1. Record Nr. UNISA996495563803316

Autore	Chen Xiaofeng
Titolo	Security and privacy in social networks and big data : 8th international symposium, SocialSec 2022, Xi'an, China, October 16-18, 2022, proceedings / / Xiaofeng Chen, Xinyi Huang, and Mirosaw Kutyowski
Pubbl/distr/stampa	Singapore : , : Springer, , [2022] ©2022
ISBN	981-19-7242-7
Descrizione fisica	1 online resource (372 pages)
Collana	Communications in Computer and Information Science
Disciplina	005.8
Soggetti	Big data - Security measures Big data - Social aspects
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- Cryptography and its Applications -- Improved (t,n)-Threshold Proxy Signature Scheme -- 1 Introduction -- 2 Briefly Review of Liu's Scheme -- 2.1 Initialization Phase -- 2.2 Proxy Key Generation Phase -- 2.3 Proxy Signature Generation Phase -- 2.4 Proxy Signature Verification Phase -- 3 Analysis of Liu's Scheme -- 3.1 Equation Error -- 3.2 Forgery Attack -- 3.3 No Anonymity -- 4 Improved Scheme -- 4.1 System Initialization -- 4.2 Proxy Share and Key Generation -- 4.3 Proxy Signature Generation -- 4.4 Proxy Signature Verification -- 5 Analysis of Improvement Scheme -- 5.1 Scheme Correctness -- 5.2 Scheme Security -- 5.3 Scheme Performance -- 6 Conclusions -- References -- Algorithm Substitution Attacks on Identity-Based Encryption -- 1 Introduction -- 1.1 Algorithm Substitution Attack -- 1.2 Identity-Based Encryption -- 1.3 Our Work -- 2 Preliminaries -- 3 ASA Model of IBE Scheme -- 3.1 Subverting Key Extraction Algorithm -- 3.2 Subverting Encryption Algorithm -- 4 Instantiations -- 4.1 ASA on Waters-IBE Scheme -- 4.2 ASA on BB-IBE Scheme -- 5 Conclusion -- References -- Authenticated Continuous Top-k Spatial Keyword Search on Dynamic Objects -- 1 Introduction -- 2 Related Work -- 2.1 Static Query Authentication -- 2.2 Moving Query Authentication -- 3 Preliminaries -- 3.1 Similarity Measurement -- 3.2 Safe Zone -- 3.3

Authentication Techniques -- 4 Problem Formulation -- 4.1 System Model -- 4.2 Threat Model -- 4.3 Problem Definition -- 4.4 Design Goals -- 5 Proposed Solution -- 5.1 Overview -- 5.2 Authenticated Continuous Top-k Spatial Keyword Search on Dynamic Objects Schemes -- 6 Security Analysis -- 7 Performance Evaluation -- 8 Conclusion -- References -- Efficient Attribute-Based Proxy Re-encryption for Secure Deduplication -- 1 Introduction -- 1.1 Contributions.
