1. Record Nr. UNISA996503470903316

Titolo	Information security : 25th International Conference, ISC 2022, Bali, Indonesia, December 18-22, 2022 : proceedings / / Willy Susilo [and four others]
Pubbl/distr/stampa	Cham, Switzerland : , : Springer International Publishing, , [2022] ©2022
ISBN	3-031-22390-X
Descrizione fisica	1 online resource (522 pages)
Collana	Lecture Notes in Computer Science Ser. ; ; v.13640
Disciplina	005.8
Soggetti	Computer networks - Security measures Computer networks - Security measures - Automation
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- Keynote and Invited Talks -- Efficiently Deployable and Efficiently Searchable Encryption (EDESE) - Applications, Attacks, and Countermeasures -- Software Vulnerability Detection by Fuzzing and Deep Learning -- Cybersecurity Policies and Challenges in Indonesia -- Blockchain Security: Primitives and Protocols -- Covert Communication: Past, Present and Future -- Contents -- Cryptography -- Privacy Preserving Computation in Cloud Using Reusable Garbled Oblivious RAMs -- 1 Introduction -- 2 Cloud Data Storage and Oblivious RAMs -- 3 Reusable Garbled ORAMs -- 3.1 Constrained Peseudo Random Functions -- 3.2 Garbled Circuits (GC) -- 3.3 Indistinguishability Obfuscation and Reusable Garbled Circuits -- 3.4 Construction of Reusable Garbled ORAMs -- 3.5 Proof of Security -- 4 Conclusion -- References -- Efficient Private Set Intersection Cardinality Protocol in the Reverse Unbalanced Setting -- 1 Introduction -- 2 Related Work -- 3 Preliminaries -- 3.1 Notations -- 3.2 Cuckoo Filter -- 3.3 Commutative Encryption -- 3.4 Hash-Prefix Filter -- 3.5 The Semi-honest Model -- 4 Our Proposal -- 5 Security Analysis -- 6 Performance Evaluation -- 6.1 Complexity Analysis -- 6.2 Environment and Parameters -- 6.3 Overhead Analysis -- 6.4 Feasibility Analysis of Anonymous Identity Authentication -- 7 Conclusions -- References -- Crypto-Steganographic Validity for

Additive Manufacturing (3D Printing) Design Files -- 1 Introduction -- 2 Background -- 3 Definitions: Watermarking for AM -- 4 Steganographic Channels in STL File Format -- 4.1 STL Transformations for Bit Encoding -- 4.2 Steganographic Channels in STL File Format -- 5 Validity: STL Watermarking and Fingerprinting -- 6 Defining and Verifying Semantic Preservation for AM -- 6.1 Verifying G-Code Toolpath-Based Semantic Preservation.
6.2 Verification of Form- And Fit-Based Semantic Preservation -- 7 Conclusion -- References -- Witness Encryption from Smooth Projective Hashing System -- 1 Introduction -- 2 Related Work -- 3 Preliminaries -- 3.1 Notations and Conventions -- 3.2 Non-Interactive Zero-Knowledge Arguments of Knowledge -- 3.3 Smooth Projective Hashing Functions -- 3.4 Symmetric Key Encryption -- 4 Witness Encryption over Smooth Projective Hashing -- 4.1 Definition -- 4.2 Our Construction 1 -- 4.3 Correctness -- 4.4 Security Proof -- 5 Instantiating of SPHFfrom SNARK -- 5.1 Tools -- 5.2 Our Construction 2: SPHFfor SNARK -- 5.3 Correctness and Security of SPHF -- 6 Discussion -- 7 Conclusion -- References -- Post-quantum Cryptography -- More Efficient Adaptively Secure Lattice-Based IBE with Equality Test in the Standard Model -- 1 Introduction -- 1.1 Our Contribution -- 2 Identity-Based Encryption with Equality Test -- 3 Construction -- 3.1 ABB-Type Identity-Based Encryption -- 3.2 Constructions of IBEET Schemes from ABB-Type IBE -- References -- QUIC Protocol with Post-quantum Authentication -- 1 Introduction -- 2 Background of QUIC and NIST PQC -- 2.1 QUIC Protocol -- 2.2 NIST PQC Ciphers -- 3 Performance Analysis -- 3.1 Implementation and Experimentation -- 3.2 QUIC and TCP/TLS Performance -- 3.3 Performance with Packet Dropping (D) -- 4 Related Work -- 5 Conclusion -- References -- Batched Fully Homomorphic Encryption from TFHE -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Work -- 1.3 Roadmap -- 2 Preliminaries -- 2.1 Background on TFHE -- 2.2 Number Theoretic Transform -- 2.3 Homomorphic Evalutation of Automorphisms -- 3 Building Blocks -- 3.1 Key Switching on TLWE Ciphertexts -- 3.2 Binary Packing Tree -- 3.3 Homomorphic Ring Decryption -- 4 Batched FHE from TFHE -- 4.1 The Construction -- 4.2 Analysis -- 4.3 Comparisons -- 5 Performance Evaluation.
