# Table of Contents – Part I

## Symmetric Encryption and PRFs

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

## Formal Methods

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automated Analysis of Cryptographic Assumptions in Generic Group Models</td>
<td>95</td>
</tr>
<tr>
<td>Gilles Barthe, Edvard Fagerholm, Dario Fiore, John Mitchell, Andre Scedrov, and Benedikt Schmidt</td>
<td></td>
</tr>
</tbody>
</table>

## Hash Functions

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Exact PRF-Security of NMAC and HMAC</td>
<td>113</td>
</tr>
<tr>
<td>Peter Gaži, Krzysztof Pietrzak, and Michal Rybár</td>
<td></td>
</tr>
<tr>
<td>Updates on Generic Attacks against HMAC and NMAC</td>
<td>131</td>
</tr>
<tr>
<td>Jian Guo, Thomas Peyrin, Yu Sasaki, and Lei Wang</td>
<td></td>
</tr>
<tr>
<td>Improved Generic Attacks against Hash-Based MACs and HAIFA</td>
<td>149</td>
</tr>
<tr>
<td>Itai Dinur and Gaëtan Leurent</td>
<td></td>
</tr>
<tr>
<td>Cryptography from Compression Functions: The UCE Bridge to the ROM</td>
<td>169</td>
</tr>
<tr>
<td>Mihir Bellare, Viet Tung Hoang, and Sriram Keelveedhi</td>
<td></td>
</tr>
</tbody>
</table>
# Table of Contents – Part I

## Indistinguishability Obfuscation and UCEs:
The Case of Computationally Unpredictable Sources

*Christina Brzuska, Pooya Farshim, and Arno Mittelbach* 188

## Groups and Maps

- **Low Overhead Broadcast Encryption from Multilinear Maps**
  *Dan Boneh, Brent Waters, and Mark Zhandry* 206

- **Security Analysis of Multilinear Maps over the Integers**
  *Hyung Tae Lee and Jae Hong Seo* 224

- **Converting Cryptographic Schemes from Symmetric to Asymmetric Bilinear Groups**
  *Masayuki Abe, Jens Groth, Miyako Ohkubo, and Takeya Tango* 241

## Lattices

- **Revisiting the Gentry-Szydlo Algorithm**
  *H.W. Lenstra and A. Silverberg* 280

- **Faster Bootstrapping with Polynomial Error**
  *Jacob Alperin-Sheriff and Chris Peikert* 297

- **Hardness of $k$-LWE and Applications in Traitor Tracing**
  *San Ling, Duong Hieu Phan, Damien Stehlé, and Ron Steinfeld* 315

- **Improved Short Lattice Signatures in the Standard Model**
  *Léo Ducas and Daniele Micciancio* 335

- **New and Improved Key-Homomorphic Pseudorandom Functions**
  *Abhishek Banerjee and Chris Peikert* 353

## Asymmetric Encryption and Signatures

- **Homomorphic Signatures with Efficient Verification for Polynomial Functions**
  *Dario Catalano, Dario Fiore, and Bogdan Warinschi* 371

- **Structure-Preserving Signatures from Type II Pairings**
  *Masayuki Abe, Jens Groth, Miyako Ohkubo, and Mehdi Tibouchi* 390
### Table of Contents - Part I

**XIII**

(Hierarchical) Identity-Based Encryption from Affine Message Authentication ........................................... 408

*Olivier Blazy, Eike Kiltz, and Jiaxin Pan*

Witness Encryption from Instance Independent Assumptions .................. 426

*Craig Gentry, Allison Lewko, and Brent Waters*

### Side Channels and Leakage Resilience I

RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis................. 444

*Daniel Genkin, Adi Shamir, and Eran Tromer*

On the Impossibility of Cryptography with Tamperable Randomness ... 462

*Per Austrin, Kai-Min Chung, Mohammad Mahmoody, Rafael Pass, and Karn Seth*

### Obfuscation I

Multiparty Key Exchange, Efficient Traitor Tracing, and More from Indistinguishability Obfuscation .............................................. 480

*Dan Boneh and Mark Zhandry*

Indistinguishability Obfuscation from Semantically-Secure Multilinear Encodings......................................................... 500

