Contents – Part I

Masking

Fully Homomorphic Encryption

Cryptanalysis II

Number Theory

Hash Functions

Multilinear Maps

Message Authentication Codes

Attacks on SSL/TLS

Real-World Protocols

Robust Designs

Lattice Reduction

Contents – Part II

Separations

Zero-Knowledge II

Protocols

Round Complexity

Commitments

Lattices

Leakage

Indifferentiability

Multi-Party Computation II

Obfuscation

Automated Analysis, Functional Encryption, and Non-malleable Codes

http://www.springer.com/978-3-662-49889-7

Advances in Cryptology – EUROCRYPT 2016
35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part I
Fischlin, M.; Coron, J.-S. (Eds.)
2016, XXVIII, 853 p. 155 illus., Softcover
ISBN: 978-3-662-49889-7