6 Conclusion -- References -- Implicit Rejection in Fujisaki-Okamoto: Framework and a Novel Realization -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Technical Overview -- 1.3 A New Realization for Our Framework -- 1.4 Related Works -- 1.5 Paper Organization -- 2 Preliminaries -- 2.1 Public-Key Encryption -- 2.2 Key Encapsulation Mechanism -- 2.3 Quantum Random Oracle Model -- 3 Our Framework -- 3.1 Transformation T: From IND-CPA to OW-qPCA -- 3.2 Our Framework for Implicit Rejection -- 3.3 Explanation for FO by Using Our Framework -- 4 Our New Realization -- 5 Conclusions -- References -- Cryptanalysis -- Further Cryptanalysis of a Type of RSA Variants -- 1 Introduction -- 1.1 Background -- 1.2 Our Contributions -- 1.3 Organization -- 2 Preliminaries -- 3 Multiple Private Keys Attack -- 4 Partial Key Exposure Attack -- 5 Small Prime Difference Attack -- 6 Experimental Results -- 7 Conclusion -- References -- The SAT-Based Automatic Searching and Experimental Verification for Differential Characteristics with Application to Midori64 -- 1 Introduction -- 2 A Brief Description of Midori64 -- 3 The Method Proposed by Sun et al. with Application to Midori64 -- 4 Verifying the Validity of Differential Characteristics Based on SAT -- 5 Our New Algorithm for Finding Valid Differential Characteristics -- 6 Conclusion and Future Work -- References -- Efficient Scalar Multiplication on Koblitz Curves with Pre-computation -- 1 Introduction -- 2 Preliminary

-- 2.1 Double Bases -- 2.2 Koblitz Curves -- 2.3 The Width- -NAF -- 2.4 Curve Operations' Costs on Koblitz Curves -- 3 DBNS Recoding and Scalar Multiplication -- 3.1 Theoretical Background -- 3.2 Our New Recoding Algorithms -- 4 Costs of Scalar Multiplications -- 4.1 Scalar Multiplications on 4-Koblitz Curves -- 4.2 Comparison with Other Methods -- 5 Conclusion.
