1. Record Nr. UNINA990005652800403321

Titolo	L'imagination créatrice : rencontre internationale organisée par la Fondation pour une entraide intellectuelle européenne, Poigny-la-Forêt, 9-13 octobre 1970 / actes mis en forme par Roselyne Chenu ; avant-propos de Pierre Emmanuel
Pubbl/distr/stampa	Neuchâtel : A la Bacomière, c1971
Descrizione fisica	286 p. ; 21 cm
Collana	Langages
Disciplina	372.5
Locazione	FLFBC
Collocazione	P.1 PG 761
Lingua di pubblicazione	Francese
Formato	Materiale a stampa
Livello bibliografico	Monografia

2. Record Nr. UNISALENTO991002285439707536

Autore	Touring club italiano
Titolo	Venezia Giulia / L.V. Bertarelli
Pubbl/distr/stampa	Milano : Touring club italiano, 1934
Edizione	[3. ed.]
Descrizione fisica	443 p., [30] c. geogr. : ill. ; 16 cm
Collana	Guida d'Italia del Touring club italiano
Altri autori (Persone)	Bertarelli, Luigi Vittorioauthor
Disciplina	914.539
Soggetti	Venezia Giulia - Guide
Lingua di pubblicazione	Italiano
Formato	Materiale a stampa
Livello bibliografico	Monografia

3. Record Nr. UNISA996594168903316

Autore	Tang Qiang
Titolo	Public-Key Cryptography – PKC 2024 : 27th IACR International Conference on Practice and Theory of Public-Key Cryptography, Sydney, NSW, Australia, April 15–17, 2024, Proceedings, Part II / / edited by Qiang Tang, Vanessa Teague
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
ISBN	3-031-57722-1
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (468 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14602
Altri autori (Persone)	TeagueVanessa
Disciplina	5,824
Soggetti	Cryptography Data encryption (Computer science) Cryptology
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia

Nota di contenuto

Intro -- Preface -- Organization -- Contents - Part II -- Commitments -- Updatable, Aggregatable, Succinct Mercurial Vector Commitment from Lattice -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Technique Overview -- 1.3 Related Work -- 2 Preliminaries -- 2.1 Notation -- 2.2 Lattice Preliminaries -- 2.3 BASIS Assumption -- 2.4 Mercurial Vector Commitment -- 3 Succinct Mercurial Vector Commitments Based on BASIS -- 3.1 Updatable Mercurial Vector Commitments -- 3.2 Aggregatable Mercurial Vector Commitment -- 4 Application: Lattice-Based ZK-EDB -- References -- Vector Commitments with Proofs of Smallness: Short Range Proofs and More -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Technical Overview -- 1.3 Related Work -- 1.4 Organization -- 2 Background and Definitions -- 2.1 Hardness Assumptions -- 2.2 Non-interactive Arguments -- 2.3 Algebraic Group Model -- 3 Short Proofs that a Committed Vector Is Binary -- 4 A Range Proof with Very Short Proofs -- 4.1 Description -- 4.2 Security in the AGM and ROM -- 4.3 Batched Range Proofs and Proving the Smallness of Vectors -- 4.4 Comparisons -- References -- Simulation-Extractable KZG Polynomial Commitments and Applications to HyperPlonk -- 1 Introduction -- 1.1 Contributions -- 1.2 Technical Overview -- 1.3 Related Work -- 2 Background and Definitions -- 2.1 Definitions for Polynomials -- 2.2 Hardness Assumptions -- 2.3 Succinct Non-interactive Arguments -- 2.4 Algebraic Group Model -- 2.5 Polynomial Commitments -- 3 Commitments to Multivariate Polynomials -- 3.1 The Multivariate PCS of Zhang et al. -- 3.2 Enforcing a Special Shape for Committed Polynomials -- 4 A Simulation-Extractable Variant of Zhang et al.'s Polynomial Commitment -- 4.1 Description -- 4.2 Extensions -- 5 A Simulation-Extractable Variant of HyperPlonk -- 5.1 Description -- 5.2 Security -- References -- Oblivious Accumulators.
1 Introduction -- 1.1 Our Contributions -- 2 Preliminaries -- 2.1 Notation -- 2.2 Compressing Primitives -- 3 KVC Based on Acc and VC -- 3.1 Construction I with Weak Key Binding -- 3.2 Construction II with Strong Key Binding -- 3.3 Relation to Existing Constructions -- 4 Oblivious Accumulators -- 4.1 Definition -- 4.2 Obliviousness Properties -- 5 OblvAcc Based on KVC -- 5.1 Construction -- 5.2 Soundness -- 5.3 Element Hiding -- 5.4 Add-Del Indistinguishability -- 5.5 Extension for Unique Accumulation of Elements -- 6 Lower Bounds -- 6.1 Oblivious Accumulators -- 6.2 Oblivious Accumulators Without Add-Del Indistinguishability -- References -- Witness Encryption for Succinct Functional Commitments and Applications -- 1 Introduction -- 1.1 Our Work: WE for Succinct Functional Commitments -- 1.2 Our Contributions -- 1.3 Technical Overview -- 1.4 Related Work -- 2 Preliminaries -- 2.1 Functional Commitment Schemes -- 3 WEFC: Witness Encryption for Functional Commitment -- 4 Our WEFC Construction -- 4.1 Smooth Projective Hash Functions -- 4.2 Our Construction -- 5 Our WEFC Instantiations -- 5.1 Our FC for Monotone Span Programs -- 5.2 Other Instantiations -- 6 From WEFC to Reusable Non-interactive MPC -- 6.1 Preliminaries on mrNISC -- 6.2 Our mrNISC Construction -- 7 Other Application Scenarios -- 7.1 Targeted Broadcast -- 7.2 Simple Contingent Payment for Services -- References -- Multiparty Computation -- Network-Agnostic Multi-party Computation Revisited (Extended Abstract) -- 1 Introduction -- 1.1 Technical Overview -- 2 Preliminaries and Definitions -- 2.1 Primitives and Definitions -- 2.2 Existing Building Blocks -- 3 Network-Agnostic Byzantine Broadcast -- 3.1 Asynchronous Broadcast with Weaker Synchronous Guarantees -- 3.2 Synchronous Byzantine Agreement -- 3.3 BOBW BC -- 4 Network-Agnostic VSS -- 5 Agreement on a Common Subset (ACS).

