Table of Contents – Part I

Session 1: Lattices and FHE

Practical Bootstrapping in Quasilinear Time 1
Jacob Alperin-Sheriff and Chris Peikert

Hardness of SIS and LWE with Small Parameters 21
Daniele Micciancio and Chris Peikert

Lattice Signatures and Bimodal Gaussians 40
Léo Ducas, Alain Durmus, Tancrède Lepoint, and Vadim Lyubashevsky

Learning with Rounding, Revisited: New Reduction, Properties and Applications 57
Joël Alwen, Stephan Krenn, Krzysztof Pietrzak, and Daniel Wichs

Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based 75
Craig Gentry, Amit Sahai, and Brent Waters

Invited Talk: Crypto Wars Part 2 Have Begun

Session 2: Foundations of Hardness

A Uniform Min-Max Theorem with Applications in Cryptography 93
Salil Vadhan and Colin Jia Zheng

Limits of Provable Security for Homomorphic Encryption 111
Andrej Bogdanov and Chin Ho Lee

Session 3: Cryptanalysis I

Counter-Cryptanalysis 129
Marc Stevens

Fuming Acid and Cryptanalysis: Handy Tools for Overcoming a Digital Locking and Access Control System 147
Daehyun Strobel, Benedikt Driessen, Timo Kasper, Gregor Leander, David Oswald, Falk Schellenberg, and Christof Paar

Real Time Cryptanalysis of Bluetooth Encryption with Condition Masking (Extended Abstract) 165
Bin Zhang, Chao Xu, and Dengguo Feng

Bibliografische Informationen
http://d-nb.info/1038377080

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

Session 4: Cryptanalysis II

Structural Evaluation of AES and Chosen-Key Distinguisher of 9-Round AES-128 183
Pierre-Alain Fouque, Jérémy Jean, and Thomas Peyrin

Bounds in Shallows and in Miseries 204
Céline Blondeau, Andrey Bogdanov, and Gregor Leander

Sieve-in-the-Middle: Improved MITM Attacks 222
Anne Canteaut, María Naya-Plasencia, and Bastien Vayssière

Construction of Differential Characteristics in ARX Designs Application to Skein 241
Gaëtan Leurent

Session 5: MPC – New Directions

On Fair Exchange, Fair Coins and Fair Sampling 259
Shashank Agrawal and Manoj Prabhakaran

Limits on the Power of Cryptographic Cheap Talk 277
Pavel Hubáček, Jesper Buus Nielsen, and Alon Rosen

Accuracy-Privacy Tradeoffs for Two-Party Differentially Private Protocols 298
Vipul Goyal, Ilya Mironov, Omkant Pandey, and Amit Sahai

Session 6: Leakage Resilience

Secure Computation against Adaptive Auxiliary Information 316
Elette Boyle, Sanjam Garg, Abhishek Jain, Yael Tauman Kalai, and Amit Sahai

Leakage-Resilient Symmetric Cryptography under Empirically Verifiable Assumptions 335
François-Xavier Standaert, Olivier Pereira, and Yu Yu

Session 7: Symmetric Encryption and PRFs

Highly-Scalable Searchable Symmetric Encryption with Support for Boolean Queries 353
David Cash, Stanislaw Jarecki, Charanjit Jutla, Hugo Krawczyk, Marcel-Cătălin Roşu, and Michael Steiner

Message-Locked Encryption for Lock-Dependent Messages 374
Martín Abadi, Dan Boneh, Ilya Mironov, Ananth Raghunathan, and Gil Segev

The Mix-and-Cut Shuffle: Small-Domain Encryption Secure against N Queries 392
Thomas Ristenpart and Scott Yilek

Key Homomorphic PRFs and Their Applications 410
Dan Boneh, Kevin Lewi, Hart Montgomery, and Ananth Raghunathan

Session 8: Key Exchange

On the Security of the TLS Protocol: A Systematic Analysis 429
Hugo Krawczyk, Kenneth G. Paterson, and Hoeteck Wee

New Techniques for SPHFs and Efficient One-Round PAKE Protocols 449
Fabrice Benhamouda, Olivier Blazy, Céline Chevalier, David Pointcheval, and Damien Vergnaud

Session 9: Multi Linear Maps

Practical Multilinear Maps over the Integers 476
Jean-Sébastien Coron, Tancrède Lepoint, and Mehdi Tibouchi

Full Domain Hash from (Leveled) Multilinear Maps and Identity-Based Aggregate Signatures 494
Susan Hohenberger, Amit Sahai, and Brent Waters

Programmable Hash Functions in the Multilinear Setting 513
Eduarda S.V. Freire, Dennis Hofheinz, Kenneth G. Paterson, and Christoph Striecks

Session 10: Ideal Ciphers

On the Indifferentiability of Key-Alternating Ciphers 531
Elena Andreeva, Andrey Bogdanov, Yevgeniy Dodis, Bart Mennink, and John P. Steinberger

Plain versus Randomized Cascading-Based Key-Length Extension for Block Ciphers 551
Peter Gaži

Digital Signatures with Minimal Overhead from Indifferentiable Random Invertible Functions 571
Eike Kiltz, Krzysztof Pietrzak, and Mario Szegedy

Author Index 589