

Table of Contents – Part I

Symmetric Encryption and PRFs

Security of Symmetric Encryption against Mass Surveillance	1
<i>Mihir Bellare, Kenneth G. Paterson, and Phillip Rogaway</i>	
The Security of Multiple Encryption in the Ideal Cipher Model	20
<i>Yuanxi Dai, Jooyoung Lee, Bart Mennink, and John Steinberger</i>	
Minimizing the Two-Round Even-Mansour Cipher	39
<i>Shan Chen, Rodolphe Lampe, Jooyoung Lee, Yannick Seurin, and John Steinberger</i>	
Block Ciphers – Focus on the Linear Layer (feat. PRIDE)	57
<i>Martin R. Albrecht, Benedikt Driessen, Elif Bilge Kavun, Gregor Leander, Christof Paar, and Tolga Yalçın</i>	
Related-Key Security for Pseudorandom Functions Beyond the Linear Barrier	77
<i>Michel Abdalla, Fabrice Benhamouda, Alain Passelègue, and Kenneth G. Paterson</i>	

Formal Methods

Automated Analysis of Cryptographic Assumptions in Generic Group Models	95
<i>Gilles Barthe, Edvard Fagerholm, Dario Fiore, John Mitchell, Andre Scedrov, and Benedikt Schmidt</i>	

Hash Functions

The Exact PRF-Security of NMAC and HMAC	113
<i>Peter Gazi, Krzysztof Pietrzak, and Michal Rybár</i>	
Updates on Generic Attacks against HMAC and NMAC	131
<i>Jian Guo, Thomas Peyrin, Yu Sasaki, and Lei Wang</i>	
Improved Generic Attacks against Hash-Based MACs and HAIFA	149
<i>Itai Dinur and Gaëtan Leurent</i>	
Cryptography from Compression Functions: The UCE Bridge to the ROM	169
<i>Mihir Bellare, Viet Tung Hoang, and Sriram Keelveedhi</i>	

Indistinguishability Obfuscation and UCEs: The Case of Computationally Unpredictable Sources	188
<i>Christina Brzuska, Pooya Farshim, and Arno Mittelbach</i>	

Groups and Maps

Low Overhead Broadcast Encryption from Multilinear Maps	206
<i>Dan Boneh, Brent Waters, and Mark Zhandry</i>	
Security Analysis of Multilinear Maps over the Integers	224
<i>Hyung Tae Lee and Jae Hong Seo</i>	
Converting Cryptographic Schemes from Symmetric to Asymmetric Bilinear Groups	241
<i>Masayuki Abe, Jens Groth, Miyako Ohkubo, and Takeya Tango</i>	
Polynomial Spaces: A New Framework for Composite-to-Prime-Order Transformations	261
<i>Gottfried Herold, Julia Hesse, Dennis Hofheinz, Carla Ràfols, and Andy Rupp</i>	

Lattices

Revisiting the Gentry-Szydlo Algorithm	280
<i>H.W. Lenstra and A. Silverberg</i>	
Faster Bootstrapping with Polynomial Error	297
<i>Jacob Alperin-Sheriff and Chris Peikert</i>	
Hardness of k -LWE and Applications in Traitor Tracing	315
<i>San Ling, Duong Hieu Phan, Damien Stehlé, and Ron Steinfeld</i>	
Improved Short Lattice Signatures in the Standard Model	335
<i>Léo Ducas and Daniele Micciancio</i>	
New and Improved Key-Homomorphic Pseudorandom Functions	353
<i>Abhishek Banerjee and Chris Peikert</i>	

Asymmetric Encryption and Signatures

Homomorphic Signatures with Efficient Verification for Polynomial Functions	371
<i>Dario Catalano, Dario Fiore, and Bogdan Warinschi</i>	
Structure-Preserving Signatures from Type II Pairings	390
<i>Masayuki Abe, Jens Groth, Miyako Ohkubo, and Mehdi Tibouchi</i>	

(Hierarchical) Identity-Based Encryption from Affine Message Authentication	408
<i>Olivier Blazy, Eike Kiltz, and Jiazin Pan</i>	
Witness Encryption from Instance Independent Assumptions	426
<i>Craig Gentry, Allison Lewko, and Brent Waters</i>	
 Side Channels and Leakage Resilience I	
RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis	444
<i>Daniel Genkin, Adi Shamir, and Eran Tromer</i>	
On the Impossibility of Cryptography with Tamperable Randomness ...	462
<i>Per Austrin, Kai-Min Chung, Mohammad Mahmoody, Rafael Pass, and Karn Seth</i>	
 Obfuscation I	
Multiparty Key Exchange, Efficient Traitor Tracing, and More from Indistinguishability Obfuscation	480
<i>Dan Boneh and Mark Zhandry</i>	
Indistinguishability Obfuscation from Semantically-Secure Multilinear Encodings	500
<i>Rafael Pass, Karn Seth, and Sidharth Telang</i>	
On the Implausibility of Differing-Inputs Obfuscation and Extractable Witness Encryption with Auxiliary Input	518
<i>Sanjam Garg, Craig Gentry, Shai Halevi, and Daniel Wichs</i>	
 FHE	
Maliciously Circuit-Private FHE	536
<i>Rafail Ostrovsky, Anat Paskin-Cherniavsky, and Beni Paskin-Cherniavsky</i>	
Algorithms in HELib	554
<i>Shai Halevi and Victor Shoup</i>	
 Author Index	 573