6 The Preprocessing Phase Protocol -- 6.1 Network-Agnostic Beaver's Multiplication Protocol -- 6.2 Network-Agnostic Triple-Transformation Protocol -- 6.3 Network-Agnostic Protocol for Generating a Random Value -- 6.4 Network-Agnostic Polynomial-Verification Protocol -- 6.5 Network-Agnostic Triple-Sharing Protocol -- 6.6 Network-Agnostic Triple-Extraction Protocol -- 6.7 The Network-Agnostic Preprocessing Phase Protocol -- 7 The Network-Agnostic Circuit-Evaluation Protocol -- 8 Conclusion and Open Problems -- References -- On Information-Theoretic Secure Multiparty Computation with Local Repairability -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Related Work -- 1.3 Organization -- 2 Preliminaries -- 2.1 Secret Sharing Schemes -- 2.2 Linear Codes -- 2.3 Security Model -- 3 Our Linear Secret-Sharing Scheme with Good Locality -- 3.1 Reconstruction, Multiplicativity and Strong Multiplicativity -- 3.2 Privacy Analysis -- 4 Passively Secure Repairing Protocol for Multiplicative Variants of -- 5 Actively Secure Repairing Protocol for Strongly-Multiplicative Variants of -- A Comparison with a Two-Level Shamir's Secret Sharing Scheme -- References -- Zero Knowledge Proofs -- Zero Knowledge Protocols and Signatures from the Restricted Syndrome Decoding Problem -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Paper Organization -- 2 Notation and Preliminaries -- 2.1 Cryptographic Tools -- 2.2 Linear Codes -- 3 The Restricted Syndrome Decoding Problem -- 3.1 Solving R-SDP -- 4 Building ZK Protocols from the R-SDP: A Preliminary Analysis -- 4.1 Zero Knowledge Masking of Restricted Vectors -- 4.2 The Case Study of CVE with R-SDP -- 5 R-SDP(G): Using Subgroups of the Restricted Group -- 5.1 Properties of the Restricted Group -- 5.2 Cyclic Subgroups of the Restricted Group -- 5.3 Solving R-SDP with Restricted Subgroup -- 5.4 Criteria to Design R-SDP(G).
5.5 R-SDP(G) in Practice: Easy to Implement and Tight Parameters -- 6 ZK Protocols from the R-SDP: Modern Protocols -- 6.1 R-GPS: The GPS Scheme with R-SDP -- 6.2 R-BG: The BG-PKP Scheme with R-SDP -- 7 Comparison with NIST Candidates -- 8 Conclusion -- References -- Ring/Module Learning with Errors Under Linear Leakage - Hardness and Applications -- 1 Introduction -- 1.1 Our Results -- 1.2 Technical Overview -- 2 Preliminaries -- 2.1 Cyclotomic Rings -- 2.2 Discrete Gaussian Distribution -- 2.3 MLWE -- 3 Hardness: MLWE with Linear Leakage -- 4 Application: More Efficient Opening Proof for One-Time BDLOP Commitment -- 4.1 Classical Opening Proof of BDLOPCommitment and Rejection Sampling Algorithms -- 4.2 More Efficient One-Time Opening Proof Through Using Generalized Subset Rejection Sampling Algorithms -- 4.3 Comparison of Efficiency -- References -- Succinct Verification of Compressed Sigma Protocols in the Updatable SRS Setting -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Work -- 1.3 Technical Overview -- 2 Preliminaries -- 2.1 Interactive Arguments -- 2.2 Assumptions -- 3 CSP for Committed Linear Forms -- 3.1 Opening a Committed Linear Form -- 3.2 Improved Protocol for Opening a Committed Linear Form -- 4 Updatable SRS zkSNARK for Circuit Satisfiability -- 4.1 Committing to a Linear Form for Multiplication Gates -- 4.2 Hadamard Product Argument -- 4.3 Permutation Argument -- 4.4 Putting Things Together - zkSNARK for Circuit SAT -- 5 CSP for Committed Homomorphism -- 5.1 Commitment Scheme -- 5.2 Succinct Verifier - Protocol for Opening Committed Homomorphism -- References -- Lookup Arguments: Improvements, Extensions and Applications to Zero-Knowledge Decision Trees -- 1 Introduction -- 1.1 Technical Overview -- 1.2 Related Work -- 2 Preliminaries -- 2.1 Commit-and-Prove SNARKs -- 2.2 Extractable Commitment Schemes.
2.3 Polynomial, Vector and Matrix Commitment Schemes -- 3 Zero-