*Rafael Pass, Karn Seth, and Siddharth Telang*

On the Implausibility of Differing-Inputs Obfuscation and Extractable Witness Encryption with Auxiliary Input ......................... 518

*Sanjam Garg, Craig Gentry, Shai Halevi, and Daniel Wichs*

### FHE

Maliciously Circuit-Private FHE ........................................... 536

*Rafail Ostrovsky, Anat Paskin-Cherniavsky, and Beni Paskin-Cherniavsky*

Algorithms in HElib .................................................. 554

*Shai Halevi and Victor Shoup*

### Author Index

.......................... 573
Table of Contents – Part II

Quantum Cryptography

Quantum Position Verification in the Random Oracle Model
by Dominique Unruh

Single-Shot Security for One-Time Memories in the Isolated Qubits
Model by Yi-Kai Liu

Foundations of Hardness

How to Eat Your Entropy and Have It Too – Optimal Recovery
Strategies for Compromised RNGs by Yeugeniy Dodis, Adi Shamir, Noah Stephens-Davidowitz, and Daniel Wichs

Cryptography with Streaming Algorithms by Periklis A. Papakonstantinou and Guang Yang

Obfuscation II

The Impossibility of Obfuscation with Auxiliary Input or a Universal
Simulator by Nir Bitansky, Ran Canetti, Henry Cohn, Shafi Goldwasser,
Yael Tauman Kalai, Omer Paneth, and Alon Rosen

Self-bilinear Map on Unknown Order Groups from Indistinguishability
Obfuscation and Its Applications by Takashi Yamakawa, Shota Yamada, Goichiro Hanaoka, and Noboru Kunihiro

On Virtual Grey Box Obfuscation for General Circuits by Nir Bitansky, Ran Canetti, Yael Tauman Kalai, and Omer Paneth

Number-Theoretic Hardness

Breaking ‘128-bit Secure’ Supersingular Binary Curves (Or How to
Solve Discrete Logarithms in $\mathbb{F}_{2^{4.1223}}$ and $\mathbb{F}_{2^{12.367}}$) by Robert Granger, Thorsten Kleinjung, and Jens Zumbrägel
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  
  
  **Ran Canetti, Abhishek Jain, and Omer Paneth**

Round-Efficient Black-Box Construction of Composable Multi-Party Computation .................................................. 351  
  
  **Susumu Kiyoshima**

## Secure Computation — Foundations

Secure Multi-Party Computation with Identifiable Abort .................. 369  
  
  **Yuval Ishai, Rafail Ostrovsky, and Vassilis Zikas**

Non-Interactive Secure Multiparty Computation .......................... 387  
  
  **Amos Beimel, Ariel Gabizon, Yuval Ishai, Eyal Kushilevitz, Sigurd Meldgaard, and Anat Paskin-Cherniavsky**

Feasibility and Infeasibility of Secure Computation with Malicious PUFs .................................................. 405  
  
  **Dana Dachman-Soled, Nils Fleischhacker, Jonathan Katz, Anna Lysyanskaya, and Dominique Schröder**

How to Use Bitcoin to Design Fair Protocols .......................... 421  
  
  **Iddo Bentov and Ranjit Kumaresan**

## Secure Computation — Implementations

FleXOR: Flexible Garbling for XOR Gates That Beats Free-XOR ........ 440  
  
  **Vladimir Kolesnikov, Payman Mohassel, and Mike Rosulek**

Amortizing Garbled Circuits .................................................. 458  
  
  **Yan Huang, Jonathan Katz, Vladimir Kolesnikov, Ranjit Kumaresan, and Alex J. Malozemoff**

Cut-and-Choose Yao-Based Secure Computation in the Online/Offline and Batch Settings .................................................. 476  
  
  **Yehuda Lindell and Ben Riva**

Dishonest Majority Multi-Party Computation for Binary Circuits ........ 495  
  
  **Enrique Larraia, Emmanuela Orsini, and Nigel P. Smart**

Efficient Three-Party Computation from Cut-and-Choose ............... 513  
  
  **Seung Geol Choi, Jonathan Katz, Alex J. Malozemoff, and Vassilis Zikas**

### Author Index

- 531