1. Record Nr. UNISA996594166903316

Autore	Joye Marc
Titolo	Advances in Cryptology - EUROCRYPT 2024 : 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26-30, 2024, Proceedings, Part VI
Pubbl/distr/stampa	Cham : , : Springer International Publishing AG, , 2024 ©2024
ISBN	3-031-58751-0
Edizione	[1st ed.]
Descrizione fisica	1 online resource (493 pages)
Collana	Lecture Notes in Computer Science Series ; ; v.14656
Altri autori (Persone)	LeanderGregor
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- Contents - Part VI -- Multi-party Computation and Zero-Knowledge (II/II) -- Jolt: SNARKs for Virtual Machines via Lookups -- 1 Introduction -- 1.1 SNARKs for Virtual Machine Abstractions -- 1.2 Jolt: a0- New Paradigm for zkVM Design -- 1.3 Costs of Jolt -- 1.4 Comparison of Prover Costs to Prior Works -- 1.5 Technical Details: CPU Instructions as Structured Polynomials -- 1.6 Decomposable Instructions -- 2 Technical Preliminaries -- 2.1 Multilinear Extensions -- 2.2 Lookup Arguments -- 2.3 Memory Checking -- 3 An Overview of RISC-V and Jolt's Approach -- 3.1 Performing Instruction Logic Using Lookups -- 3.2 Using Memory-Checking -- 3.3 Formatting Assembly Code -- 4 Analyzing MLE-Structure and Decomposability -- 4.1 The Equality Function -- 4.2 Less Than Comparision -- 4.3 Shift Left Logical -- 4.4 The Multiplication Extension -- 5 Putting It All Together: A SNARK for RISC-V Emulation -- 5.1 Combining Instruction Lookup Tables into One -- 6 Qualitative Cost Estimation -- 6.1 Cost of a Lookup -- 6.2 Overall Prover Costs in Jolt -- 6.3 Cost of Memory Operations -- References -- Constant-Size zk-SNARKs in ROM from Falsifiable Assumptions -- 1 Introduction -- 2 Preliminaries -- 2.1 Polynomial Commitment Schemes -- 2.2 Succinct Zero-Knowledge Arguments -- 3 ARSDH: Underlying Security Assumption -- 4 Special Soundness of KZG -- 4.1 Special Soundness -- 5 Rewinding Lemma -- 6 Black-Box Extractability -- 7 Application

to SNARKs -- 7.1 Polynomial IOP -- 7.2 Compiling Polynomial IOPs into Arguments -- References -- Lower-Bounds on Public-Key Operations in PIR -- 1 Introduction -- 1.1 Our Results -- 2 Technical Overview -- 2.1 Generic Group Model -- 2.2 Proof Sketch of Main Theorem -- 2.3 PIR Related Protocols -- 2.4 Oracles -- 3 Related Work -- 4 Preliminaries -- 4.1 Oblivious Transfer.
