1.

| | |
|---|---|
| Record Nr. | UNINA9910616370103321 |
| Titolo | Advances in cryptology - CRYPTO 2022 : 42nd annual international cryptology conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, proceedings, Part II / / edited by Yevgeniy Dodis and Thomas Shrimpton |
| Pubbl/distr/stampa | Cham, Switzerland : , : Springer, , [2022]<br>©2022 |
| ISBN | 3-031-15979-9 |
| Descrizione fisica | 1 online resource (830 pages) |
| Collana | Lecture Notes in Computer Science ; ; v.13508 |
| Disciplina | 652.8 |
| Soggetti | Cryptography<br>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 II -- Secure Messaging -- .24em plus .1em minus .1emUniversally Composable End-to-End Secure Messaging -- 1 Introduction -- 1.1 This Work -- 1.2 On the Ideal Secure Messaging Functionality, FSM -- 1.3 Realizing FSM, Modularly -- 1.4 Streamlining UC Analysis -- 1.5 Related Work -- 2 Universally Composable Security: New Capabilities -- 3 Formal Modeling and Analysis -- References -- On the Insider Security of MLS -- 1 Introduction -- 1.1 Background and Motivation -- 1.2 Our Contribution -- 1.3 Related Work -- 1.4 Outline of the Rest of the Paper -- 2 Preliminaries -- 2.1 Notation -- 2.2 Universal Composability -- 3 Insider-Secure Continuous Group Key Agreement -- 3.1 Overview -- 3.2 PKI Setup -- 3.3 Interfaces of the CGKA Functionality -- 3.4 History Graph -- 3.5 Details of the CGKA Functionality -- 4 The Insider-Secure TreeKEM Protocol -- 5 Security of ITK -- 6 Insider Attacks -- 6.1 An Attack on Authenticity in Certain Modes -- 6.2 Breaking Agreement -- 6.3 Inadequate Joiner Security (Tree-Signing) -- 6.4 IND-CPA Security Is Insufficient -- References -- Lattice-Based Zero Knowledge -- Lattice-Based Zero-Knowledge Proofs and Applications: Shorter, Simpler, and More General -- 1 Introduction -- 1.1 Prior Art for Proofs of (1) -- 1.2 Our Results -- 1.3 Techniques |

Overview -- 2 Preliminaries -- 2.1 Notation -- 2.2 Probability Distributions -- 2.3 Module-SIS and Module-LWE Problems -- 2.4 Rejection Sampling -- 2.5 Challenge Space -- 3 The ABDLOP Commitment Scheme and Proofs of Linear Relations -- 3.1 The ABDLOP Commitment Scheme -- 4 Proofs of Quadratic Relations -- 4.1 Single Quadratic Equation with Automorphisms -- 4.2 Many Quadratic Equations with Automorphisms -- 4.3 Polynomial Evaluations with Vanishing Constant Coefficients -- References.

