1. Record Nr. UNISA996574258103316

Titolo	Advances in Cryptology - ASIACRYPT 2023 : 29th International Conference on the Theory and Application of Cryptology and Information Security, Guangzhou, China, December 4-8, 2023, Proceedings, Part II / / Jian Guo and Ron Steinfeld, editors
Pubbl/distr/stampa	Singapore : , : Springer, , [2023] ©2023
ISBN	981-9987-24-5
Edizione	[First edition.]
Descrizione fisica	1 online resource (504 pages)
Collana	Lecture Notes in Computer Science Series ; ; Volume 14439
Disciplina	005.8
Soggetti	Computer security 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 II -- Proof Systems - Succinctness and Foundations -- Fiat-Shamir Security of FRI and Related SNARKs -- 1 Introduction -- 1.1 Our Results -- 1.2 Technical Details -- 1.3 Additional Related Work -- 1.4 Organization -- 2 Technical Overview -- 2.1 Round-by-Round Soundness and Fiat-Shamir -- 2.2 Round-by-Round Soundness of FRI -- 2.3 Correlated IOPs and Round-by-Round Knowledge Soundness -- 2.4 Round-by-Round Knowledge of Plonk-Like Protocols -- 2.5 Round-by-Round Knowledge of EthSTARK -- 2.6 From Round-by-Round Soundness to Fiat-Shamir Security -- 3 Our Results -- 3.1 Round-by-Round Soundness of FRI and Batched FRI -- 3.2 Correlated IOPs -- 3.3 A Plonk-Like Protocol Abstraction OPlonky -- 4 Conclusions and Open Problems -- References -- On Black-Box Knowledge-Sound Commit-And-Prove SNARKs -- 1 Introduction -- 2 Technical Overview -- 2.1 Background -- 2.2 FANA Is Not Sound -- 2.3 Semi-adaptive Black-Box Knowledge-Soundness -- 2.4 New SNARK -- 2.5 Fully Algebraic F-Position-Binding Vector Commitment -- 2.6 Efficiency -- 3 Preliminaries -- 3.1 Underlying Commitment Schemes -- 3.2 QA-NIZK

