1. Record Nr. UNINA9910741190803321

Titolo	Advances in Cryptology – CRYPTO 2023 [[electronic resource]] : 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20–24, 2023, Proceedings, Part II / / edited by Helena Handschuh, Anna Lysyanskaya
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2023
ISBN	3-031-38545-4
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (XIX, 792 p. 81 illus., 18 illus. in color.)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14082
Disciplina	005.824
Soggetti	Cryptography Data encryption (Computer science) Computer engineering Computer networks Computer networks—Security measures Coding theory Information theory Cryptology Computer Engineering and Networks Mobile and Network Security Coding and Information Theory
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- Contents - Part II -- Succinctness -- Revisiting Cycles of Pairing-Friendly Elliptic Curves -- 1 Introduction -- 1.1 Avoiding Non-native Arithmetic with Cycles -- 1.2 State of the Art -- 1.3 Contributions and Organization -- 2 Pairing-Friendly Elliptic Curves -- 2.1 Elliptic Curves -- 2.2 Pairing-Friendly Polynomial Families -- 3 Cycles of Elliptic Curves -- 3.1 Definition and Known Results -- 3.2 Some Properties of Cycles -- 4 Cycles from Known Families -- 4.1 Cycles from Parametric-Families -- 4.2 2-cycles from Parametric Families -- 5 Density of Pairing-Friendly Cycles -- 6 Conclusions -- A Polynomial Division -- B Tables -- C SageMath Code

-- References -- Non-interactive Zero-Knowledge from Non-interactive Batch Arguments -- 1 Introduction -- 1.1 Technical Overview -- 2 Preliminaries -- 2.1 Non-Interactive Zero-Knowledge Arguments for NP -- 2.2 Non-Interactive Batch Arguments for NP -- 2.3 Hidden-Bits Generator -- 3 Hidden-Bits Generator from Batch Arguments -- References -- Lattice-Based Succinct Arguments from Vanishing Polynomials -- 1 Introduction -- 1.1 Our Results -- 1.2 Related Work -- 1.3 Subsequent Work -- 2 Technical Overview -- 2.1 Vanishing-SIS Commitments -- 2.2 Efficient Proofs for SIS Relations -- 2.3 Applications -- 3 Preliminaries -- 3.1 Cyclotomic Rings -- 3.2 Lattice Trapdoors -- 3.3 Presumed Hard Problems -- 3.4 Argument Systems -- 4 Vanishing Short Integer Solutions -- 4.1 Definition -- 4.2 On Choice of Parameters -- 4.3 A Family of Hash Functions with Short Keys -- 5 Foldable Structures -- 6 Folding Protocols -- 6.1 Type-0 Linear Relations -- 6.2 Type-1 Linear Relations -- 7 Knowledge-Based Protocols -- 7.1 Linear Relations -- 7.2 Well-Formedness of vSIS Commitments -- 8 Applications -- 8.1 Proving Binary-Satisfiability of (Structured) Linear Equations -- 8.2 Rank-1 Constraint Systems. References -- Orbweaver: Succinct Linear Functional Commitments from Lattices -- 1 Introduction -- 1.1 Our Results -- 1.2 Related Work -- 1.3 Technical Overview -- 2 Preliminaries -- 2.1 Functional Commitments -- 2.2 Sampling Algorithm -- 2.3 Cryptographic Assumptions -- 3 Cryptanalysis of k-P-R-ISIS -- 4 Orbweaver: Linear Map Commitments for rings -- 4.1 Extensions -- 5 Linear Map Commitments for ZM -- 5.1 Polynomial Commitments for integers mod p -- 6 Evaluation -- 6.1 Optimizations -- 6.2 Proof and CRS Sizes -- References -- Non-interactive Universal Arguments -- 1 Introduction -- 1.1 Results -- 1.2 Technical Overview -- 2 Preliminaries -- 2.1 Homomorphic Encryption -- 2.2 Non-interactive Arguments for Deterministic Computations -- 2.3 Incrementally Verifiable Computation -- 2.4 Average-Case Puzzles -- 3 Universal Lifting -- 3.1 Incrementally Verifiable Computation Lifting -- 4 Constructing Average-Case Puzzles -- 4.1 Worst-Case Hardness Assumptions -- 4.2 Average-Case Puzzles from FHE -- References -- Succinct Arguments for RAM Programs via Projection Codes -- 1 Introduction -- 1.1 Black-Box Succincts Argument for RAM Programs -- 1.2 Projection Codes -- 1.3 Related Work -- 2 Overview of Techniques -- 2.1 Projection Codes -- 2.2 Holographic PCPs for RAM Programs -- 2.3 Succinct Arguments for RAM Programs -- 3 Preliminaries -- 3.1 Model of Computation -- 3.2 Encoding Scheme -- 3.3 Probabilistically Checkable Proofs of Proximity (PCPPs) -- 4 Projection Codes -- 4.1 Constructing Projection Codes -- 4.2 Instantiations -- 5 Holographic PCPs for RAM Programs -- 5.1 Holographic PCPs for Subsets -- 5.2 Holographic PCPs for RAM Programs -- 6 Succinct Arguments for RAM Programs -- References -- Brakedown: Linear-Time and Field-Agnostic SNARKs for R1CS -- 1 Introduction -- 1.1 Results and Contributions -- 2 Preliminaries. 3 Linear-Time Polynomial Commitments -- 3.1 Polynomial Commitments for t=2 -- 4 Fast Linear Codes with Linear-Time Encoding -- 5 Linear-Time SNARKs for R1CS -- 5.1 A Self-contained Description of Brakedown and Shockwave -- 6 Implementation and Evaluation -- 6.1 Evaluation of Polynomial Commitment Schemes -- 6.2 Evaluation of Brakedown and Shockwave SNARKs -- References -- Lattice-Based Succinct Arguments for NP with Polylogarithmic-Time Verification -- 1 Introduction -- 1.1 Our Results -- 1.2 Related Work -- 2 Techniques -- 2.1 Our Approach -- 2.2 Polynomial Commitments from Sumcheck Arguments -- 2.3 Warmup: Delegation over Bilinear Groups -- 2.4 Leveled Bilinear Modules -- 2.5 Delegation over Leveled Bilinear-Module Systems -- 2.6 Polynomial IOP for Product Rings -- 2.7

