1. Record Nr. UNINA9910508454703321

Titolo	Provable and practical security : 15th international conference, ProvSec 2021, Guangzhou, China, November 5-8, 2021, proceedings / / Qiong Huang, Yu Yu, editors
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2021] ©2021
ISBN	3-030-90402-4
Descrizione fisica	1 online resource (397 pages)
Collana	Lecture Notes in Computer Science ; ; 13059
Disciplina	005.8
Soggetti	Computer security Computer systems - Access control Cryptography
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- Searchable Encryption -- Public Key Based Searchable Encryption with Fine-Grained Sender Permission Control -- 1 Introduction -- 1.1 Contribution -- 1.2 Organization -- 2 Related Work -- 3 Preliminaries -- 3.1 Notations -- 3.2 Bilinear Maps -- 3.3 Hardness Assumption -- 3.4 Linear Secret-Sharing Schemes -- 3.5 Public Key Tree (PKTree) -- 4 Definition of SCPEKS -- 4.1 System Model -- 4.2 Definition of Algorithm -- 4.3 Security Model -- 5 Construction of SCPEKS -- 6 Security Proof and Experimental Evaluation -- 6.1 Security Proof -- 6.2 Performance Analysis -- 7 Conclusion -- References -- Improved Security Model for Public-Key Authenticated Encryption with Keyword Search -- 1 Introduction -- 2 Preliminaries -- 2.1 Bilinear Map -- 2.2 Complexity Assumptions -- 2.3 The Syntax of PAEKS -- 3 Improved CI-Security Model of PAEKS -- 3.1 Fully (M)CI-Security Model -- 3.2 TI-Security Model -- 4 Security Analysis of Previous PAEKS Schemes -- 5 New PAEKS Scheme -- 6 Efficiency Evaluation -- 7 Conclusion -- References -- Public Key Encryption with Fuzzy Matching -- 1 Introduction -- 1.1 Related Work -- 1.2 Our Work -- 1.3 Paper Organization -- 2 Preliminaries -- 2.1 Decisional Diffie-Hellman (DDH) Assumption -- 2.2 Symmetric External Diffie-Hellman (SXDH) Assumption -- 2.3 Split

Function -- 2.4 Edit Distance -- 2.5 Similarity Function -- 3 Public Key Encryption with Fuzzy Matching -- 3.1 Definition -- 3.2 Security Threats -- 4 Our PKEFM Scheme -- 5 Improved Construction Supporting Decryption and Wildcards -- 5.1 Decryption Algorithm -- 5.2 Edit Distance with Encrypted Wildcard -- 5.3 An Improved Construction Supporting Wildcards -- 5.4 Security Discussion -- 6 Performance Evaluation -- 7 Applications -- 8 Conclusion -- A Security Models -- B Security Analysis -- B.1 Ciphertext Indistinguishability.
B.2 Unlinkability -- References -- Partitioned Searchable Encryption -- 1 Introduction -- 1.1 Our Results -- 2 Preliminaries -- 2.1 Searchable Encryption -- 2.2 Bloom Filters -- 3 Partitioned Symmetric Searchable Encryption -- 3.1 Dealing with Malicious Users -- 4 PSSE Instantiations from FE and Trapdoor Permutation Using BF -- 4.1 A PSSE Scheme from FE -- 4.2 PSSE from Trapdoor Permutation: PSSE from oo -- 4.3 Dealing with Malicious Users -- 5 Conclusion -- References -- Key Exchange and Zero Knowledge Proof -- Key Exposure Resistant Group Key Agreement Protocol -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Organization -- 2 Related Works -- 3 Preliminaries -- 3.1 Homomorphic Encryption -- 3.2 Secret Sharing Scheme -- 3.3 The Group Key Agreement Protocol -- 3.4 Notations -- 4 The Proposed Protocol -- 4.1 The Basic Protocol -- 4.2 The Enhanced Protocol -- 5 Security and Performance Analyses -- 5.1 Security Analysis -- 5.2 Performance Analysis -- 6 Conclusion -- References -- NIKE from Affine Determinant Programs -- 1 Introduction -- 1.1 Prior Work on NIKE -- 1.2 Our Result and Techniques -- 2 Background -- 2.1 Randomized Encodings -- 2.2 Multi-party Non-interactive Key-Exchange -- 2.3 Affine Determinant Programs -- 3 Warm-Up: ADP from Randomized Encodings -- 3.1 Randomized Encodings via Branching Programs -- 3.2 Augmenting NC1 Branching Programs for Keyed Functions -- 3.3 ADPs for Keyed Functions from RE -- 4 Multi-party NIKE via ADP -- 4.1 Our NIKE Scheme -- 4.2 Security from IND-Secure ADP -- 5 Sufficiency Conditions for IND-Secure ADP -- 5.1 Admissible Classes of Functions for Matrix-Based ADPs -- 5.2 Our Claim -- References -- OrBit: OR-Proof Identity-Based Identification with Tight Security for (as Low As) 1-Bit Loss -- 1 Identity-Based Identification -- 2 Intuitive View of IBI IMP-CA Security Reduction -- 3 Preliminaries.
