Security: New Framework and Constructions	75
<i>Benoît Libert and Moti Yung</i>	
Round-Optimal Privacy-Preserving Protocols with Smooth Projective Hash Functions	94
<i>Olivier Blazy, David Pointcheval, and Damien Vergnaud</i>	
On the Instantiability of Hash-and-Sign RSA Signatures	112
<i>Yevgeniy Dodis, Iftach Haitner, and Aris Tentes</i>	
Beyond the Limitation of Prime-Order Bilinear Groups, and Round Optimal Blind Signatures	133
<i>Jae Hong Seo and Jung Hee Cheon</i>	

Zero-Knowledge and Security Models

On Efficient Zero-Knowledge PCPs	151
<i>Yuval Ishai, Mohammad Mahmoody, and Amit Sahai</i>	
Progression-Free Sets and Sublinear Pairing-Based Non-Interactive Zero-Knowledge Arguments	169
<i>Helger Lipmaa</i>	
Point Obfuscation and 3-Round Zero-Knowledge	190
<i>Nir Bitansky and Omer Paneth</i>	

Confidentiality and Integrity: A Constructive Perspective	209
<i>Ueli Maurer, Andreas Rüedlinger, and Björn Tackmann</i>	

Leakage-Resilience

Leakage-Resilient Circuits without Computational Assumptions	230
<i>Stefan Dziembowski and Sebastian Faust</i>	
A Parallel Repetition Theorem for Leakage Resilience	248
<i>Zvika Brakerski and Yael Tauman Kalai</i>	
Leakage-Tolerant Interactive Protocols	266
<i>Nir Bitansky, Ran Canetti, and Shai Halevi</i>	

Hash Functions

On the Public Indifferentiability and Correlation Intractability of the 6-Round Feistel Construction	285
<i>Avradip Mandal, Jacques Patarin, and Yannick Seurin</i>	
Collisions Are Not Incidental: A Compression Function Exploiting Discrete Geometry	303
<i>Dimitar Jetchev, Onur Özen, and Martijn Stam</i>	

Differential Privacy

Lower Bounds in Differential Privacy	321
<i>Anindya De</i>	
Iterative Constructions and Private Data Release	339
<i>Anupam Gupta, Aaron Roth, and Jonathan Ullman</i>	

Pseudorandomness I

From Non-adaptive to Adaptive Pseudorandom Functions	357
<i>Itay Berman and Iftach Haitner</i>	
Hardness Preserving Constructions of Pseudorandom Functions	369
<i>Abhishek Jain, Krzysztof Pietrzak, and Aris Tentes</i>	
Computational Extractors and Pseudorandomness	383
<i>Dana Dachman-Soled, Rosario Gennaro, Hugo Krawczyk, and Tal Malkin</i>	

Dedicated Encryption I

Functional Re-encryption and Collusion-Resistant Obfuscation	404
<i>Nishanth Chandran, Melissa Chase, and Vinod Vaikuntanathan</i>	
How to Delegate and Verify in Public: Verifiable Computation from Attribute-Based Encryption	422
<i>Bryan Parno, Mariana Raykova, and Vinod Vaikuntanathan</i>	
On Black-Box Reductions between Predicate Encryption Schemes	440
<i>Vipul Goyal, Virendra Kumar, Satya Lokam, and Mohammad Mahmoody</i>	

Security Amplification

Lossy Functions Do Not Amplify Well	458
<i>Krzysztof Pietrzak, Alon Rosen, and Gil Segev</i>	
Counterexamples to Hardness Amplification beyond Negligible	476
<i>Yevgeniy Dodis, Abhishek Jain, Tal Moran, and Daniel Wichs</i>	

Resettable and Parallel Zero Knowledge

Resettable Statistical Zero Knowledge	494
<i>Sanjam Garg, Rafail Ostrovsky, Ivan Visconti, and Akshay Wadia</i>	
The Knowledge Tightness of Parallel Zero-Knowledge	512
<i>Kai-Min Chung, Rafael Pass, and Wei-Lung Dustin Tseng</i>	
Simultaneously Resettable Arguments of Knowledge	530
<i>Chongwon Cho, Rafail Ostrovsky, Alessandra Scafuro, and Ivan Visconti</i>	

Dedicated Encryption II

Subspace LWE	548
<i>Krzysztof Pietrzak</i>	
Bounded-Collusion IBE from Key Homomorphism	564
<i>Shafi Goldwasser, Allison Lewko, and David A. Wilson</i>	
A Unified Approach to Deterministic Encryption: New Constructions and a Connection to Computational Entropy	582
<i>Benjamin Fuller, Adam O'Neill, and Leonid Reyzin</i>	

Pseudorandomness II

A Dichotomy for Local Small-Bias Generators 600
 Benny Applebaum, Andrej Bogdanov, and Alon Rosen

Randomness Condensers for Efficiently Samplable, Seed-Dependent
Sources 618
 Yevgeniy Dodis, Thomas Ristenpart, and Salil Vadhan

Uniqueness Is a Different Story: Impossibility of Verifiable Random
Functions from Trapdoor Permutations 636
 Dario Fiore and Dominique Schröder

Author Index 655