1. Record Nr. UNINA9910616395803321

Titolo	Cyberspace safety and security : 14th International Symposium, CSS 2022, Xi'an, China, October 16-18, 2022, Proceedings / / edited by Xiaofeng Chen, Jian Shen, and Willy Susilo
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2022] ©2022
ISBN	3-031-18067-4
Descrizione fisica	1 online resource (381 pages)
Collana	Lecture Notes in Computer Science ; ; v.13547
Disciplina	016.391
Soggetti	Data encryption (Computer science) Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- Cryptography and Its Applications -- Publicly Verifiable Conjunctive Keyword Search with Balanced Verification Overhead -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Related Work -- 2 Preliminaries -- 2.1 RSA Group -- 2.2 RSA Accumulator -- 2.3 Hardness Assumptions -- 2.4 Security Definitions -- 3 Publicly Verifiable SSE Based on Accumulator -- 4 Security Analysis -- 5 Performance Analysis -- 6 Conclusion -- References -- A Secure and Efficient Certificateless Authenticated Key Agreement Scheme for Smart Healthcare -- 1 Introduction -- 2 Security Model -- 3 Review and Cryptanalysis of WHX AKA Protocol -- 3.1 Review of WHX AKA Protocol -- 3.2 Cryptanalysis of WHX AKA Protocol -- 4 The Improved Scheme -- 4.1 Initialization Phase -- 4.2 Registration Phase -- 4.3 Authentication and Key Agreement Phase -- 5 Security Analysis of the Proposed Scheme -- 6 Performance Analysis -- 6.1 Security Comparison -- 6.2 Computation Cost -- 6.3 Communication Cost -- 7 Conclusion -- References -- Digital Signature Scheme to Match Generalized Reed-Solomon Code over GF(q) -- 1 Introduction -- 2 Preliminary -- 2.1 Public Key Cryptosystem Based on Error Correction Codes -- 2.2 Digital Signature Scheme Based on Error Correction Code -- 2.3 Security Concept -- 3 The Proposed Scheme -- 3.1 Reductionist Security Proof -- 4 Performance Analysis of

the Proposed Algorithm -- 4.1 Signature Complexity -- 4.2 Public Key Size -- 4.3 Signature Length -- 5 Security Analysis -- 5.1 Information Set Decoding Attack -- 5.2 Distinguisher Attack -- 6 Result -- 7 Conclusions -- References -- A Collaborative Access Control Scheme Based on Incentive Mechanisms -- 1 Introduction -- 2 Related Work -- 3 The Proposed Scheme -- 3.1 Setup -- 3.2 KenGey -- 3.3 Encryption -- 3.4 Decryption -- 3.5 Incentive Mechanism of Blockchain -- 4 Analysis.
4.1 Security Analysis -- 4.2 Performance Analysis -- 5 Conclusion -- References -- Quartet: A Logarithmic Size Linkable Ring Signature Scheme from DualRing -- 1 Introduction -- 1.1 Organization -- 2 Preliminaries -- 2.1 Notations -- 2.2 Sum Arguments of Knowledge -- 2.3 The DL-Based DualRing Signature -- 3 Syntax and Security Model -- 3.1 Syntax of LRS -- 3.2 Security Model -- 4 The Proposed Linkable Ring Signatures -- 4.1 Quartet: a Basic Version -- 4.2 Security Analysis of Quartet -- 4.3 Quartet+: An Improved Version with Logarithmic Size -- 4.4 Security Analysis of Quartet+ -- 5 Evaluation and Analysis -- 5.1 Communication Cost -- 5.2 Computation Cost -- 6 Conclusion -- References -- Updatable Hybrid Encryption Scheme with No-Directional Key Update for Cloud Storage -- 1 Introduction -- 1.1 Our Motivations and Contributions -- 1.2 Related Works -- 2 Preliminaries -- 3 Formal Updatable Hybrid Encryption -- 3.1 Syntax -- 3.2 Instantiation Scheme -- 3.3 Correctness -- 3.4 UP-IND-CCA Security -- 3.5 Evaluation of the Proposed UHE Scheme -- 4 Conclusions -- References -- Data Security -- FDLedger: Dynamic and Efficient Anonymous Audit for Distributed Ledgers -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Work -- 2 Preliminaries -- 2.1 Notation -- 2.2 ElGamal Encryption Variant -- 2.3 Order-Revealing Encryption -- 2.4 Consensus -- 3 System Model -- 3.1 Architecture -- 3.2 Assumptions -- 3.3 Security Goals -- 4 FDLedger Construction -- 4.1 Main Idea -- 4.2 Sparse Prefix Symbol Tree -- 4.3 Our Construction -- 4.4 Discussions and Comparisons -- 5 Security Analysis -- 6 Performance Evaluation -- 6.1 Experiment Setup -- 6.2 Experiment Evaluation -- 7 Conclusion -- References -- A Method of Traceless File Deletion for NTFS File System -- 1 Introduction -- 2 Related Work -- 3 Brief Introduction for NTFS File System.