3.1 Security Model -- 3.2 Security Assumptions -- 3.3 Homomorphic Trapdoor Sampleable Relations, Honest Verifier Zero Knowledge and 1-2 Oblivious Transfer Protocols -- 4 OB1: IMP-CA IBI Schemes from OR-Proof and HTSR -- 4.1 Application of the Framework -- 4.2 Improving the Security of BLS-IBI -- 4.3 Comparison with Existing IBI Frameworks for IMP-CA Security -- 5 OB2: Tight IMP-CA IBI Scheme from OR-Proof and 1-2 OT -- 5.1 Comparison with Existing Schnorr-Based IBI Schemes -- 6 Conclusion -- References -- Card-Based Zero-Knowledge Proof Protocols for Graph Problems and Their Computational Model -- 1 Introduction -- 1.1 Existing Physical ZKP Protocols -- 1.2 Contribution -- 2 Preliminaries -- 2.1 A Deck of Cards -- 2.2 Pile-Scramble Shuffle -- 2.3 Known Physical Protocol for 3-Coloring Problem ch8Goldreich91 -- 2.4 Graph Isomorphism Problem -- 3 Card-Based ZKP for 3-Coloring Problem -- 4 Card-Based ZKP for Graph Isomorphism Problem -- 4.1 Idea -- 4.2 Description -- 5 Basic Formalization of Card-Based ZKP Protocols -- 5.1 Witness Subsequence -- 5.2 Input to Protocol -- 5.3 Abstract Protocol for ZKP -- 5.4 Properties of ZKP -- 6 Proof of ZKP Properties for Our Protocols -- 6.1 3-Coloring Problem -- 6.2 Graph Isomorphism Problem -- 7 Conclusion -- References -- Post Quantum Cryptography -- Recovery

Attack on Bob's Reused Randomness in CRYSTALS-KYBER and SABER -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Works -- 1.3 Roadmap -- 2 Preliminary -- 2.1 Mathematical Notations -- 2.2 CRYSTALS-KYBER ch9BDKLLSSSS18 -- 2.3 SABER ch9DKRV18 -- 2.4 Wang et al.'s Proposition -- 3 Our Proposed Attack -- 3.1 General Attack Model -- 3.2 Key Reuse Attack on CRYSTALS-KYBER -- 3.3 Key Reuse Attack on SABER -- 4 Experiments -- 5 Conclusion and Discussion -- A Plots of Experimental Results -- References -- A Lattice Reduction Algorithm Based on Sublattice BKZ.