-- 4 New Vector Commitment Scheme -- 4.1 Definitions -- 4.2 Construction -- 4.3 Security Analysis -- 4.4 Committing to Linear Maps -- 5 New C&amp -- P Zk-SNARK Security Notions -- 5.1 R1CS and R1CSf -- 5.2 Security Definitions -- 6 New C&amp -- P SA-SNARK Punic -- 6.1 Intuition -- 6.2 Description of Punic -- 7 Security of Punic -- 7.1 Semi-adaptive Computational (n, G)-Special-Soundness -- References -- Protostar: Generic Efficient Accumulation/Folding for Special-Sound Protocols -- 1 Introduction -- 1.1 Technical Overview -- 2 Preliminaries -- 2.1 Incremental Verifiable Computation (IVC) -- 2.2 Simple Accumulation -- 3 Protocols -- 3.1 Special-Sound Protocols and Their Basic Transformations.
3.2 Accumulation Scheme for Vnark -- 3.3 Compressing Verification Checks for High-Degree Verifiers -- 3.4 Computation of Error Terms -- 4 Special-Sound Subprotocols for ProtoStar -- 4.1 Permutation Relation -- 4.2 High-Degree Custom Gate Relation -- 4.3 Lookup Relation -- 4.4 Circuit Selection -- 5 Protostar -- References -- Polynomial IOPs for Memory Consistency Checks in Zero-Knowledge Virtual Machines -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Technical Overview -- 1.3 Related Works -- 2 Preliminaries -- 2.1 Vectors and Polynomials -- 2.2 Interactive Proof System -- 2.3 Polynomial IOP -- 2.4 PIOP for Vector Languages -- 2.5 Building Blocks -- 3 The Memory Consistency Check Problem -- 4 The Sorting Paradigm -- 4.1 Contiguous Read-Only Memory -- 4.2 Read-Write Memory with 32-Bit Addresses -- 4.3 Read-Write Memory with the Full Address Space -- 5 Permem: New Construction with the Full Address Space -- 5.1 Address Cycle Method and Permem -- 5.2 Grand-Sum-Based Lookup Argument -- 6 Efficiency Analysis -- 7 Conclusion -- References -- Weak Zero-Knowledge via the Goldreich-Levin Theorem -- 1 Introduction -- 2 Our Techniques -- 3 Preliminaries -- 3.1 Goldreich-Levin List Decoding -- 3.2 Building Blocks -- 3.3 Proof Systems -- 4 Construction -- 5 Proof of Security -- 5.1 Simulator -- 5.2 Proof of Theorem 2 -- 5.3 Argument of Knowledge Property -- References -- A Simple and Efficient Framework of Proof Systems for NP -- 1 Introduction -- 1.1 Motivation -- 1.2 Our Contributions -- 1.3 Technical Overview -- 2 Preliminaries -- 2.1 Pairing Groups and Matrix Diffie-Hellman Assumptions -- 2.2 Non-Interactive Zero-Knowledge Proof -- 2.3 Batch Argument -- 3 Simple NIZK from OR-Proof -- 3.1 NIZK for OR-Language -- 3.2 Our NIZK for NP -- 4 Batch Argument for NP -- 5 Experimental Performance -- A GOS-NIZK in the Asymmetric Pairing Setting -- References.
Sigma Protocols from Verifiable Secret Sharing and Their Applications -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Work -- 2 Preliminaries -- 2.1 Commitment Schemes -- 2.2 Sigma Protocols -- 2.3 Secure Multiparty Computation -- 2.4 (Verifiable) Secret Sharing -- 3 A Framework of Sigma Protocols from VSS -- 3.1 A Refined Definition of VSS Schemes -- 3.2 The Framework of Sigma Protocols -- 4 Instantiations of Our Framework -- 4.1 Proof of Knowledge of a Discrete Logarithm -- 4.2 Proof of Knowledge of Several Discrete Logarithms -- 4.3 Proof of Knowledge of a Representation -- 4.4 Proof of Knowledge of An -th Root -- 5 A Framework of ZKPs for Composite Statements -- 5.1 A Generalization of MPC-in-the-Head Paradigm -- 5.2 Separable VSS Schemes -- 5.3 Generic Construction of ZKPs for Composite Statements -- 6 An Instantiation of ZKP for Composite Statements -- 6.1 Review of Ligero++ -- 6.2 A Sigma Protocol for Pedersen Commitments -- 7 Conclusion -- References -- Anonymity -- Anonymous Counting Tokens -- 1 Introduction -- 1.1 Technical Approach -- 1.2 Organization of the Paper -- 2 Preliminaries -- 2.1 Cyclic Groups, Bilinear Groups, and Associated Assumptions -- 2.2