4.2 Private-Information Retrieval (PIR) -- 5 Protocols that Imply Non-Trivial PIR -- 5.1 Oblivious Transfer -- 5.2 Unbalanced Private-Set Intersection -- 6 Lower-Bounds on the Number Oracle Queries in PIR -- 7 Communication Lower-Bounds for OT Extension -- References -- Fast Public-Key Silent OT and More from Constrained Naor-Reingold -- 1 Introduction -- 2 Technical Overview -- 2.1 A PCF for OT from Pseudorandomly Constrained PRFs -- 2.2 A CPRF for Inner-Product Membership from the Naor-Reingold PRF -- 2.3 Inner-Product Membership Weak Pseudorandom Functions -- 2.4 Optimizations -- 2.5 Final PCF Construction -- 2.6 Concrete Parameters -- 2.7 Public Key PCF -- 2.8 Application: A Simple Reusable DV-NIZK Reusable -- 3 Preliminaries -- 4 Constraining the Naor-Reingold PRF -- 5 Fast PCFs for OTs from Pseudorandomly Constrained PRFs -- 6 Public-Key PCF for OT Correlations -- 7 DV-NIZKs from PK-PCFs -- References -- Best-of-Both-Worlds Multiparty Quantum Computation with Publicly Verifiable Identifiable Abort -- 1 Introduction -- 1.1 Our Results -- 2 Technical Overview -- 2.1 Why is MPQC-PVIA Hard to Achieve? -- 2.2 Our Solution: Auditable Quantum Authentication (AQA) -- 2.3 From AQA to MPQC-PVIA -- 2.4 Best-of-Both-Worlds Security -- 3 Preliminary -- 3.1 Quantum Computation -- 3.2 Quantum One-Time Pad -- 3.3 Quantum Authentication Code -- 3.4 Quantum Error-Correction Code -- 3.5 Quantum Teleportation -- 4 Model and Definition -- 4.1 The Ideal World of BoBW-MPQC-PVIA -- 4.2 (Preprocessing) MPC-Hybrid Model -- 5 Auditable Quantum Authentication (AQA) -- 5.1 Construction -- 5.2 Security -- 6 MPQC-PVIA with Trusted Setup -- 6.1 Security -- 7 BoBW-MPQC-PVIA with Trusted Setup -- 8 BoBW-MPQC-PVIA Without Trusted Setup -- 8.1 Protocol -- References -- The Hardness of LPN over Any Integer Ring and Field for PCG Applications -- 1 Introduction.
1.1 Our Contributions -- 2 Preliminary -- 2.1 Notation -- 2.2 Learning Parity with Noise -- 3 The Hardness of LPN with Regular Noise Distributions -- 4 The Hardness of LPN over Integer Rings -- 4.1 Reduction from Decisional LPN over Z2 to LPN over F2 -- 4.2 Reduction from LPN over F2 to Decisional LPN over Z2 -- 4.3 Reduction from Computational LPN over Z2 to LPN over F2 -- 5 Concrete Analysis of Low-Noise LPN over Finite Fields -- 5.1 The Hardness of LPN with Regular Noise Distributions -- References -- Unlocking the Lookup Singularity with Lasso -- 1 Introduction -- 1.1 Lasso: A New Lookup Argument -- 1.2 Additional Discussion of Lasso's Costs -- 1.3 A Companion Work: Jolt, and the Lookup Singularity -- 2 Technical Overview -- 2.1 Starting Point: Spark Sparse Polynomial Commitment Scheme -- 2.2 Surge: A Generalization of Spark -- 3 A Stronger Analysis of Spark -- 3.1 A (slightly) Simpler Result: c=2 -- 3.2 The General Result -- 3.3 Specializing the Spark Sparse Commitment Scheme to Lasso -- 4 Surge: A Generalization of Spark, Providing Lasso -- References -- Efficient Pre-processing PIR Without Public-Key Cryptography -- 1 Introduction -- 1.1 Our Results -- 1.2 Technical Highlights -- 2 Formal Definitions -- 3 Privately Programmable Pseudorandom Set with List Decoding -- 3.1 Definition -- 3.2 Construction -- 3.3 Proof of Correctness -- 3.4 Proof of Security -- 4 Our Two-Server PIR Scheme -- 4.1 Construction -- 4.2 Privacy Proof -- 4.3 Correctness Proof -- 5 Our Single-Server PIR Scheme -- 5.1

Construction -- 5.2 Privacy Proof -- 5.3 Correctness Proof -- 6 Evaluation -- 6.1 Experiments Results -- References -- Strong Batching for Non-interactive Statistical Zero-Knowledge -- 1 Introduction -- 1.1 Technical Overview -- 1.2 Related Works -- 1.3 Discussion and Open Problems -- 2 Preliminaries -- 2.1 Probability Theory Background.