4 A Method of Traceless Data Deletion for NTFS File System -- 4.1 The Requirements of Traceless Data Deletion -- 4.2 A Traceless Method of Data Deletion for NTFS File System -- 5 Performance Analysis -- 5.1 Experiment Result -- 5.2 Performance Analysis -- 6 Conclusion -- References -- Efficient and Collusion Resistant Multi-party Private Set Intersection Protocols for Large Participants and Small Sets Setting -- 1 Introduction -- 1.1 Contributions -- 2 Related Work -- 2.1 Traditional PSI -- 2.2 Collusion Resisting MP-PSI -- 3 Preliminaries -- 3.1 Diffie-Hellman Key Agreement -- 3.2 Zero Sharing Technique -- 4 Security Model -- 4.1 Functionality -- 4.2 Security Definitions -- 5 Concrete Protocols -- 5.1 System Initialization Step -- 5.2 Key Agreement Step -- 5.3 Zero Sharing Step -- 5.4 Intersection Calculation Step -- 6 Security Analysis -- 6.1 Correctness -- 6.2 Security Proof -- 6.3 Malicious Secure MP-PSI -- 7 Performance and Performance -- 7.1 Complexity Analysis -- 7.2 Experimental Implementation -- 7.3 Experiment Results -- 8 Conclusion -- References -- Multi-user Verifiable Database with Efficient Keyword Search -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Related Work -- 1.3 Organization -- 2 Preliminaries -- 2.1 Mathematical Assumption -- 2.2 Verifiable Database (VDB) -- 3 Multi-user Verifiable Database with Efficient Keyword Search -- 3.1 Framework -- 3.2 High Level Description -- 3.3 A Concrete MUVDB Scheme -- 3.4 Extended Construction: Support

Conjunctive Keyword Search -- 4 Security and Efficiency Analysis -- 4.1 Security -- 4.2 Comparison -- 5 Conclusion -- References -- A Blockchain-Based Collaborative Auditing Scheme for Cloud Storage -- 1 Introduction -- 1.1 Our Contribution -- 2 Public Provable Data Possession Scheme -- 2.1 System Model -- 2.2 Adversary Model and Design Goals -- 2.3 EigenTrust Model -- 2.4 A Concrete Scheme.