Lattice-Based SNARKs: Publicly Verifiable, Preprocessing, and Recursively Composable -- 1 Introduction -- 1.1 The Seascape of SNARKs -- 1.2 Our Contributions -- 1.3 Technical Overview -- 1.4 Application -- 1.5 Related Work -- 2 Preliminaries -- 2.1 Lattices -- 2.2 Sampling Algorithms -- 2.3 Hard Problems -- 3 The kMISIS Assumption -- 3.1 Knowledge Variants -- 4 Compact Extractable Vector Commitments -- 4.1 Definitions -- 4.2 Construction -- References -- Practical Sublinear Proofs for R1CS from Lattices -- 1 Introduction -- 1.1 Technical Overview -- 2 Preliminaries -- 2.1 Notation -- 2.2 Module-SIS and Module-LWE Problems -- 2.3 Challenge Space -- 2.4 BDLOP Commitment Scheme -- 3 Interactive Schwartz-Zippel -- 3.1 Making Use of Lemma 2 in Zero-Knowledge Protocols -- 4 Exact Amortized Binary Opening Proof -- 4.1 Extending the Proof to Linear and Product Relations -- 4.2 Proof Size -- 5 Induction -- References -- Quantum Cryptography II -- On the Impossibility of Key Agreements from Quantum Random Oracles -- 1 Introduction -- 1.1 Our Results -- 1.2 Technical Overview -- 1.3 Related Work -- 2 Preliminaries and Notation -- 2.1 Quantum Computation -- 2.2 Key Agreement Using Quantum Computation and Classical Communication -- 3 Attacking Classical-Alice Quantum-Bob Protocols -- 3.1 Useful Lemmas -- 3.2 The Attack and Its Analysis -- 4 Attacking Quantum-Alice Quantum-Bob Protocols -- 4.1 Main Conjecture and Related Notions -- 4.2 Attacking Quantum-Alice Quantum-Bob Protocols -- 4.3 Proof of Lemma 4.7 -- 5 Case of Exponentially Small Influences: Proving Theorem 4.4 -- 5.1 The Polynomial Formulation -- 5.2 Proving Theorem 4.4 -- References -- Succinct Classical Verification of Quantum Computation -- 1 Introduction -- 2 Technical Overview -- 2.1 Recap: Mahadev's Measurement Protocol -- 2.2 Defining a (Succinct) Measurement Protocol.

2.3 Constructing a Verifier-Succinct Measurement Protocol -- 2.4 Proof of Soundness -- 2.5 From a Verifier-Succinct Measurement Protocol to Succinct Arguments for BQP -- References -- On the Feasibility of Unclonable Encryption, and More -- 1 Introduction -- 1.1 Achieving Unclonable Indistinguishability: Challenges -- 1.2 Our Results -- 1.3 Organization -- 1.4 Technical Overview -- 1.5 Related Work -- 2 Preliminaries -- 2.1 Basics -- 2.2 Quantum Random Oracle Model (QROM) -- 2.3 More on Jordan's Lemma -- 2.4 Measuring Success Probability -- 2.5 Unclonable Encryption -- 3 More on Coset States -- 3.1 Preliminaries -- 3.2 Strengthened MOE Game in the QROM -- 3.3 Proof for Theorem 12 -- 4 Unclonable Encryption in the QROM -- 5 Copy-Protection for Point Functions in QROM -- 5.1 Copy-Protection Preliminaries -- 5.2 Construction -- References -- Lattice-Based Signatures -- Shorter Hash-and-Sign Lattice-Based Signatures -- 1 Introduction -- 1.1 Hash-and-Sign Signatures over Lattices -- 1.2 Our Contributions -- 1.3 Related Works -- 2 Background -- 3 New Hash-and-Sign Tradeoffs -- 3.1 Shorter Signatures by Elliptic Sampling -- 3.2 Parameters Selection -- 4 Security Analysis -- 4.1 Forging Signatures -- 4.2 Key-Recovery Attacks -- 4.3 Concrete Security Estimates -- 5 Batch Compressing Gaussian Vectors -- 5.1 Preliminary