2.2 Hash Functions with Bounded Independence -- 3 Non-Interactive Statistical Zero-Knowledge -- 3.1 Smooth Entropy Approximation -- 4 Derandomizing Batch Reductions -- 5 Batching AI by Direct Composition -- 5.1 Proof of Lemma 8 -- 5.2 Proof of Proposition 1 -- 5.3 Proof of Proposition 2 -- References -- Two-Round Maliciously-Secure Oblivious Transfer with Optimal Rate -- 1 Introduction -- 2 Technical Overview -- 2.1 Warmup: The PVW Protocol -- 2.2 Batch OT with Trapdoor Hash Functions -- 2.3 Computational Sender Security via LPN -- 2.4 Key-Homomorphic Trapdoor Hash Functions -- 2.5 Compressing the Receiver's Message via LPN and Key-Homomorphic TDH -- 2.6 Correcting Errors and Achieving Malicious Security -- 2.7 Discussion -- 3 Key-Homomorphic Trapdoor Hash Function -- 3.1 Construction from QR -- 4 Composable Oblivious Transfer with Optimal Rate -- 4.1 Ingredients -- 4.2 Universally Composable Oblivious Transfer with Optimal Rate -- References -- Succinct Homomorphic Secret Sharing -- 1 Introduction -- 1.1 Our Results -- 1.2 Technical Overview-Construction of Succinct HSS -- 1.3 Technical Overview-Applications of Succinct HSS -- 2 Notation and Preliminaries -- 2.1 Computational Assumptions -- 2.2 The NIDLS Framework -- 3 Defining Bilinear HSS -- 4 Public-Key Bilinear HSS Constructions -- 4.1 Public-Key Bilinear HSS for All Matrices Based in the NIDLS Framework -- 5 Succinct Half-Chosen Vector OLE -- 5.1 Succinct Half-Chosen VOLE and Key-Compact, Matrix-Compact Bilinear HSS -- 6 Succinct HSS -- References -- How to Garble Mixed Circuits that Combine Boolean and Arithmetic Computations -- 1 Introduction -- 1.1 Our Results -- 2 Preliminaries -- 2.1 Computation Models -- 2.2 Garbled Circuits (GC) -- 3 Technical Overview -- 3.1 Background: Key-Extension Implies Arithmetic GC -- 3.2 Bit-Decomposition and Bit-Composition Imply Mixed GC.
3.3 The Naive Construction -- 4 Mixed GC for Zpk -- 4.1 Extension: Linear BC and General BD -- 4.2 Extension: Emulating Computations for ZN -- 5 Mixed GC Based on Chinese Remainder Theorem -- 6 Mixed GC Based on DCR -- 6.1 Bit-Composition Based on Paillier Encryption -- 6.2 Bit-Decomposition Based on Damgård-Jurik Encryption -- References -- Classic Public Key Cryptography (I/II) -- M&amp -- M'S: Mix and Match Attacks on Schnorr-Type Blind Signatures with Repetition -- 1 Introduction -- 1.1 Our Contribution -- 2 Background -- 2.1 Notation -- 2.2 Sigma Protocols -- 2.3 Blind Signature Schemes -- 3 Mix-and-Match Attacks -- 3.1 Schnorr-Type Blind Signatures -- 3.2 Main Attack -- 3.3 Two Out of k Attack -- 3.4 One Out of One Attack -- 4 Cryptanalysis of CSI-Otter -- 4.1 Cryptographic Group Actions -- 4.2 The Scheme -- 5 Discussion -- 5.1 Concurrent Security -- 5.2 Sequential Security -- 5.3 Revisiting CSI-Otter Parameters -- 6 Conclusion -- References -- The Supersingular Endomorphism Ring and One Endomorphism Problems are Equivalent -- 1 Introduction -- 1.1 Contributions -- 1.2 Technical Overview -- 2 Preliminaries -- 2.1 Notation -- 2.2 Quaternion Algebras -- 2.3 Elliptic Curves -- 2.4 Computing with Isogenies -- 2.5 Computational Problems -- 2.6 Probabilities -- 2.7 Categories -- 3 Equidistribution of Elliptic Curves with Extra Data -- 3.1 Statement of the Equidistribution Theorem -- 3.2 Proof of Theorem 3.10 and Proposition 3.11 -- 4 Enriching a OneEnd Oracle -- 5 On Conjugacy-Invariant Distributions