

1. Record Nr.	UNISA996503468403316
Titolo	Theory of cryptography : 20th international conference, TCC 2022, Chicago, IL, USA, November 7-10, 2022, proceedings, Part I // edited by Eike Kiltz and Vinod Vaikuntanathan
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2023] ©2023
ISBN	3-031-22318-7
Descrizione fisica	1 online resource (748 pages)
Collana	Lecture Notes in Computer Science ; ; v.13747
Disciplina	652.8
Soggetti	Cryptography Data encryption (Computer science)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Intro -- Preface -- Organization -- Contents - Part I -- Contents - Part II -- Contents - Part III -- Post-quantum Cryptography -- Post-quantum Insecurity from LWE -- 1 Introduction -- 1.1 Our Results -- 1.2 Related Work -- 2 Technical Overview -- 3 Open Problems -- 4 Preliminaries -- 4.1 Interactive Proofs of Quantumness -- 5 Deterministic Oracles with Quantum Advantage -- 5.1 Quantum Advantage for Unbounded-Classical Query Algorithms -- 5.2 Quantum Disclosure of Secrets -- 6 Counterexamples for Post-quantum Security -- 6.1 Counterexamples for Standard Cryptographic Primitives -- 6.2 Counterexamples for One-Time Primitives -- References -- Adaptive Versus Static Multi-oracle Algorithms, and Quantum Security of a Split-Key PRF -- 1 Introduction -- 2 Preliminaries -- 3 A General Adaptive-to-Static Reduction for Multi-oracle Algorithms -- 3.1 Our Result -- 3.2 The Technical Core -- 3.3 Wrapping up the Proof of Theorem 1 -- 3.4 Applications -- 4 Quantum Security of a Split-Key PRF -- 4.1 Hybrid Security and skPRFs -- 4.2 Quantum-Security of the skPRF -- 4.3 Proof of Theorem 2 -- References -- The Parallel Reversible Pebbling Game: Analyzing the Post-quantum Security of iMHFs -- 1 Introduction -- 1.1 Our Results -- 1.2 Technical Overview -- 1.3 Related Work -- 2 Parallel Reversible Pebbling Games -- 3 Reversible Pebbling Attacks and Applications on iMHFs -- 3.1 Warmup: Parallel

Reversible Pebbling Attack on a Line Graph -- 3.2 Reversible Pebbling Attacks on (e,d)-Reducible DAGs -- 3.3 Reversible Pebbling Attacks Using an Induced Line Graph -- 4 Reversible Pebbling Attacks for Minimizing Cumulative Complexity -- 4.1 A Reversible Pebbling Attack -- References -- Quantum Rewinding for Many-Round Protocols -- 1 Introduction -- 1.1 Our Results -- 1.2 Related Work -- 1.3 Organization -- 2 Technical Overview -- 2.1 Quantum Rewinding. 2.2 Lattice-Based Bulletproofs -- 3 Preliminaries -- 3.1 Lattices -- 3.2 Quantum Information -- 4 Recursive Special Sound and Last-Round Collapsing Arguments -- 5 Quantum Tree-Extraction -- 5.1 Notation and Quantum Algorithms -- 5.2 Description of the Extractor -- 5.3 Correctness -- 6 Collapsing Hash Function Families -- 6.1 Definitions -- 6.2 Bounded Homomorphic Public-Key Encryption -- 6.3 A Fold-Collapsing Hash Function -- References -- Interactive Proofs -- Fiat-Shamir Transformation of Multi-round Interactive Proofs -- 1 Introduction -- 1.1 Background and State of the Art -- 1.2 Our Results -- 1.3 Related Work -- 1.4 Structure of the Paper -- 2 Preliminaries -- 2.1 (Non-)Interactive Proofs -- 2.2 Negative Hypergeometric Distribution -- 3 An Abstract Sampling Game -- 4 Fiat-Shamir Transformation of Sigma-Protocols -- 5 Refined Analysis of the Abstract Sampling Game -- 6 Fiat-Shamir Transformation