Table of Contents – Part II

Quantum Cryptography

Quantum Position Verification in the Random Oracle Model	1
<i>Dominique Unruh</i>	
Single-Shot Security for One-Time Memories in the Isolated Qubits Model	19
<i>Yi-Kai Liu</i>	

Foundations of Hardness

How to Eat Your Entropy and Have It Too – Optimal Recovery Strategies for Compromised RNGs	37
<i>Yevgeniy Dodis, Adi Shamir, Noah Stephens-Davidowitz, and Daniel Wichs</i>	
Cryptography with Streaming Algorithms	55
<i>Periklis A. Papakonstantinou and Guang Yang</i>	

Obfuscation II

The Impossibility of Obfuscation with Auxiliary Input or a Universal Simulator	71
<i>Nir Bitansky, Ran Canetti, Henry Cohn, Shafi Goldwasser, Yael Tauman Kalai, Omer Paneth, and Alon Rosen</i>	
Self-bilinear Map on Unknown Order Groups from Indistinguishability Obfuscation and Its Applications	90
<i>Takashi Yamakawa, Shota Yamada, Goichiro Hanaoka, and Noboru Kunihiro</i>	
On Virtual Grey Box Obfuscation for General Circuits	108
<i>Nir Bitansky, Ran Canetti, Yael Tauman Kalai, and Omer Paneth</i>	

Number-Theoretic Hardness

Breaking ‘128-bit Secure’ Supersingular Binary Curves (Or How to Solve Discrete Logarithms in $\mathbb{F}_{2^{4 \cdot 1223}}$ and $\mathbb{F}_{2^{12 \cdot 367}}$)	126
<i>Robert Granger, Thorsten Kleinjung, and Jens Zumbärgel</i>	

Side Channels and Leakage Resilience II

Leakage-Tolerant Computation with Input-Independent
Preprocessing 146
 Nir Bitansky, Dana Dachman-Soled, and Huijia Lin

Interactive Proofs under Continual Memory Leakage 164
 Prabhanjan Ananth, Vipul Goyal, and Omkant Pandey

Information-Theoretic Security

Amplifying Privacy in Privacy Amplification 183
 Divesh Aggarwal, Yevgeniy Dodis, Zahra Jafargholi, Eric Miles, and Leonid Reyzin

On the Communication Complexity of Secure Computation 199
 Deepesh Data, Manoj M. Prabhakaran, and Vinod M. Prabhakaran

Optimal Non-perfect Uniform Secret Sharing Schemes 217
 Oriol Farràs, Torben Hansen, Tarik Kaced, and Carles Padró

Key Exchange and Secure Communication

Proving the TLS Handshake Secure (As It Is) 235
 Karthikeyan Bhargavan, Cédric Fournet, Markulf Kohlweiss, Alfredo Pironti, Pierre-Yves Strub, and Santiago Zanella-Béguelin

Memento: How to Reconstruct Your Secrets from a Single Password in
a Hostile Environment 256
 Jan Camenisch, Anja Lehmann, Anna Lysyanskaya, and Gregory Neven

Zero Knowledge

Scalable Zero Knowledge via Cycles of Elliptic Curves 276
 Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, and Madars Virza

Switching Lemma for Bilinear Tests and Constant-Size NIZK Proofs
for Linear Subspaces 295
 Charanjit S. Jutla and Arnab Roy

Physical Zero-Knowledge Proofs of Physical Properties 313
 Ben Fisch, Daniel Freund, and Moni Naor

Composable Security

Client-Server Concurrent Zero Knowledge with Constant Rounds and Guaranteed Complexity	337
<i>Ran Canetti, Abhishek Jain, and Omer Paneth</i>	
Round-Efficient Black-Box Construction of Composable Multi-Party Computation	351
<i>Susumu Kiyoshima</i>	

Secure Computation – Foundations

Secure Multi-Party Computation with Identifiable Abort	369
<i>Yuval Ishai, Rafail Ostrovsky, and Vassilis Zikas</i>	
Non-Interactive Secure Multiparty Computation	387
<i>Amos Beimel, Ariel Gabizon, Yuval Ishai, Eyal Kushilevitz, Sigurd Meldgaard, and Anat Paskin-Cherniavsky</i>	
Feasibility and Infeasibility of Secure Computation with Malicious PUFs	405
<i>Dana Dachman-Soled, Nils Fleischhacker, Jonathan Katz, Anna Lysyanskaya, and Dominique Schröder</i>	
How to Use Bitcoin to Design Fair Protocols	421
<i>Iddo Bentov and Ranjit Kumaresan</i>	

Secure Computation – Implementations

FleXOR: Flexible Garbling for XOR Gates That Beats Free-XOR	440
<i>Vladimir Kolesnikov, Payman Mohassel, and Mike Rosulek</i>	
Amortizing Garbled Circuits	458
<i>Yan Huang, Jonathan Katz, Vladimir Kolesnikov, Ranjit Kumaresan, and Alex J. Malozemoff</i>	
Cut-and-Choose Yao-Based Secure Computation in the Online/Offline and Batch Settings	476
<i>Yehuda Lindell and Ben Riva</i>	
Dishonest Majority Multi-Party Computation for Binary Circuits	495
<i>Enrique Larraia, Emmanuela Orsini, and Nigel P. Smart</i>	
Efficient Three-Party Computation from Cut-and-Choose	513
<i>Seung Geol Choi, Jonathan Katz, Alex J. Malozemoff, and Vassilis Zikas</i>	
Author Index	531