

Table of Contents

Parallel Repetition

An Efficient Parallel Repetition Theorem	1
<i>Johan Håstad, Rafael Pass, Douglas Wikström, and Krzysztof Pietrzak</i>	
Parallel Repetition Theorems for Interactive Arguments	19
<i>Kai-Min Chung and Feng-Hao Liu</i>	
Almost Optimal Bounds for Direct Product Threshold Theorem	37
<i>Charanjit S. Jutla</i>	

Obfuscation

On Symmetric Encryption and Point Obfuscation	52
<i>Ran Canetti, Yael Tauman Kalai, Mayank Varia, and Daniel Wichs</i>	
Obfuscation of Hyperplane Membership	72
<i>Ran Canetti, Guy N. Rothblum, and Mayank Varia</i>	

Invited Talk

Secure Computation and Its Diverse Applications	90
<i>Yuval Ishai</i>	

Multiparty Computation

On Complete Primitives for Fairness	91
<i>Dov Gordon, Yuval Ishai, Tal Moran, Rafail Ostrovsky, and Amit Sahai</i>	
On the Necessary and Sufficient Assumptions for UC Computation	109
<i>Ivan Damgård, Jesper Buus Nielsen, and Claudio Orlandi</i>	
From Passive to Covert Security at Low Cost	128
<i>Ivan Damgård, Martin Geisler, and Jesper Buus Nielsen</i>	

CCA Security

A Twist on the Naor-Yung Paradigm and Its Application to Efficient CCA-Secure Encryption from Hard Search Problems	146
<i>Ronald Cramer, Dennis Hofheinz, and Eike Kiltz</i>	

Two Is a Crowd? A Black-Box Separation of One-Wayness and Security
under Correlated Inputs 165
Yevgeniy Vahlis

Threshold Cryptography and Secret Sharing

Efficient, Robust and Constant-Round Distributed RSA Key
Generation 183
Ivan Damgård and Gert Læssøe Mikkelsen

Threshold Decryption and Zero-Knowledge Proofs for Lattice-Based
Cryptosystems 201
Rikke Bendlin and Ivan Damgård

Ideal Hierarchical Secret Sharing Schemes 219
Oriol Farràs and Carles Padró

Symmetric Cryptography

A Hardcore Lemma for Computational Indistinguishability: Security
Amplification for Arbitrarily Weak PRGs with Optimal Stretch 237
Ueli Maurer and Stefano Tessaro

On Related-Secret Pseudorandomness 255
David Goldenberg and Moses Liskov

A Domain Extender for the Ideal Cipher 273
*Jean-Sébastien Coron, Yevgeniy Dodis, Avradip Mandal, and
Yannick Seurin*

Delayed-Key Message Authentication for Streams 290
Marc Fischlin and Anja Lehmann

Key-Leakage and Tamper-Resistance

Founding Cryptography on Tamper-Proof Hardware Tokens 308
*Vipul Goyal, Yuval Ishai, Amit Sahai,
Ramarathnam Venkatesan, and Akshay Wadia*

Truly Efficient String Oblivious Transfer Using Resettable
Tamper-Proof Tokens 327
Vladimir Kolesnikov

Leakage-Resilient Signatures 343
*Sebastian Faust, Eike Kiltz, Krzysztof Pietrzak, and
Guy N. Rothblum*

Public-Key Encryption Schemes with Auxiliary Inputs	361
<i>Yevgeniy Dodis, Shafi Goldwasser, Yael Tauman Kalai,</i> <i>Chris Peikert, and Vinod Vaikuntanathan</i>	

Public-Key Cryptographic Primitives Provably as Secure as Subset Sum	382
<i>Vadim Lyubashevsky, Adriana Palacio, and Gil Segev</i>	

Rationality and Privacy

Rationality in the Full-Information Model	401
<i>Ronen Gradwohl</i>	

Efficient Rational Secret Sharing in Standard Communication Networks	419
<i>Georg Fuchsbauer, Jonathan Katz, and David Naccache</i>	

Bounds on the Sample Complexity for Private Learning and Private Data Release	437
<i>Amos Beimel, Shiva Prasad Kasiviswanathan, and Kobbi Nissim</i>	

Public-Key Encryption

New Techniques for Dual System Encryption and Fully Secure HIBE with Short Ciphertexts	455
<i>Allison Lewko and Brent Waters</i>	

Robust Encryption	480
<i>Michel Abdalla, Mihir Bellare, and Gregory Neven</i>	

Invited Talk

Privacy-Enhancing Cryptography: From Theory into Practice	498
<i>Jan Camenisch</i>	

Zero-Knowledge

Concise Mercurial Vector Commitments and Independent Zero-Knowledge Sets with Short Proofs	499
<i>Benoît Libert and Moti Yung</i>	

Eye for an Eye: Efficient Concurrent Zero-Knowledge in the Timing Model	518
<i>Rafael Pass, Wei-Lung Dustin Tseng, and</i> <i>Muthuramakrishnan Venkitasubramaniam</i>	

XII Table of Contents

Efficiency Preserving Transformations for Concurrent Non-malleable Zero Knowledge	535
<i>Rafail Ostrovsky, Omkant Pandey, and Ivan Visconti</i>	
Efficiency Limitations for Σ -Protocols for Group Homomorphisms	553
<i>Endre Bangerter, Jan Camenisch, and Stephan Krenn</i>	
Composition of Zero-Knowledge Proofs with Efficient Provers.....	572
<i>Eleanor Birrell and Salil Vadhan</i>	
Private Coins versus Public Coins in Zero-Knowledge Proof Systems ...	588
<i>Rafael Pass and Muthuramakrishnan Venkatasubramanian</i>	
Author Index	607