

# Table of Contents – Part II

## Encryption Schemes

|                                                                                               |    |
|-----------------------------------------------------------------------------------------------|----|
| Concise Multi-challenge CCA-Secure Encryption and Signatures with Almost Tight Security ..... | 1  |
| <i>Benoît Libert, Marc Joye, Moti Yung, and Thomas Peters</i>                                 |    |
| Efficient Identity-Based Encryption over NTRU Lattices .....                                  | 22 |
| <i>Léo Ducas, Vadim Lyubashevsky, and Thomas Prest</i>                                        |    |
| Order-Preserving Encryption Secure Beyond One-Wayness .....                                   | 42 |
| <i>Isamu Teranishi, Moti Yung, and Tal Malkin</i>                                             |    |

## Outsourcing and Delegation

|                                                                                      |    |
|--------------------------------------------------------------------------------------|----|
| Statistically-secure ORAM with $\tilde{O}(\log^2 n)$ Overhead .....                  | 62 |
| <i>Kai-Min Chung, Zhenming Liu, and Rafael Pass</i>                                  |    |
| Adaptive Security of Constrained PRFs .....                                          | 82 |
| <i>Georg Fuchsbauer, Momchil Konstantinov, Krzysztof Pietrzak, and Vanishree Rao</i> |    |

## Obfuscation

|                                                                                                         |     |
|---------------------------------------------------------------------------------------------------------|-----|
| Poly-Many Hardcore Bits for Any One-Way Function and a Framework for Differing-Inputs Obfuscation ..... | 102 |
| <i>Mihir Bellare, Igors Stepanous, and Stefano Tessaro</i>                                              |     |
| Using Indistinguishability Obfuscation via UCEs .....                                                   | 122 |
| <i>Christina Brzuska and Arno Mittelbach</i>                                                            |     |
| Indistinguishability Obfuscation versus Multi-bit Point Obfuscation with Auxiliary Input .....          | 142 |
| <i>Christina Brzuska and Arno Mittelbach</i>                                                            |     |
| Bootstrapping Obfuscators via Fast Pseudorandom Functions .....                                         | 162 |
| <i>Benny Applebaum</i>                                                                                  |     |

## Homomorphic Cryptography

|                                                                                    |     |
|------------------------------------------------------------------------------------|-----|
| Homomorphic Authenticated Encryption Secure against Chosen-Ciphertext Attack ..... | 173 |
| <i>Chihong Joo and Aaram Yun</i>                                                   |     |

|                                                                                              |     |
|----------------------------------------------------------------------------------------------|-----|
| Authenticating Computation on Groups: New Homomorphic Primitives and Applications .....      | 193 |
| <i>Dario Catalano, Antonio Marcedone, and Orazio Puglisi</i>                                 |     |
| Compact VSS and Efficient Homomorphic UC Commitments .....                                   | 213 |
| <i>Ivan Damgård, Bernardo David, Irene Giacomelli, and Jesper Buus Nielsen</i>               |     |
| <b>Secret Sharing</b>                                                                        |     |
| Round-Optimal Password-Protected Secret Sharing and T-PAKE in the Password-Only Model .....  | 233 |
| <i>Stanislaw Jarecki, Aggelos Kiayias, and Hugo Krawczyk</i>                                 |     |
| Secret-Sharing for NP .....                                                                  | 254 |
| <i>Ilan Komargodski, Moni Naor, and Eylon Yogev</i>                                          |     |
| <b>Block Ciphers and Passwords</b>                                                           |     |
| Tweaks and Keys for Block Ciphers: The TWEAKEY Framework .....                               | 274 |
| <i>Jérémy Jean, Ivica Nikolić, and Thomas Peyrin</i>                                         |     |
| Memory-Demanding Password Scrambling .....                                                   | 289 |
| <i>Christian Forler, Stefan Lucks, and Jakob Wenzel</i>                                      |     |
| <b>Side Channel Analysis II</b>                                                              |     |
| Side-Channel Analysis of Multiplications in $GF(2^{128})$ : Application to AES-GCM .....     | 306 |
| <i>Sonia Belaïd, Pierre-Alain Fouque, and Benoît Gérard</i>                                  |     |
| Higher-Order Threshold Implementations .....                                                 | 326 |
| <i>Begül Bilgin, Benedikt Gierlichs, Svetla Nikova, Ventzislav Nikov, and Vincent Rijmen</i> |     |
| <i>Masks Will Fall Off</i> : Higher-Order Optimal Distinguishers .....                       | 344 |
| <i>Nicolas Bruneau, Sylvain Guilley, Annelie Heuser, and Olivier Rioul</i>                   |     |
| <b>Black-Box Separation</b>                                                                  |     |
| Black-Box Separations for One-More (Static) CDH and Its Generalization .....                 | 366 |
| <i>Jiang Zhang, Zhenfeng Zhang, Yu Chen, Yanfei Guo, and Zongyang Zhang</i>                  |     |
| Black-Box Separations for Differentially Private Protocols .....                             | 386 |
| <i>Dakshita Khurana, Hemanta K. Maji, and Amit Sahai</i>                                     |     |

## Composability

|                                                                                         |     |
|-----------------------------------------------------------------------------------------|-----|
| Composable Security of Delegated Quantum Computation .....                              | 406 |
| <i>Vedran Dunjko, Joseph F. Fitzsimons, Christopher Portmann,<br/>and Renato Renner</i> |     |
| All-But-Many Encryption: A New Framework for Fully-Equipped UC<br>Commitments .....     | 426 |
| <i>Eiichiro Fujisaki</i>                                                                |     |

## Multi-Party Computation

|                                                                                      |     |
|--------------------------------------------------------------------------------------|-----|
| Multi-valued Byzantine Broadcast: The $t < n$ Case .....                             | 448 |
| <i>Martin Hirt and Pavel Raykov</i>                                                  |     |
| Fairness versus Guaranteed Output Delivery in Secure Multiparty<br>Computation ..... | 466 |
| <i>Ran Cohen and Yehuda Lindell</i>                                                  |     |
| Actively Secure Private Function Evaluation .....                                    | 486 |
| <i>Payman Mohassel, Saeed Sadeghian, and Nigel P. Smart</i>                          |     |
| Efficient, Oblivious Data Structures for MPC .....                                   | 506 |
| <i>Marcel Keller and Peter Scholl</i>                                                |     |
| Author Index .....                                                                   | 527 |