1. Record Nr. UNISA996587860203316

Autore	Ge Chunpeng
Titolo	Information Security and Cryptology : 19th International Conference, Inscrypt 2023, Hangzhou, China, December 9-10, 2023, Revised Selected Papers, Part II
Pubbl/distr/stampa	Singapore : , : Springer, , 2024 ©2024
ISBN	981-9709-45-8
Edizione	[1st ed.]
Descrizione fisica	1 online resource (426 pages)
Collana	Lecture Notes in Computer Science Series ; ; v.14527
Altri autori (Persone)	YungMoti
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- Contents - Part II -- Contents - Part I -- System Security -- Text Laundering: Mitigating Malicious Features Through Knowledge Distillation of Large Foundation Models -- 1 Introduction -- 2 Related Work -- 2.1 Adversarial Attack and Defense -- 2.2 Backdoor Attack and Defense -- 2.3 Prompt Learning -- 2.4 Knowledge Distillation -- 3 Methodology -- 3.1 Threat Model -- 3.2 Zero-Shot Prompt Learning -- 3.3 Knowledge Distillation -- 4 Experimental Settings -- 4.1 Datasets and Victim Models -- 4.2 Attack Schemes -- 4.3 Defence Baseline -- 4.4 Knowledge Distillation Setting -- 4.5 Metrics -- 5 Evaluation -- 5.1 Text Laundering Against Backdoor Attack -- 5.2 Text Laundering Against Adversarial Attack -- 5.3 Analyses of Knowledge Distillation of Text Laundering -- 6 Discussion and Future Work -- 7 Conclusion -- References -- An Android Malware Detection Method Using Better API Contextual Information -- 1 Introduction -- 2 Related Work -- 2.1 Detection Method Using API Frequency Information -- 2.2 Detection Method Using API Contextual Information -- 3 Android Malware Detection Method -- 3.1 Call Graph Optimization -- 3.2 Feature Embedding -- 4 Experiment and Analysis -- 4.1 Experimental Setup -- 4.2 Malware Detection Performance -- 4.3 Impact of Call Graph Optimization -- 5 Conclusion -- References -- TAElog: A Novel Transformer AutoEncoder-Based Log Anomaly Detection Method -- 1 Introduction

-- 2 Related Works -- 3 Methods -- 3.1 Preliminaries -- 3.2 Overview -- 3.3 Data Processing -- 3.4 Transformer Based Autoencoder -- 3.5 Loss and Detection -- 4 Experiments -- 4.1 Datasets -- 4.2 Setup and Evaluation Criteria -- 4.3 Results and Analysis -- 5 Conclusion and Future Works -- References -- EVFLR: Efficient Vertical Federated Logistic Regression Based on Batch Operations -- 1 Introduction -- 2 Related Work.
2.1 Packaging Methods in FL -- 2.2 Chinese Remainder Representation -- 2.3 Privacy Protection Methods in FL -- 3 Background and Preliminaries -- 3.1 Chinese Remainder Representation -- 3.2 Multiplicative Symmetric Quantization -- 3.3 Analytical Clipping for Integer Quantization -- 3.4 Paillier Homomorphic Encryption -- 4 EVFLR -- 4.1 Problem Statement -- 4.2 Packaged Matrix Operations -- 4.3 Data Conversion -- 4.4 Design -- 5 Experients -- 5.1 Setting -- 5.2 Effectiveness -- 5.3 Efficiency -- 6 Discussion -- 7 Conclusion -- References -- Clustered Federated Learning with Inference Hash Codes Based Local Sensitive Hashing -- 1 Introduction -- 2 Related Work -- 2.1 Personalized Federated Learning -- 2.2 Clustered Federated Learning -- 3 Preliminaries -- 3.1 Local Sensitive Hashing -- 3.2 DBSCAN -- 4 Methodology -- 4.1 Design Goal -- 4.2 Inference Hash Codes -- 4.3 Overview of FedCC -- 4.4 Security Analysis -- 5 Experiments -- 5.1 Experimental Settings -- 5.2 Effect of Hyperparameters -- 5.3 Performance Comparison -- 6 Conclusion -- References -- TIA: Token Importance Transferable Attack on Vision Transformers -- 1 Introduction -- 2 Related Work -- 2.1 Transfer-Based Attacks on CNNs -- 2.2 Transfer-Based Attacks on ViTs -- 3 Methodology -- 3.1 Problem Definition -- 3.2 Overview -- 3.3 Randomly Shuffle Patches -- 3.4 Token Importance Attack -- 4 Experiments -- 4.1 Experimental Settings -- 4.2 Comparison of Transferability -- 4.3 Ablation Study -- 5 Conclusion -- References -- Cryptography Engineering -- Hardware Acceleration of NTT-Based Polynomial Multiplication in CRYSTALS-Kyber -- 1 Introduction -- 1.1 Related Work -- 1.2 Our Contributions -- 2 Preliminaries -- 2.1 Notation -- 2.2 CRYSTAL-KYBER -- 2.3 NTT in KYBER -- 3 Proposed Design Overview -- 3.1 Module Reduction Unit -- 3.2 Butterfly Unit -- 3.3 PWM Operation Unit -- 3.4 Overall Design Scheme.
4 Results and Comparison -- 4.1 Results -- 4.2 Comparisons -- 5 Conclusion -- References -- V-Curve25519: Efficient Implementation of Curve25519 on RISC-V Architecture -- 1 Introduction -- 1.1 Contributions and Paper Organization -- 2 Preliminaries -- 2.1 Curve25519 -- 2.2 Diffie-Hellman Key Negotiation Algorithm and ECDH -- 2.3 RISC-V and VisionFive -- 3 Methodology -- 3.1 Radix-264 Limb Representation of Large Integer -- 3.2 Implementation of Finite Field Arithmetic -- 3.3 Implementation of Scalar Multiplication Arithmetic -- 4 Performance Evaluation -- 4.1 Experiment Results -- 4.2 Performance Comparison -- 5 Conclusion -- References -- Cryptanalysis -- Improved Integral Cryptanalysis of Block Ciphers BORON and Khudra -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Paper Outline -- 2 Preliminaries -- 2.1 Notations and Definitions -- 2.2 Integral Cryptanalysis -- 2.3 Division Property -- 2.4 Searching Division Trails -- 2.5 A Brief Introduction of BORON and Khudra -- 3 Our Model to Calculate Linear Constraints -- 3.1 Model for Generating More Inequalities -- 3.2 MILP Method for Selecting Inequalities -- 4 Applications on BORON and Khudra -- 4.1 Describing Available Division Property Propagation Through S-Boxes of BORON and Khudra -- 4.2 Division Trail Search Model -- 4.3 Results -- 5 Conclusion -- A Appendix -- A.1 Division Trail Search Model -- A.2 BORON and Khudra's Structure -- References -- Automatic Search of Linear

Structure: Applications to Keccak and Ascon -- 1 Introduction -- 2 Preliminaries -- 2.1 Notations -- 2.2 Description of Keccak-p Permutation -- 2.3 Description of Keccak Hash Function -- 2.4 Description of Ascon -- 2.5 Linear Structures -- 2.6 SAT-Based Cryptanalysis -- 3 SAT Model for Linear Structure Search -- 3.1 Model Initialization and Parameter Setting -- 3.2 Propagation of Linear Bits in the Linear Layer.