Final Protocol: Combining Polynomial Commitments and PIOP -- References -- SNARGs for Monotone Policy Batch NP -- 1 Introduction -- 1.1 Our Results -- 2 Our Techniques -- 2.1 The Canonical Protocol -- 2.2 Enforcing Global Properties with Predicate Extractable Hashing -- 2.3 New SNARG Construction -- 2.4 Achieving Somewhere Extractability -- 2.5 Shortening the CRS -- 3 Preliminaries -- 3.1 Hash Family with Local Opening -- 3.2 Fully Homomorphic Encryption -- 3.3 Somewhere Extractable Batch Arguments (seBARGs) -- 3.4 RAM SNARGs -- 4 SNARGs for Monotone Policy BatchNP -- 4.1 Definition -- 5 Predicate Extractable Hash Families -- 5.1 Syntax and Basic Properties -- 5.2 Extractable Hash for Bit-Fixing Predicates -- 5.3 Extractable Hash with Tags for Bit-Fixing Predicates -- 6 Non-Adaptive SNARG Construction -- 6.1 Analysis -- References -- TreePIR: Sublinear-Time and Polylog-Bandwidth Private Information Retrieval from DDH -- 1 Introduction -- 1.1 Client-Preprocessing PIR -- 1.2 Our Contribution -- 1.3 Related Work -- 1.4 Notation -- 1.5 Paper Outline -- 2 Preliminaries.
2.1 Security Definitions for PIR -- 2.2 Pseudorandom Generators (PRGs) and Pseudorandom Functions (PRFs) -- 2.3 The GGM PRF Construction and Puncturing -- 3 Weak Privately Puncturable PRFs -- 3.1 A wpPRF Construction -- 4 Applying wpPRFs to PIR -- 4.1 Constructing Pseudorandom Sets from wpPRFs -- 4.2 Our TreePIR Scheme -- 4.3 Sublinear Time, Polylog Bandwidth PIR from the DDH Assumption -- 4.4 Tuning Efficiencies in TreePIR -- 5 Performance -- 5.1 TreePIR with No Recursion -- 5.2 Recursing to Improve Bandwidth -- 5.3 Supporting Changing Databases -- A Further Optimizations -- A.1 Deterministic Client Time -- A.2 Generalizing TreePIR to More Flexible Database Sizes -- References -- Multi-party Homomorphic Secret Sharing and Sublinear MPC from Sparse LPN -- 1 Introduction -- 1.1 Our Results -- 1.2 Related Work -- 2 Technical Overview -- 2.1 HSS Construction -- 2.2 Arguing KDM Security -- 2.3 Sublinear MPC Construction -- 3 Preliminaries -- 3.1 Linear Secret Sharing Schemes -- 3.2 Homomorphic Secret Sharing -- 4 Sparse LPN -- 4.1 KDM Security -- 5 HSS Construction -- 5.1 Scheme Description -- 5.2 Security Analysis -- 6 Sublinear MPC -- 6.1 Protocol Description -- References -- Anonymous Credentials -- Lattice Signature with Efficient Protocols, Application to Anonymous Credentials -- 1 Introduction -- 1.1 Related Works -- 1.2 Our Contributions -- 2 Preliminaries -- 2.1 Lattices -- 2.2 Probabilities -- 2.3 Hardness Assumption -- 2.4 Signature Scheme -- 3 A Lattice-Based Signature Scheme -- 3.1 Description of the Signature -- 3.2 Security of the Signature -- 3.3 Our Signature on Modules -- 4 Zero-Knowledge Arguments of Knowledge -- 4.1 A Framework for Quadratic Relations over Zq -- 4.2 Zero-Knowledge Fast Mode Revisited -- 4.3 Zero-Knowledge Arguments and Relations -- 5 Privacy-Preserving Protocols and Anonymous Credentials.
5.1 Oblivious Signing Protocol -- 5.2 Message-Signature Pair Possession Protocol -- 5.3 Application to Anonymous Credentials -- References -- A Framework for Practical Anonymous Credentials from Lattices -- 1 Introduction -- 1.1 Blind Signatures and Anonymous Credentials from ISISf -- 1.2 Related Work -- 1.3 Concurrent Work -- 1.4 Discussion and Open Problems -- 2 Preliminaries -- 2.1 NTRU Lattices -- 2.2 Module-SIS and Module-LWE Problems -- 2.3 Non-interactive Zero-Knowledge Proofs in the ROM -- 3 The ISISf Assumption -- 3.1 Concrete Instantiations of f -- 3.2 Interactive Version -- 3.3 Applications to Exotic Signatures -- References -- Anonymous Tokens with Stronger Metadata Bit Hiding from Algebraic MACs -- 1 Introduction -- 2 PMBT: A Case Study -- 2.1 AT Interface and Security -- 2.2 Potential Attack for PMBT -- 3 Anonymous Tokens