3 Security Analysis and Efficiency Analysis -- 3.1 Correctness -- 3.2 Security Analysis -- 4 Performance Evaluation -- 4.1 Functionality Comparisons -- 4.2 Implementation -- 5 Conclusion -- References -- Attack and Defense Techniques -- High Quality Audio Adversarial Examples Without Using Psychoacoustics -- 1 Introduction -- 2 Related Work -- 3 Problem Definition -- 3.1 Threat Model and Assumptions -- 3.2 Evaluation Metrics -- 4 Method -- 4.1 Adversarial Convolution -- 4.2 Regularization -- 4.3 Impulse Response -- 4.4 Two-Stage Generation Process -- 5 Experimental Results -- 5.1 Setup -- 5.2 Regularization -- 5.3 Adversarial Example Generation -- 5.4 Robustness -- 6 Conclusion and Future Work -- References -- Working Mechanism of Eternalblue and Its Application in Ransomworm -- 1 Introduction -- 2 Eternalblue's Working Mechanism in Metasploit -- 2.1 Crafting Original List -- 2.2 Buffer Grooming -- 2.3 Sending the Shellcode -- 3 Code Analysis -- 3.1 Summary of Wannacry's Network Behaviour -- 3.2 Detailed Analysis of Wannacry Network Behaviour -- 4 Conclusion -- References -- Substitution Attacks Against Sigma Protocols -- 1 Introduction -- 2 Preliminaries -- 2.1 Notations and Definitions -- 2.2 Protocols -- 3 ASA Models for Protocols -- 3.1 Subverting Prover -- 3.2 Subverting Verifier -- 4 Mounting ASAs on Protocols -- 4.1 The Biased-Commitment Attack -- 4.2 The Biased-Challenge Attack -- 5 Instantiations of Subvertible Protocols -- 5.1 Schnorr's Identification Protocol -- 5.2 Okamoto's Protocol for Representations -- 6 Conclusion -- References -- A Multi-stage APT Attack Detection Method Based on Sample Enhancement -- 1 Introduction -- 2 Related Work -- 3 Multi-stage APT Attack Detection Method Based on Sample Enhancement -- 3.1 Multi-stage Sample Enhancement -- 3.2 Multi-stage APT Attack Detection -- 4 Experimental Results.
4.1 Environment and Evaluation Metrics -- 4.2 Experimental Results and Analysis -- 5 Conclusion -- References -- VDHGT: A Source Code Vulnerability Detection Method Based on Heterogeneous Graph Transformer -- 1 Introduction -- 2 Overview -- 3 VDHGT Method -- 3.1 Generation of VDRG -- 3.2 Node Embedding -- 3.3 Graph Learning Network and Vulnerability Detection -- 4 Experiment and Result Analysis -- 4.1 Experimental Dataset -- 4.2 Experimental Results and Analysis -- 5 Conclusion -- References -- Anomalous Network Traffic Detection Based on CK Sketch and Machine Learning -- 1 Introduction -- 2 Related Work -- 2.1 Sketch Structure -- 2.2 Sketch Improvement Structure on the Basis of Cuckoo Hash -- 3 Anomalous Network Traffic Detection Solution on the Basis of Machine Learning and CK Sketch -- 3.1 Design of the Anomalous Network Traffic Detection Process -- 3.2 CK Sketch Structure Improvement -- 4 Experience -- 4.1 Experimental Environment and Data Set -- 4.2 Metrics -- 4.3 Experimental Comparison Analysis -- 5 Conclusion -- References -- FedMCS: A Privacy-Preserving Mobile Crowdsensing Defense Scheme -- 1 Introduction -- 2 Related Works -- 3 Problem Formulation -- 3.1 System Model -- 3.2 Threat Model -- 3.3 Design Goals -- 4 Preliminaries -- 4.1 Notations -- 4.2 Poisoning Attack -- 4.3 Paillier Encryption System -- 5 Proposed Scheme -- 5.1 Request Task Publishing -- 5.2 Sensing Gradient Uploading -- 5.3 Model Secure Aggregation -- 6 Safety Certificate -- 7 Performance Evaluation -- 7.1

Experimental Settings -- 7.2 Experiment Results -- 8 Conclusion -- References -- Membership Inference Attacks Against Robust Graph Neural Network -- 1 Introduction -- 2 Related Work -- 2.1 Graph Convolutional Networks -- 2.2 Graph Adversarial Training -- 2.3 Graph Inference Attacks -- 3 Background -- 3.1 Graph Convolutional Network -- 3.2 Graph Membership Inference Attacks.
3.3 Graph Adversarial Training.