1. Record Nr. UNISA996587860903316

Autore	Ge Chunpeng
Titolo	Information Security and Cryptology : 19th International Conference, Inscrypt 2023, Hangzhou, China, December 9-10, 2023, Revised Selected Papers, Part I
Pubbl/distr/stampa	Singapore : , : Springer, , 2024 ©2024
ISBN	981-9709-42-3
Edizione	[1st ed.]
Descrizione fisica	1 online resource (480 pages)
Collana	Lecture Notes in Computer Science Series ; ; v.14526
Altri autori (Persone)	YungMoti
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- Contents - Part I -- Contents - Part II -- Signature -- TVES: Threshold Verifiably Encrypted Signature and Its Applications -- 1 Introduction -- 1.1 Background -- 1.2 Related Works -- 1.3 Our Contributions -- 1.4 Organization -- 2 Preliminaries -- 2.1 Secret Sharing and Distributed Key Generation (DKG) -- 2.2 Bilinear Pairings -- 2.3 BLS Short Signature Scheme -- 3 Threshold Verifiably Encrypted Signature (TVES) Scheme -- 3.1 Definition -- 3.2 Security Notions -- 4 A Concrete Construction of TVES: TVES-BP from Bilinear Pairings -- 5 Security and Performance Analysis -- 5.1 Validity -- 5.2 Unforgeability -- 5.3 Opacity -- 5.4 Efficiency -- 6 Application -- 7 Conclusion -- References -- Compact Accountable Ring Signatures in the Plain Model -- 1 Introduction -- 1.1 Related Work -- 1.2 Our Contribution -- 1.3 Overview of Our Techniques -- 2 Preliminaries -- 3 Compact Accountable Ring Signatures -- 3.1 Definition and Security Model -- 3.2 Our Compact Accountable Ring Signatures Construction -- 4 Security Proofs -- 4.1 Anonymity -- 4.2 Unforgeability -- 4.3 Tracing Soundness -- 5 Conclusion -- References -- Universally Composable Key-Insulated and Privacy-Preserving Signature Scheme with Publicly Derived Public Key -- 1 Introduction -- 1.1 Our Results -- 1.2 Related Work -- 2 Preliminaries -- 2.1 Notations -- 2.2 PDPKS: Signature Scheme with Publicly Derived Public Key -- 2.3 Universal Composability -- 3 Security Model of PDPKS in UC Framework

-- 4 A UC-Secure PDPKS Construction -- 5 Conclusion -- References -- Compact Ring Signatures with Post-Quantum Security in Standard Model -- 1 Introduction -- 1.1 Literature Review and Motivation -- 1.2 Our Contributions -- 1.3 Technical Overview -- 2 Preliminaries -- 2.1 Quantum Oracle Indistinguishability -- 2.2 Chameleon Hash Functions. 2.3 Somewhere Perfectly Binding Hash Functions -- 2.4 Lossy PKEs -- 2.5 ZAPs -- 3 Blind-Unforgeable Signatures -- 3.1 Security Model -- 3.2 Construction -- 3.3 Security Proof -- 4 Compact Post-Quantum Ring Signatures -- 4.1 Ring Signatures -- 4.2 Security Model -- 4.3 Construction -- 4.4 ZAP Super-Complement Language -- 4.5 Security Proof -- References -- Secure Multi-party SM2 Signature Based on SPDZ Protocol -- 1 Introduction -- 2 Related Work -- 3 Preliminaries -- 3.1 Secure Multi-party Computation -- 3.2 The SPDZ Protocol -- 3.3 SM2 Signature Algorithm -- 3.4 Secret Sharing -- 3.5 Message Authentication Code -- 3.6 Notation -- 4 Models and Functionalities -- 4.1 System Model -- 4.2 Security Model -- 4.3 Communication Model -- 4.4 Functionalities -- 5 Multi-party Signature Protocol -- 5.1 Preprocessing Phase -- 5.2 Signing Phase -- 6 Security Proof -- 7 Performance Evaluation -- 7.1 Experiment Setting -- 7.2 Performance Evaluation -- 8 Conclusion -- References -- Blockchain -- Epoch: Enabling Path Concealing Payment Channel Hubs with Optimal Path Encryption -- 1 Introduction -- 1.1 Related Works -- 1.2 Motivations and Contributions -- 1.3 Roadmap -- 2 Preliminary -- 2.1 Payment Channel Network -- 2.2 Payment Channel Hub -- 2.3 Homomorphic One-Way Functions -- 2.4 Non-interactive Zero-Knowledge Proof -- 2.5 Commitment Scheme -- 2.6 LockDown Attack -- 3 Epoch -- 3.1 Security and Privacy Goals -- 3.2 Our Solution -- 4 Security Analysis -- 4.1 Ideal Functionality FOPE -- 4.2 Security Proof of the OPE Protocol -- 4.3 Discussion -- 5 Performance Analysis -- 6 Conclusion -- References -- A General Federated Learning Scheme with Blockchain on Non-IID Data -- 1 Introduction -- 2 Preliminaries -- 2.1 Differential Privacy -- 2.2 Generative Adversarial Network -- 2.3 Blockchain -- 2.4 Federated Learning -- 3 Proposed GBA-FL Scheme -- 3.1 Overview. 3.2 Non-IID Data Augmentation -- 3.3 Privacy-Preserving Training of GANs -- 3.4 Generators Decentralized Sharing -- 4 Experiments -- 4.1 Network Structure -- 4.2 Datasets and Division Strategies -- 4.3 Model Accuracy Testing -- 5 Conclusion -- References -- A Blockchain-Based Personal Health Record Sharing Scheme with Security and Privacy Preservation -- 1 Introduction -- 2 Related Work -- 3 Preliminaries -- 3.1 Complexity Assumptions -- 3.2 Blockchain and Smart Contract -- 3.3 InterPlanetary File System -- 3.4 Attribute-Based Access Control -- 3.5 Proxy Re-encryption -- 4 The Proposed Scheme -- 4.1 System Model -- 4.2 Threat Model and Security Goal -- 4.3 Scheme Construction -- 4.4 Smart Contract Design -- 5 Security Analysis -- 5.1 Data Integrity and Confidentiality -- 5.2 Fine-Grained Access Control -- 5.3 Collusion Resistance -- 5.4 Auditability -- 6 Performance Evaluation -- 6.1 Scheme Comparison -- 6.2 Experimental Setting -- 6.3 Communication Overhead -- 6.4 Computational Overhead -- 6.5 Performance of Smart Contracts -- 7 Conclusion -- References -- Cryptography Primitive -- General Constructions of Fuzzy Extractors for Continuous Sources -- 1 Introduction -- 1.1 Related Work for Continuous-Source Fuzzy Extractors -- 1.2 Our Contributions -- 2 Preliminaries -- 2.1 Min-Entropy, Secure Sketch and Extractor -- 2.2 Lattice and Lattice Code -- 3 New Measure of Unpredictability -- 4 Fuzzy Extractors and Fuzzy Conductors -- 4.1 Fuzzy Extractors for Continuous Sources -- 4.2 Fuzzy Conductors for Continuous Sources -- 4.3 On the Relations Between CS-Fuzzy Extractors and CS-Fuzzy Conductors -- 5

Constructions for Euclidean Distance -- 6 Instantiation -- 7 Conclusion -- References -- Geometry-Based Garbled Circuits Relying Solely on One Evaluation Algorithm Under Standard Assumption -- 1 Introduction -- 1.1 Background -- 1.2 Overview of Our Approach. 