of Multi-round Protocols -- 7 The Fiat-Shamir Transformation of Parallel Repetitions -- References -- Steganography-Free Zero-Knowledge -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Applications -- 1.3 Our Techniques -- 1.4 Related Work -- 2 Preliminaries -- 3 Defining Steganography-Freeness -- 3.1 Steganography-Free Zero-Knowledge -- 4 A Steganography-Free ZK Protocol -- 4.1 Our Protocol -- 4.2 Analysis -- References -- Vector Commitments over Rings and Compressed -Protocols -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Related Work -- 2 Technical Overview -- 3 Preliminaries -- 3.1 Vector Commitments -- 3.2 Interactive Proofs -- 4 Vector Commitments over Z_m -- 4.1 Vector Commitments from Single-Value Commitments -- 4.2 Single-Value Commitments via Commitment Friendly Groups -- 4.3 Single-Value Commitment Schemes for Even m -- 5 Compressed -Protocol -- 5.1 Vector Commitments over Ring Extensions -- 5.2 Standard -Protocol. 5.3 Compression Mechanism -- 5.4 Compressed -Protocol -- 6 An Application: Verifiable Computation on Encrypted Data with Context-Hiding -- References -- Universally Composable -protocols in the Global Random-Oracle Model -- 1 Introduction -- 2 Preliminaries -- 2.1 -protocols, Revisited -- 2.2 Straight-Line Compilers -- 2.3 OR-Protocols -- 3 Properties of GUC NIZKPoK -- 3.1 GroRO and GrpoRO, Revisited -- 3.2 The NIZKPoK Ideal Functionality -- 3.3 The CRS Ideal Functionality -- 3.4 GUC Security Definitions -- 3.5 GUC NIZKPoK are Complete, NIM-SHVZK, and NI-SSS -- 4 GUC NIZKPoK in the Programmable Global ROM -- 5 GUC NIZKPoK in the Observable Global ROM -- 5.1 Generating a CRS that Plays Nice with -protocols -- 5.2 GUC Compiler -- 5.3 Realizing FNIZK in the GRO-FCRS-hybrid Model -- 6 Constructions via the Randomized Fischlin Transform -- 6.1 The Randomized Fischlin Transform, Revisited -- 6.2 Efficient, GUC NIZKPoK in the GrpoRO-hybrid Model -- 6.3 Efficient, GUC NIZKPoK in the GroRO-FCRS-hybrid Model -- References -- Quantum Cryptography -- Pseudorandom (Function-Like) Quantum State Generators: New Definitions and Applications -- 1 Introduction -- 1.1 Our Results -- 1.2 Threshold for Computational Assumptions -- 1.3 Cryptographic Applications with Classical Communication -- 2 Preliminaries -- 2.1 Distance Metrics and Matrix Norms -- 2.2 Quantum Algorithms -- 2.3 Pseudorandomness Notions -- 3 Adaptive

Security -- 3.1 Classical Access -- 3.2 Quantum Access -- 4 On the Necessity of Computational Assumptions -- 5 Tomography with Verification -- 5.1 Correctness Notions for Verifiable Tomography -- 5.2 Verifiable Tomography Procedures -- 6 Applications -- 6.1 Commitment Scheme -- References -- Candidate Trapdoor Claw-Free Functions from Group Actions with Applications to Quantum Protocols -- 1 Introduction -- 1.1 Our Results -- 1.2 Technical Overview. 