2 System Model and Security Model -- 2.1 System Model -- 2.2 Security Model -- 3 The Formal of Definition of the Basic Scheme -- 3.1 Algorithm Definition -- 3.2 The Constructions of the Basic Scheme -- 4 The Formal of Definition of the Improved Scheme -- 4.1 System Model -- 4.2 Algorithm Definition -- 5 The Constructions of the Improved Scheme -- 6 Secure Analysis -- 7 Performance Analysis and Evaluation -- 7.1 Performance Analysis -- 7.2 Performance Evaluation -- 8 Conclusion -- References -- A Secure Word Vector Training Scheme Based on Inner-Product Functional Encryption -- 1 Introduction -- 2 Problem Statement -- 2.1 Backgrounds -- 3 Our Proposed Secure Word Training Protocol -- 3.1 Initialization -- 3.2 Privacy-Preserving Training Protocol -- 4 Theoretical Analysis -- 4.1 Security Analysis -- 4.2 Performance -- 5 Experimental Analysis -- 5.1 Accuracy -- 5.2 Efficiency -- 6 Conclusion and Future Work -- References -- D2D Authentication Scheme for IoT-enabled Smart Home -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Work -- 2 Preliminaries -- 2.1 Bilinear Pairing -- 2.2 Complexity Assumption -- 3 System and Security Models -- 3.1 System Model -- 3.2 Security Model -- 4 Main Idea -- 4.1 Overview -- 4.2 Registration Phase -- 4.3 Authentication Phase -- 4.4 Session Key Generation Phase -- 5 Security Analysis -- 5.1 Correctness -- 5.2 Security -- 6 Performance Analysis -- 7 Conclusion -- References -- Inner Product Encryption from Middle-Product Learning with Errors -- 1 Introduction -- 1.1 Background -- 1.2 Our Contributions -- 2 Preliminaries -- 2.1 Notations -- 2.2 Discrete Gaussian Distribution -- 2.3 MP-LWE -- 2.4 Leftover Hash Lemma -- 2.5 Inner Product Encryption -- 3 Public-Key Encryption from MP-LWE -- 3.1 The Correctness and Security -- 3.2 Linear Homomorphism -- 4 Sel-IND-CPA-Secure Inner Product Encryption -- 5 Conclusion.
A Appendix -- A.1 Proof of Theorem 2 -- References -- Network Security and Privacy Protection -- Publicly Verifiable Private Set Intersection from Homomorphic Encryption -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Technical Overview -- 1.3 Related Work -- 1.4 Roadmap -- 2 Preliminaries -- 2.1 Fully Homomorphic Encryption -- 2.2 Publicly Verifiable Computation -- 2.3 Fiore et al.'s Homomorphic Hash Function -- 2.4 Security in the Presence of Malicious Adversaries -- 3 Publicly Verifiable Inner Product Computation on Encrypted Data -- 3.1 Fiore et al.'s Hash Function for RNS Representation -- 3.2 Publicly Verifiable Inner Product Computation -- 4 Publicly Verifiable PSI from Homomorphic Encryption -- 4.1 The Full Construction -- 4.2 Security Analysis -- 4.3 Efficiency Analysis -- 5 Performance Evaluation -- 6 Conclusions -- A Fiore et al.'s Hash Function for RNS Representation -- References -- Secure Asynchronous Federated Learning for Edge Computing Devices -- 1 Introduction -- 2 Framework -- 2.1 System Environment -- 2.2 Aggregation -- 3 Performance Evaluation -- 3.1 Performance of Asynchronous Training -- 3.2 Performance of WASecAgg -- 4 Security Analysis -- 5 Conclusion -- References -- FedBC: An Efficient and Privacy-Preserving Federated Consensus 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 Practical Byzantine Fault Tolerance (PBFT) -- 4.3 DBSCAN Algorithm -- 5 Proposed Scheme -- 5.1 System Initialization -- 5.2 Model Security Consensus -- 6 Security Analysis -- 7 Performance Evaluation -- 7.1 Experiment Setup -- 7.2 Experiment Results -- 8 Conclusion -- References -- A Secure and Privacy-Preserving Authentication Scheme in IoMT -- 1 Introduction -- 2 Related Work -- 3 System and Security -- 3.1 System Architecture.