1.3 Our Contributions -- 2 Preliminaries -- 3 Our Garbling Scheme in Detail -- 3.1 Notation and Concepts. -- 3.2 Garbling Procedure: Initialization. -- 3.3 Garbling Procedure: Geometry-AND Gates. -- 3.4 Garbling Procedure: Geometry-XOR Gates. -- 3.5 Garbling Procedure: Geometry-NOT Gates. -- 3.6 Algorithms of Proposed Geometry-Based GC -- 4 Performance Analysis -- 5 Proof of Security -- 6 Conclusions -- References -- Full Domain Functional Bootstrapping with Least Significant Bit Encoding -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Related Work -- 1.3 Paper Organization -- 2 Preliminaries -- 2.1 Notation -- 2.2 Learning with Errors -- 2.3 Useful Algorithms -- 3 Full Domain Functional Bootstrapping -- 3.1 RGSW Encryption -- 3.2 LUT Encoding -- 3.3 Bootstrapping Key Generation Algorithm -- 3.4 Full Domain FBS -- 3.5 Full Domain FBS with MSB Encoding -- 4 Multi-value and Tree-Based Functional Bootstrapping -- 4.1 Multi-value Functional Bootstrapping -- 4.2 Tree-Based Functional Bootstrapping -- 5 Comparative Analysis and Experimental Results -- 5.1 Security Analysis and Parameter Selection -- 5.2 Performance Comparison -- 5.3 Practicability -- 6 Conclusion -- A Algorithms of functions presented in Section2.4 -- A.1 Correctness of the Key Switching -- A.2 Correctness of the Modulus Switching -- A.3 Correctness of the Encoding Transformation -- References -- Public Key Cryptography -- PFE: Linear Active Security, Double-Shuffle Proofs, and Low-Complexity Communication -- 1 Introduction -- 1.1 Secure Multi-party Computation -- 1.2 Motivation and Contributions -- 2 Notations and Definitions -- 3 ZKDS: Double Shuffles Suffice for Correct Extended Permutation -- 3.1 Ideation and Observation -- 3.2 Constructing ZKDS -- 4 General Linear-Complexity PFE Framework with Active Security -- 4.1 Description of the General Actively Secure PFE Framework. 4.2 The Offline Phase -- 4.3 The Online Phase -- 4.4 Proof of Offline Protocol -- 4.5 Proof of Online Protocol -- 5 Conclusions and Future Work -- References -- CCA-Secure Identity-Based Matchmaking Encryption from Standard Assumptions -- 1 Introduction -- 1.1 Technical Overview -- 1.2 Related Works -- 2 Preliminaries -- 2.1 Notations -- 2.2 Dual Vector Pairing Space Generation -- 2.3 (Hierarchical) Identity-Based Encryption -- 3 CCA-Security of IB-ME -- 3.1 Identity-Based Matchmaking Encryption -- 3.2 Privacy of IB-ME Against Chosen-Ciphertext Attacks -- 3.3 Authenticity of IB-ME -- 4 CCA-Secure IBE from 2-Level HIBE -- 4.1 CCA-Secure IBE Construction -- 4.2 Security Analysis -- 5 CCA-Secure IB-ME Construction -- 5.1 Construction -- 5.2 Security Analysis -- References -- Post-Quantum Public-Key Authenticated Searchable Encryption with Forward Security: General Construction, and Applications -- 1 Introduction -- 1.1 Motivation -- 1.2 Our Contributions -- 1.3 Overview of Technique -- 1.4 Related Works -- 1.5 Outline -- 2 Preliminaries -- 2.1 Public-Key Encryption with Keyword Search Scheme -- 2.2 Labelled Public-Key Encryption Scheme -- 2.3 Basic Knowledge of Lattice and Trapdoors -- 3 Syntax and Security Models of FS-PAEKS -- 3.1 Syntax of FS-PAEKS Scheme -- 3.2 Security Models -- 4 Our Proposed Construction -- 5 Security Analysis -- 6 Lattice-Based Instantiation of FS-PAEKS -- 7 Parameters and Correctness -- 7.1 Parameters Setting -- 7.2 Correctness -- 8 Theoretical Comparison -- 9 Potential Applications of FS-PAEKS -- 10 Conclusion -- References -- Public Key Authenticated Encryption with Keyword Search Improved: Strong Security Model and Multi-keyword Construction -- 1 Introduction -- 1.1 Our Contributions

-- 1.2 Related Work -- 1.3 Paper Organization -- 2 Preliminaries --
2.1 Bilinear Pairing -- 2.2 0/1-Encoding.
2.3 CDH Assumption ch15boyen2008uber.