A Scalar Multiplications Using LD Coordinates -- References -- Blockchain -- Efficient ECDSA-Based Adaptor Signature for Batched Atomic Swaps -- 1 Introduction -- 1.1 Our Contributions -- 2 Preliminaries -- 2.1 Notations -- 2.2 Hard Relation and Zero-Knowledge Proof -- 2.3 Adaptor Signature Scheme -- 2.4 ECDSA -- 3 ECDSA-Based Adaptor Signature -- 4 Fast ECDSA-Based Adaptor Signature Schemes with Offline/Online Pre-signing -- 5 Performance and Experimental Results -- 5.1 Theoretical Analysis -- 5.2 Experimental Analysis -- 6 Application -- 6.1 Verification Scenario -- 6.2 Batched Atomic Swaps -- 7 Conclusion -- References -- Searching for Encrypted Data on Blockchain: An Efficient, Secure and Fair Realization -- 1 Introduction -- 2 Overview -- 2.1 System Model -- 2.2 Threat Model -- 2.3 Append-Only Block Store -- 2.4 ABS-Based Lookup Table -- 2.5 ABS-Based Publicly Verifiable Searchable Symmetric Encryption -- 2.6 Cryptographic Primitives -- 3 The Proposed Constructions -- 3.1 B' Tree: An Implementation of the ABS-Based Lookup Table -- 3.2 ABSPVSSE Construction -- 3.3 fair Construction -- 4 Security Analysis -- 4.1 Confidentiality -- 4.2 Soundness -- 4.3 Fairness -- 5 Implementation and Experimental Results -- 5.1 Implementation Details -- 5.2 Performance Evaluation -- 6 Conclusion -- References -- GRUZ: Practical Resource Fair Exchange Without Blockchain -- 1 Introduction -- 2 Preliminaries -- 2.1 Relation and Language -- 2.2 Zero-Knowledge Proof -- 2.3 Garbling Scheme -- 2.4 Garbled Circuits and Elliptic Curves Group -- 2.5 Symmetric Encryption -- 2.6 Commitment -- 2.7 ECDSA -- 3 Construction -- 3.1 Intuitions -- 3.2 Zero-Knowledge Verification of ECDSA -- 3.3 Free-XOR on Elliptic Curves Group -- 3.4 Protocol Description -- 3.5 Security Analysis -- 4 Implementation and Experimental Results -- 5 Conclusion and Future Directions -- References.
Daric: A Storage Efficient Payment Channel with Punishment Mechanism -- 1 Introduction -- 1.1 Contributions -- 1.2 Related Works -- 2 Background and Notations -- 2.1 Outputs and Transactions -- 2.2 Payment Channel -- 3 Solution Overview -- 4 Protocol Description -- 4.1 Create -- 4.2 Update -- 4.3 Close -- 4.4 Punish -- 5 Security Analysis -- 5.1 Notation and Security Model -- 5.2 Ideal Functionality -- 6 Daric Versus Eltoo -- 6.1 HTLC Security -- 6.2 Punishment Mechanism -- 7 Performance Analysis -- A Ideal Functionality -- References -- A Blockchain-Based Mutual Authentication Protocol for Smart Home -- 1 Introduction -- 1.1 Contributions -- 1.2 Organization -- 2 Review of HomeChain -- 3 Cryptanalysis of HomeChain -- 3.1 Linkable Message Attack -- 3.2 Untraceable Signature Attack -- 4 The Enhanced Protocol -- 4.1 Correctness and Security Analysis -- 5 Experiment Analysis -- 6 Conclusions -- References -- Email and Web Security -- OblivSend: Secure and Ephemeral File Sharing Services with Oblivious Expiration Control -- 1 Introduction -- 1.1 Motivation -- 1.2 Our Contributions -- 2 Related Work -- 2.1 Existing Secure File Sharing Services -- 2.2 Privacy-Preserving Web Services -- 3 Preliminaries -- 4 System Overview -- 4.1 Intuition -- 4.2 Framework -- 4.3 Threat Models and Security Goals -- 5 Detailed Construction -- 5.1 Security Guarantee -- 6 Implementation and Evaluation -- 6.1 Implementation -- 6.2 Evaluation -- 7 Conclusion -- References -- EarlyCrow: Detecting APT Malware Command and Control over HTTP(S) Using

Contextual Summaries -- 1 Introduction -- 2 Threat Model -- 2.1 TTP Relevant Data -- 2.2 Measurements -- 3 EarlyCrow -- 3.1 Architecture Overview -- 3.2 PairFlow -- 3.3 PairFlow Features -- 3.4 Profiles Features -- 3.5 ContextualSummary -- 3.6 ContextualSummary Updating Process -- 4 Evaluation -- 4.1 Datasets. 4.2 Classification Performance.