4 Our Proposed Scheme -- 4.1 Initialization Phase -- 4.2 Registration Phase -- 4.3 Update Key Phase -- 4.4 User-to-Sensors Authentication Phase -- 4.5 Sensors-to-Server Authentication Phase -- 4.6 Dynamic Revocation Phase -- 5 Security Analysis -- 6 Performance Analysis -- 6.1 Security Features -- 6.2 Computation Cost -- 6.3 Communication Cost -- 7 Conclusion -- References -- Secure and Efficient k-Nearest Neighbor Query with Privacy-Preserving Authentication -- 1 Introduction -- 1.1 Contributions -- 1.2 Related Works -- 1.3 Paper Organization -- 2 Preliminaries -- 3 System Framework -- 3.1 System Model -- 3.2 Security Assumptions and Security Goals -- 3.3 Secure Sub-protocols -- 3.4 The Main Idea of kNN Query -- 4 Secure Index Structure -- 4.1 Secure Two-Level Partition Index -- 5 Pre-read Protocol -- 5.1 Type-1: Secure Group Read Based on E(N) -- 5.2 Type-2: Secure Group Read Based on E(id) -- 5.3 Type-3: Secure Record Read Based on E(id) -- 6 Secure kNN Schemes S-kQ and SV-kQ -- 6.1 Secure kNN Scheme S-kQ -- 6.2 Verifiable Scheme Based on LT -- 6.3 Secure and Verifiable kNN Scheme SV-kQ -- 6.4 The Optimized Ciphertext Generation -- 7 Performance Evaluation -- 7.1 Evaluation of Different SkNN Schemes -- 7.2 Evaluation of Verification Process -- 8 Conclusion -- A Indistinguishable Read Operation -- B Complexity Analysis -- C Security Analysis -- D Evaluation of Read Protocol and Other Data Setting -- References -- A Network Security Situation Assessment Method Based on Multi-attention Mechanism and HHO-ResNeXt -- 1 Introduction -- 2 Related Work -- 3 Convolutional Neural Network (CNN) -- 3.1 The Structure of the ResNeXt Block -- 3.2 Efficient Channel Attention (ECA) Module -- 3.3 Contextual Transformer (CoT) Block -- 4 Harris Hawks Optimization (HHO) -- 4.1 Eploration Phase -- 4.2 Transition from Exploration to Exploitation -- 4.3 Exploitation Phase.
5 Construction of Network Model Based on Multi-attention Mechanism and HHO-ResNeXt -- 5.1 The ECA-ResNeXt Block -- 5.2 The CoTNeXt Block -- 5.3 The Complete Structure of the Model in This Paper -- 6 Experiments -- 6.1 Dataset Description -- 6.2 UNSW-NB15 Dataset Preprocessing -- 6.3 Selected Hyperparameters -- 6.4 Experiment Results -- 7 Conclusion -- References -- A Privacy-Preserving Federated Learning with Mutual Verification on Vector Spaces -- 1 Introduction -- 2 Related Work -- 3 System Model and Design Goal -- 3.1 System Model -- 3.2 Design Goal -- 4 Our Scheme -- 4.1 System Initialization -- 4.2 Local Training -- 4.3 Gradients Verification -- 4.4 Gradients Aggregation -- 4.5 Subkeys Distribution -- 4.6 Recovery of the Aggregation Result -- 5 Security Analysis -- 5.1 Privacy -- 5.2 Verification -- 6 Conclusion -- References -- Data Detection -- Patch-Based Backdoors Detection and Mitigation with Feature Masking -- 1 Introduction -- 2 Related Work -- 2.1 Backdoor Attack -- 2.2 Backdoor Defense -- 3 Abnormal Feature Distribution and Detection and Defense -- 3.1 Backdoors Detection and Defense Based on Feature Cells Importance -- 3.2 Backdoors Detection Based on Gradient Method -- 4 Experimental Evaluations -- 4.1 Backdoors Detection and Mitigation Against Trojan Attack -- 4.2 Backdoors Mitigation and Defense Against Badnets Attack -- 4.3 Further Exploration of the Proposed Schemes --

5 Conclusion -- References -- Detection and Defense Against DDoS Attack on SDN Controller Based on Feature Selection -- 1 Introduction -- 2 Background -- 2.1 Software Defined Network -- 2.2 OpenFlow -- 3 Related Work -- 4 The Designed Scheme -- 4.1 Data Process Module -- 4.2 Attack Detection Module -- 4.3 Attack Defense Module -- 5 Experiments and Evaluation -- 5.1 Experiment -- 5.2 Performance Metrics -- 6 Conclusion -- References.
Commodity-Tra: A Traceable Transaction Scheme Based on FISCO BCOS.