1 Introduction -- 1.1 Background -- 1.2 Related Work -- 1.3 Our Contribution -- 1.4 Outline -- 2 Preliminaries -- 2.1 Lattice -- 2.2 Lattice Reduction Algorithms -- 3 Sublattice Reduction -- 3.1 Determinant of Sublattice -- 3.2 Basis Reduction on Sublattice -- 4 m-SubBKZ Reduction -- 4.1 Basic Algorithm -- 4.2 A Practical SubBKZ Variant -- 5 Implementation and Experiment -- 5.1 Implementation Details -- 5.2 Experimental Results -- 6 Conclusion -- References -- On the (M)iNTRU Assumption in the Integer Case -- 1 Introduction -- 1.1 Contribution 1: Breaking the Integer iNTRU Assumption -- 1.2 Contribution 2: Generalizing the One-Dimensional Attack to the MiNTRU Assumption -- 1.3 Disclaimer 1 -- 1.4 Disclaimer 2 -- 1.5 Paper Organization -- 2 Preliminaries -- 2.1 Notations -- 2.2 Lattice Preliminaries -- 3 The iNTRU Assumption -- 3.1 The iNTRU Assumption -- 3.2 Further Remarks -- 3.3 Applications -- 3.4 Our Contribution -- 4 Attacking the iNTRU Assumption - First Approach -- 4.1 Our First Lattice and Its Properties -- 4.2 Case of a Random Tuple -- 4.3 Case of a Synthetic Tuple -- 4.4 Conclusion -- 5 Attacking the iNTRU Assumption - Second Approach -- 5.1 Our Second Lattice and Its Properties -- 5.2 Case of a Random Tuple -- 5.3 Case of a Synthetic Tuple -- 5.4 Conclusion -- 6 Generalizing Our Attacks -- 6.1 iNTRU - The General Case -- 6.2 MiNTRU -- 7 Conclusion -- A Proof of Lemma 1 -- References -- Functional Encryption -- Verifiable Functional Encryption Using Intel SGX -- 1 Introduction -- 2 Preliminaries -- 3 Impossibility Result of VFE -- 4 Definitions of VFE-HW -- 5 Proposed Scheme -- 6 Security Analysis -- 6.1 Weak Verifiability -- 6.2 Simulation Security -- 7 Implementation -- 8 Conclusion -- A The Nieto et al. VPKE Scheme -- References -- Fully Secure Unbounded Zero Inner Product Encryption with Short Ciphertexts and Keys -- 1 Introduction.
2 Preliminaries -- 2.1 Basic Notions -- 3 Our UZIPE -- 3.1 Security -- 4 Conclusion -- References -- Inner-Product Functional Encryption from Random Linear Codes: Trial and Challenges -- 1 Introduction -- 2 Preliminaries -- 2.1 Notation and Conventions -- 2.2 Linear Codes -- 2.3 Hard Problems in Coding Theory -- 3 Functional Encryption -- 4 The Basic Idea of Constructing Inner-Product Encryption Scheme -- 4.1 Basic-IPFEc Scheme -- 4.2 Security Analysis -- 5 The Full Scheme -- 5.1 The Presentation of the Full Scheme -- 5.2 Correctness -- 5.3 Security -- 6 Conclusion -- References -- Digital Signature -- A CCA-Full-Anonymous Group Signature with Verifiable Controllable Linkability in the Standard Model -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Work -- 1.3 Comparison -- 2 Preliminaries -- 2.1 Mathematical Preliminaries -- 2.2 Sign-Encrypt-Proof Paradigm and Efficient Non-interactive Proofs for Bilinear Groups -- 3 Group Signatures with Verifiable Controllable Linkability -- 4 Structure Preserving Public Key Encryption with Equality Test -- 4.1 Definition -- 4.2 Security Models for SP-PKEET -- 4.3 Construction -- 5 A CCA-Full-Anonymous Group Signature with Verifiable Controllable Linkability -- 5.1 Adding the VCL Property -- 5.2 Making Use of SP-PKEET -- 5.3 Our Concrete Instantiation -- 5.4 Security Analysis -- 6

Conclusion -- References -- Cryptanalysis of LRainbow: The Lifted Rainbow Signature Scheme -- 1 Introduction -- 1.1 Our Contribution -- 2 Preliminaries -- 2.1 Multivariate Signature Scheme -- 2.2 Hardness Assumption -- 2.3 Rainbow Signature Scheme ch16ding2005rainbow -- 2.4 LRainbow: Lifting the Field for Rainbow ch16lr -- 3 Proposed Attack on LRainbow -- 3.1 General Idea of the Attack: A High Level Overview -- 3.2 Existence of Small Subfields L2 -- 3.3 Method of Finding w and Forging the Signature -- 4 Complexity of the Attack.
4.1 Preliminaries: Approach by Thomae and Wolf ch16Thomae2012SolvingUS.