Pseudorandom Function -- 2.3 Camenisch-Shoup Encryption -- 2.4 Non-interactive Zero-Knowledge Argument of Knowledge -- 2.5 Commitment Schemes -- 2.6 Equivalence-Class Signature Schemes (EQS) -- 3 Definitions -- 3.1 Security Properties -- 4 Anonymous Counting Tokens from Oblivious PRF -- 4.1 ACT Construction -- 4.2 Verifiable Oblivious Pseudorandom Function Construction -- 5 ACTs from Equivalence-Class Signature -- 5.1 ACT from EQS and Dodis-Yampolskiy PRF for Small Messages -- 5.2 ACT from EQS and a Random-Oracle-Based PRF -- 6 ACTs in the Generic Bilinear Group Model -- References -- Predicate Aggregate Signatures and Applications -- 1 Introduction -- 1.1 Our Contributions.
2 Preliminary -- 2.1 Assumptions -- 2.2 Cryptographic Primitives -- 3 Predicate Aggregate Signatures -- 3.1 Syntax -- 3.2 Model -- 4 Constructions -- 4.1 Construction Overview -- 4.2 Succinct Proofs with Logarithmic Verifier -- 4.3 Efficient Construction from BLS Signatures -- 5 Analysis -- 5.1 Performance Analysis -- 5.2 Security Analysis -- 6 Applications and Extensions -- 6.1 Extensions -- 6.2 Open Problems -- References -- .26em plus .1em minus .1emBicameral and Auditably Private Signatures -- 1 Introduction -- 2 Bicameral and Auditably Private Signatures -- 2.1 Syntax of BAPS -- 2.2 Correctness and Security of BAPS -- 3 A Generic Construction for BAPS -- 3.1 Technical Overview -- 3.2 Description -- 3.3 Analyses -- 4 A Lattice-Based BAPS Scheme -- 4.1 Technical Overview -- 4.2 Scheme Description -- 4.3 Analyses -- References -- Threshold Structure-Preserving Signatures -- 1 Introduction -- 1.1 Our Contributions -- 2 Related Work -- 3 Preliminaries and Definitions -- 3.1 General -- 3.2 Schemes -- 3.3 Assumptions -- 4 Indexed Message Structure-Preserving Signatures -- 4.1 Definition of Unforgeability for Indexed Message SPS -- 4.2 Our Indexed Message SPS -- 4.3 Security of IM-SPS -- 4.4 Our Indexed Multi-message SPS -- 5 Threshold Structure-Preserving Signatures -- 5.1 Our Indexed Multi-message TSPS -- 5.2 Security of TSPS -- 6 Applications to Threshold-Issuance Anonymous Credentials -- 6.1 Blind Signing for TSPS -- 6.2 Removing Rewinding Extractors in TIAC -- 7 Conclusion and Open Problems -- A Additional Definitions and Assumptions -- A.1 Digital Signatures -- A.2 Commitment Schemes -- A.3 Non-interactive Zero-Knowledge Proofs -- A.4 Threshold Blind Signatures -- References -- Practical Round-Optimal Blind Signatures in the ROM from Standard Assumptions -- 1 Introduction -- 1.1 Background -- 1.2 Contributions -- 1.3 Technical Overview.
2 Preliminaries -- 2.1 Cryptographic Primitives -- 3 Optimizing the Fischlin Blind Signature -- 3.1 Construction -- 3.2 Correctness and Security -- 3.3 Instantiation -- 4 Blind Signatures Based on Boneh-Boyen Signature -- 4.1 Construction -- 4.2 Correctness and Security -- 4.3 Instantiation -- References -- A Generic Construction of an Anonymous Reputation System and Instantiations from Lattices -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Related Work -- 2 Preliminaries -- 2.1 Problems on Lattices -- 2.2 NIZKs -- 3 Linking Indistinguishable Tags -- 4 Reputation System -- 4.1 Security Model -- 4.2 Generic Construction -- 4.3 Security of the Generic Construction -- 5 A Reputation System from Module Lattices -- 5.1 Instantiation with Pairing-Based Cryptography -- References -- Universally Composable Auditable Surveillance -- 1 Introduction -- 1.1 Contribution -- 1.2 Overview of Technical Challenges in Building Applications -- 1.3 Related Work -- 2 System Overview -- 2.1 Parties -- 2.2 High-Level System Overview -- 2.3 Security Properties and Trust Assumptions -- 3 A Formal Model for Auditable Surveillance Systems -- 4 Realizing the Model -- 4.1 A Protocol AS for Realizing FAS -- 4.2 Decrypting Secrets with FAD -- 4.3 A Protocol FAD for Realizing FAD -- 5 Application --

5.1 The Functionality FASTE -- 5.2 The Protocol ASTE -- 5.3 On Efficiency and the Necessity of (NI)NCE -- 5.4 Comparison with ch14EC:GreKapLae21 -- 5.5 Other Applications -- 6 Limitations and Future Work -- References -- Author Index.

Sommario/riassunto

The eight-volume set LNCS 14438 until 14445 constitutes the proceedings of the 29th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2023, held in Guangzhou, China, during December 4-8, 2023. The total of 106 full papers presented in these proceedings was carefully reviewed and selected from 375 submissions. The papers were organized in topical sections as follows: Part I: Secure Multi-party computation; threshold cryptography; . Part II: proof systems - succinctness and foundations; anonymity; Part III: quantum cryptanalysis; symmetric-key cryptanalysis; Part IV: cryptanalysis of post-quantum and public-key systems; side-channels; quantum random oracle model; Part V: functional encryption, commitments and proofs; secure messaging and broadcast; Part VI: homomorphic encryption; encryption with special functionalities; security proofs and security models; Part VII: post-quantum cryptography; Part VIII: quantum cryptography; key exchange; symmetric-key design.