Knowledge Matrix Lookup Arguments -- 4 Our New Zero-Knowledge Lookup Arguments -- 4.1 cq+ Lookup Argument -- 4.2 Our Fully Zero-Knowledge Lookup Argument -- 5 Our Matrix Lookup Argument -- 5.1 The Straw Man Solution -- 5.2 Our Scheme -- 5.3 Concrete Efficiency -- 6 Zero-Knowledge Decision Tree Statistics -- 6.1 Security Model -- 6.2 The Extended Encoding of Decision Trees -- 6.3 Extractable Commitment to Decision Trees -- 6.4 CP-SNARK for Statistics on Decision Trees -- 6.5 Efficiency and Concrete Instantiations -- References -- Short Code-Based One-out-of-Many Proofs and Applications -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Technical Overview -- 1.3 Roadmap -- 2 Preliminaries -- 2.1 Hard Problems -- 2.2 Merkle Trees -- 2.3 Seedtrees -- 3 Short One-out-of-Many Proofs from Coding Theory -- 3.1 The SD-Based One-out-of-Many Proof -- 3.2 The GSD-Based One-out-of-Many Proof -- 3.3 Our Set-Membership Proof -- 4 Our Code-Based Logarithmic-Size Ring Signature Scheme -- 5 Code-Based Group Signatures -- 5.1 The Underlying Protocol of Our Group Signature -- 5.2 Our Code-Base Logarithmic-Size Group Signature Scheme -- 6 Concrete Instantiation -- References -- Efficient KZG-Based Univariate Sum-Check and Lookup Argument -- 1 Introduction -- 1.1 Contributions -- 1.2 Technical Overview -- 1.3 Related Works -- 2 Preliminaries -- 2.1 Bilinear Pairing -- 2.2 The KZG Polynomial Commitment -- 2.3 Polynomials and Lagrange Basis -- 2.4 Algebraic Group Model -- 2.5 Argument of Knowledge -- 3 Losum: Optimal Sum-Check for KZG -- 3.1 Overview -- 3.2 Protocol Description -- 3.3 Security and Efficiency Analysis -- 4 Locq: Improved Lookup Argument -- 4.1 Overview -- 4.2 Protocol Description -- 4.3 Security and Efficiency Analysis -- 5 Conclusion -- References.
On Sigma-Protocols and (Packed) Black-Box Secret Sharing Schemes.

Sommario/riassunto

The four-volume proceedings set LNCS 14601-14604 constitutes the refereed proceedings of the 27th IACR International Conference on Practice and Theory of Public Key Cryptography, PKC 2024, held in Sydney, NSW, Australia, April 15–17, 2024. The 54 papers included in these proceedings were carefully reviewed and selected from 176 submissions. They focus on all aspects of signatures; attacks; commitments; multiparty computation; zero knowledge proofs; theoretical foundations; isogenies and applications; lattices and applications; Diffie Hellman and applications; encryption; homomorphic encryption; and implementation.