2 Preliminaries -- 2.1 Quantum Information -- 2.2 Cryptographic Group Actions and Extended LHS Assumption -- 3 Weak Trapdoor Claw-Free Functions -- 3.1 XOR Lemmas for Adaptive Hardcore Bits -- 4 wTCF from Extended LHS Assumption -- 5 Computational Test of Qubit -- 5.1 Definition -- 5.2 Protocol -- 5.3 Analysis -- References -- Collusion Resistant Copy-Protection for Watermarkable Functionalities -- 1 Introduction -- 1.1 Our Results -- 1.2 Related Works -- 1.3 Technical Overview -- 1.4 Discussions and Open Problems -- 1.5 Organization -- 2 Preliminaries -- 2.1 Coset States -- 2.2 Measure Success Probabilities of Quantum Adversaries: Projective/Threshold Implementation -- 3 Collusion Resistant Unclonable Decryption -- 3.1 Definitions -- 3.2 Construction -- 3.3 Proof of Anti-Piracy -- References -- Secret-Sharing and Applications -- On Secret Sharing, Randomness, and Random-less Reductions for Secret Sharing -- 1 Introduction -- 1.1 Our Results -- 1.2 Related Work -- 1.3 Technical Overview -- 1.4 Open Questions -- 2 Preliminaries -- 2.1 Notation -- 2.2 Probability Theory -- 2.3 Amplifying Leakage-Resilience -- 3 Randomness Extraction from Leakage-Resilient Secret Sharing Schemes -- 3.1 The Main Result -- 3.2 Efficient Leakage-Resilient Secret Sharing Requires Efficiently Extractable Randomness -- 3.3 An Extension to the Setting of Computational Security -- 4 Random-Less Reductions for Secret Sharing -- 4.1 Distribution Designs from Partial Steiner Systems -- A Proof of Lemma3 -- References -- Leakage-resilient Linear Secret-sharing Against Arbitrary Bounded-size Leakage Family -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Prior Relevant Works -- 2 Technical Overview -- 3 Preliminaries -- 3.1 Matrices -- 3.2 Codes and Linear Secret-sharing Schemes -- 3.3 Joint Leakage-resilience of Secret-sharing Scheme -- 3.4 Fourier Analysis. 4 Leakage-resilience of Fully Random Code -- 5 Leakage-resilience of Shamir Secret-sharing Schemes with Random Evaluation Places -- 6 Leakage-resilience of Partially Random Code -- References -- Asymptotically Free Broadcast in Constant Expected Time via Packed VSS -- 1 Introduction -- 1.1 Our Results -- 1.2 Applications and Discussions -- 1.3 Related Work -- 2 Technical Overview -- 2.1 Improved Broadcast in Constant Expected Rounds -- 2.2 Packed Verifiable Secret Sharing -- 2.3 Optimal Gradecast -- 3 Preliminaries -- 3.1 Bivariate Polynomials -- 3.2 Finding (n,t) -STAR -- 4 Packed Verifiable Secret Sharing -- 5 Balanced Gradecast -- 5.1 The Gradecast Protocol -- 5.2 Making the Protocol Balanced -- 6 Multi-moderated Packed Secret Sharing -- 6.1 Reconstruction -- 7 Oblivious Leader Election -- 8 Broadcast -- 8.1 Byzantine Agreement -- 8.2 Broadcast and Parallel-broadcast -- References -- Succinct Proofs -- On Black-Box Constructions of Time and Space Efficient Sublinear Arguments from Symmetric-Key Primitives -- 1 Introduction -- 1.1 Our Results -- 1.2 Technical Overview -- 1.3 A Comparison with Related Work -- 2 Preliminaries -- 2.1 Circuit Notations -- 2.2 Zero-Knowledge Arguments -- 2.3 Random-Access Machines (RAM) -- 2.4 Succinct Matrix -- 3 Lower Bound for Space-Efficient Encoding Schemes -- 3.1 Interpreting the Lower Bound in the Context of Proof Systems -- 3.2 Warm Up: A Simple Lower Bound -- 3.3 Lower Bound for Multi-pass Space-Efficient Encoding Schemes -- 4 Main Construction -- 5 Space-

Efficient Affine Code Testing for Interleaved Reed Solomon Codes --
References -- A Toolbox for Barriers on Interactive Oracle Proofs -- 1
Introduction -- 1.1 Our Results -- 1.2 Related Work -- 2 Techniques
-- 2.1 Tools for Length and Round Reduction -- 2.2 Tools for
Improving Completeness -- 2.3 Tools for Derandomization.
2.4 Deriving Our Results Using the Tools.