Revisited -- 3.1 AT Interface -- 3.2 Unforgeability -- 3.3 Unlinkability -- 3.4 Privacy of the Metadata Bit -- 4 ATHM: Anonymous Tokens with Hidden Metadata -- 4.1 The ATHM Components -- 4.2 The MAC Building Block -- 4.3 The Simulatable Proof Building Block -- 5 Performance -- 6 Security Proof for ATHM in the Generic Group Model -- 6.1 OMUF Security in GGM and ROM -- 6.2 UNLINK Security in GGM and ROM -- 6.3 PMB Security in GGM and ROM -- 7 Conclusion -- References -- New Paradigms and Foundations -- Revisiting Time-Space Tradeoffs for Function Inversion -- 1 Introduction -- 1.1 Our Results -- 1.2 Our Techniques -- 1.3 Related Work -- 1.4 A Note on the Many Facets of Function Inversion -- 2 Preliminaries -- 2.1 Definitions of Function Inversion Problems -- 2.2 Some Basic Probability Results -- 2.3 Binary Linear Codes -- 3 An Improvement to Fiat and Naor's Algorithm -- 3.1 The Algorithm -- 3.2 Analysis -- 4 A Lower Bound Against Guess-and-check Non-adaptive Algorithms -- 5 Comparing Variants of Function Inversion.
5.1 Search-to-decision Reduction for Arbitrary Functions.

Sommario/riassunto

The five-volume set, LNCS 14081, 140825, 14083, 14084, and 14085 constitutes the refereed proceedings of the 43rd Annual International Cryptology Conference, CRYPTO 2023. The conference took place at Santa Barbara, USA, during August 19-24, 2023. The 124 full papers presented in the proceedings were carefully reviewed and selected from a total of 479 submissions. The papers are organized in the following topical sections: Part I: Consensus, secret sharing, and multi-party computation; Part II: Succinctness; anonymous credentials; new paradigms and foundations; Part III: Cryptanalysis; side channels; symmetric constructions; isogenies; Part IV: Faster fully homomorphic encryption; oblivious RAM; obfuscation; secure messaging; functional encryption; correlated pseudorandomness; proof systems in the discrete-logarithm setting. .