3.3 Propagation of Linear Bits in the Non-Linear Layer -- 3.4 Objective Function -- 4 SAT-Based Automatic Linear Structure Analysis on Keccak -- 4.1 Linear Structures of Keccak-d Hash Functions -- 4.2 Improved Preimage Attacks on Keccak-512 -- 5 SAT-Based Automatic Linear Structure Analysis on Ascon -- 5.1 Modified SAT Model -- 5.2 Zero-Sum Distinguishers -- 6 Conclusion -- References -- Differential-Linear Cryptanalysis of Round-Reduced SPARX-64/128 -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Organization -- 2 Preliminaries -- 2.1 Notations -- 2.2 Description of SPARX-64/128 -- 2.3 Differential Characteristic and Linear Approximation of Modular Addition -- 2.4 Differential-Linear Cryptanalysis -- 3 Differential-Linear Characteristic of 14-Round SPARX-64/128 -- 3.1 6-Round Differential-Linear Characteristic of E2 -- 3.2 7-Round Truncated Differential Characteristic of E1 -- 3.3 One-Round Linear Approximation of E3 -- 3.4 Differential-Linear Characteristic of 14-Round SPARX-64/128 -- 4 Differential-Linear Cryptanalysis of SPARX-64/128 -- 4.1 Selection of Input Pairs -- 4.2 Key-Recovery -- 5 Conclusions -- References -- Improved Herrmann-May's Attack with Merging Variables and Lower LLL Bound -- 1 Introduction -- 2 Preliminaries -- 3 Improvements on Herrmann-May's Attack -- 3.1 Merging Variables -- 3.2 Implementing New LLL Bound -- 3.3 Improved Herrmann-May's Attack -- 4 Experiment Results -- 4.1 Experiment Results for Assumption 2 -- 4.2 Experiment Results for Verification -- 5 Conclusion -- A Probability -- References -- Full Round Distinguishing and Key-Recovery Attacks on SAND-2 -- 1 Introduction -- 2 Preliminary -- 2.1 Specification of SAND Block Cipher -- 2.2 Specification of SAND-2 Block Cipher -- 3 Iterative and Full Round Distinguishers of SAND-2 -- 3.1 Linear Distinguishers of SAND-2 -- 3.2 Differential Distinguishers of SAND-2.
4 Key Recovery Attacks on SAND-2 -- 4.1 Full Round Linear Attack -- 4.2 Full Round Differential Attack -- 5 Conclusion -- References -- Real-Time Symbolic Reasoning Framework for Cryptojacking Detection Based on Netflow-Plus Analysis -- 1 Introduction -- 2 Related Work -- 3 Problem Statement -- 4 Netflow-Plus Traffic Analysis -- 4.1 Netflow-Plus for High-Performance -- 4.2 Feature Selection -- 4.3 Pipelined Filtering Process -- 5 Model Stratum with Equations -- 5.1 Mining Machine to Mining Pool -- 5.2 Mining Pool to Mining Machine Direction -- 5.3 Equations Capturing Fixed Packet Length -- 6 Experimental Results -- 6.1 Testing Dilemma -- 6.2 Lively Traffic Testing Setup -- 6.3 Detection Performance -- 6.4 Boolean Filtering Effects -- 6.5 Detection Results -- 6.6 Experimental Evaluation -- 7 Discussion -- 8 Conclusion -- References -- Non-malleable Codes from Leakage Resilient Cryptographic Primitives -- 1 Introduction -- 2 Preliminaries -- 3 The Construction of Codeword -- 3.1 Design of AE -- 3.2 Design of Non-malleable Code -- 3.3 Security Proof Idea of the Construction -- 4 Security Proof of the Construction -- 5 Conclusion -- References -- Short Papers -- DP-Loc: A Differential Privacy-Based Indoor Localization Scheme with Bilateral Privacy Protection -- 1 Introduction -- 2 Related Work -- 3 System Model and Attack Model -- 3.1 System Model -- 3.2 Attacker Model -- 4 Design of DP-Loc -- 4.1 DP Fingerprint Clustering -- 4.2 Fingerprint Permutation -- 4.3 Location

Retrieval -- 5 Theoretical Analysis and Experimental Results -- 5.1 Security Analysis -- 5.2 Experimental Performance Analysis -- 6 Conclusion -- References -- A Practical Multi-candidate Voting Protocol on Quantum Blockchain Adapted for Various Tally Principles -- 1 Introduction -- 2 Preliminaries -- 2.1 Quantum Secure Communication -- 2.2 Quantum Blockchain -- 2.3 Quantum Bit Commitment.
2.4 Voting for Two Candidates.