Information-Theoretical Analysis -- 5.2 Golomb-Rice Style Coding of a Single Variable -- 5.3 Batch-Coding and Full Signature Compression -- 5.4 Nearly Optimal Encoding for Hash-and-Sign Signatures -- References -- MuSig-L: Lattice-Based Multi-signature with Single-Round Online Phase -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Our Techniques -- 1.3 Other Related Work -- 2 Preliminaries -- 2.1 Assumptions -- 2.2 Offline-Online Multi-signature -- 3 Our MuSig-L Scheme -- 3.1 Definition of the Scheme -- 3.2 Rejection Sampling. 3.3 Correctness and Efficiency Analysis -- 4 Security Proofs -- 4.1 Reduction to LWE and SIS -- 4.2 Switching Lemma -- 4.3 Simulating Nonces via Trapdoor Sampling -- 4.4 Oracle Simulation Lemma -- 4.5 MS-UF-CMA Security of MuSig-L -- References -- A New Framework for More Efficient Round-Optimal Lattice-Based (Partially) Blind Signature via Trapdoor Sampling -- 1 Introduction -- 1.1 Background -- 1.2 Our Contribution -- 1.3 Technical Overview -- 2 Preliminaries -- 2.1 Blind Signature -- 2.2 Non-interactive Zero-Knowledge Proofs in the (Q)ROM -- 3 Lattice-Based Blind Signature from Compatible Commitments -- 3.1 Trapdoor-Sampling-Compatible Commitments -- 3.2 Construction of Blind Signature -- 3.3 Proof of One-More Unforgeability -- 3.4 Extension: Partially Blind Signatures -- 4 Instantiating Our Generic Construction -- 4.1 Concrete Choices for Trapdoor-Sampling-Compatible Commitments and Single-Proof Extractable NIZK -- 4.2 Concrete Choice for Multi-proof Extractable NIZK -- 4.3 Putting Everything Together -- References -- Blockchain -- Ofelimos: Combinatorial Optimization via Proof-of-Useful-Work*1mm -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Work -- 1.3 Organization of the Paper -- 2 Preliminaries -- 3 Doubly Parallel Local Search -- 3.1 Overview -- 3.2 DPLS Modeled in a Blockchain Setting -- 3.3 An Example -- 3.4 Generality of the Approach -- 4 Moderately Hard DAG Computations -- 4.1 Syntax -- 4.2 Moderate Hardness -- 5 The PoUW Blockchain Protocol -- 5.1 Protocol Description -- 5.2 Deployment Considerations -- 6 Security Analysis -- 6.1 Ledger Security -- 6.2 Protocol Usefulness -- References -- Practical Statistically-Sound Proofs of Exponentiation in Any Group -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Additional Related Work -- 2 Basic Protocol -- 2.1 Soundness -- 2.2 Efficiency. 3 Reducing (Verifier-) Complexity by Batching -- 3.1 The Protocol -- 3.2 Improving Verifier's Efficiency -- A Improving Verifier's Efficiency -- B Application in Polynomial Commitments -- B.1 Efficiency -- References -- .26em plus .1em minus .1emFormalizing Delayed Adaptive Corruptions and the Security of Flooding Networks -- 1 Introduction -- 1.1 Motivation -- 1.2 Contributions and Results -- 1.3 Techniques -- 1.4 Related Work -- 2 Preliminaries -- 2.1 Notation -- 2.2 Universally Composable Security -- 3 Delayed Adversaries Within UC -- 3.1 The -Delay Shell -- 3.2 Relating Corruption Models -- 4 Functionalities -- 4.1 MessageTransfer -- 4.2 Flood -- 5 Implementations of Flood -- 5.1 Naive Flood -- 5.2 Efficient Flood -- 6 Conclusion and Future Work -- References -- Best Paper Awards -- Batch Arguments for NP and More from Standard Bilinear Group Assumptions -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Technical Overview -- 1.3 Related Work -- 2 Preliminaries -- 2.1 Non-Interactive Batch Arguments for NP -- 3 BARG for NP from Subgroup Decision in Bilinear Groups -- 4 BARG for NP from k-Lin in Bilinear Groups -- 5 Extensions and Applications -- References -- Breaking Rainbow Takes a Weekend on a Laptop -- 1 Introduction -- 2 Preliminaries -- 3 Simple Attack -- 4 Combination with Rectangular MinRank Attack -- 5 Experimental Results and Conclusion -- A Rank Experiments -- References -- Some Easy Instances of Ideal-SVP and

Implications on the Partial Vandermonde Knapsack Problem -- 1 Introduction -- 2 Preliminaries -- 2.1 Number Fields -- 2.2 Lattices -- 2.3 Representation and Size of Algebraic Objects -- 2.4 The Partial Vandermonde Knapsack Problem -- 3 Easy Instances of Ideal-SVP -- 3.1 Reducing the Ideal in a Subfield -- 3.2 Proof of Theorem 3.1 -- 4 Easy Instances of Partial Vandermonde Knapsack -- 4.1 PV-Knap as an Instance of Ideal Hermite BDD.
4.2 Reduction from Ideal Hermite BDD to Ideal Hermite SVP in the Inverse Ideal.