1. Record Nr. UNISA996464387903316

Titolo	Information security practice and experience : 16th international conference, ISPEC 2021, Nanjing, China, December 17-19, 2021 : proceedings / / Robert Deng [and six others], editors
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2022] ©2022
ISBN	3-030-93206-0
Descrizione fisica	1 online resource (406 pages)
Collana	Lecture notes in computer science
Disciplina	005.8
Soggetti	Computer networks - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- Efficient Construction of Public-Key Matrices in Lattice-Based Cryptography: Chaos Strikes Again -- 1 Introduction -- 2 Preliminaries -- 2.1 The Chaotic System: Logistic Map -- 2.2 LWE and the Encryption Scheme -- 3 The Proposed Public-Key Construction -- 3.1 Generating Uniform Chaotic Sequences -- 3.2 Public Key Matrices Constructed from Chaotic Sequences -- 3.3 The Public-Key Encryption Scheme Based on LWE and Chaos -- 4 Tests -- 4.1 Chi-Square Tests and K-S Tests -- 4.2 Gap Tests -- 4.3 Construction of Keys -- 5 Conclusion -- References -- Explore Capabilities and Effectiveness of Reverse Engineering Tools to Provide Memory Safety for Binary Programs -- 1 Introduction -- 2 Related Works -- 3 Benchmarks and Frameworks -- 3.1 Experimental Framework -- 3.2 Benchmarks -- 4 Static Reverse Engineering -- 4.1 Setup and Implementation Details -- 4.2 Efficacy of Reverse Engineering Tools -- 5 Run-Time Framework to Detect Memory Errors -- 5.1 Dynamic Tracking and Instrumentation Using Pin -- 5.2 Buffer Overflow Detection Accuracy -- 5.3 Performance Overhead -- 6 Conclusions and Future Work -- A Optimized Benchmarks -- B Detection Accuracy Using Ghidra -- C Program Execution Time Overhead by the Pin-Based Run-Time Technique -- References -- Enhanced Mixup Training: a Defense Method Against Membership Inference Attack -- 1 Introduction -- 1.1 A Subsection Sample -- 2

Preliminary -- 2.1 Membership Inference Attack -- 2.2 Recent Defense Against Membership Inference Attack -- 2.3 Definition of Mixup -- 3 Enhanced Mixup Training Against Membership Inference Attack -- 3.1 Enhanced Mixup Training -- 3.2 Regularization Proof of EMI -- 4 Experiment Results -- 4.1 Dataset -- 4.2 Experimental Setup -- 4.3 Experimental Results -- 5 Conclusion and Future Work -- References.
Isogeny Computation on Twisted Jacobi Intersections -- 1 Introduction -- 2 Preliminaries -- 3 Isogenies on Twisted Jacobi Intersections -- 3.1 2-Isogeny -- 3.2 Odd Degree Isogenies -- 4 -Coordinate on Twisted Jacobi Intersections -- 4.1 -Coordinate System for Differential Addition -- 4.2 -Coordinate for Isogenies -- 4.3 Computational Cost -- 5 Conclusion -- References -- EPFSTO-ARIMA: Electric Power Forced Stochastic Optimization Predicting Based on ARIMA -- 1 Introduction -- 2 Related Work -- 2.1 Data Poisoning and Adversarial Examples -- 2.2 ARIMA -- 2.3 Dropout -- 2.4 Data Poisoning Attack Defense -- 3 Our Approach -- 3.1 Similarity Calculation -- 3.2 Data Stochastic Sampling and Data Optimization -- 3.3 EPFSTO-ARIMA -- 4 Experiments and Results -- 4.1 Experimental Data and Parameter Description -- 4.2 Adopted Metrics -- 4.3 Experiments Results -- 5 Conclusions and Future Work -- References -- Out of Non-linearity: Search Impossible Differentials by the Bitwise Characteristic Matrix -- 1 Introduction -- 2 Preliminaries -- 2.1 Notation -- 2.2 The Boolean Function -- 3 Searching the Impossible Differentials by Bitwise Characteristic Matrix -- 3.1 Description of Bitwise Characteristic Matrix -- 3.2 Description of the Contradictions -- 4 Applications from Cryptanalysis Aspects and Main Results -- 4.1 GIFT-64 and GIFT-128 -- 4.2 Other Block Ciphers -- 5 Conclusion -- A The Matrix Representations of GIFT-64 -- B New 6-Round Impossible Differential for GIFT-64 -- C 7-Round Truncated Impossible Differential for GIFT-128 -- References -- Message-Restriction-Free Commitment Scheme Based on Lattice Assumption -- 1 Introduction -- 1.1 History of Commitment Scheme -- 1.2 Lattice-Based Commitment Schemes -- 1.3 Our Contribution -- 2 Preliminaries -- 3 Related Works -- 3.1 Commitment Scheme with Lattice Based Structure -- 4 Proposed Commitment Scheme.
4.1 (Optimal) Extension Ratio -- 4.2 Proposed commitment scheme -- 4.3 Binding and Hiding Properties of Proposed Commitment Scheme -- 4.4 Unconditional Hardness of the DKSm,k, Problem -- 5 Comparison of the Commitment Schemes -- 6 Conclusion -- References -- PUOKMS: Password-Protected Updatable Oblivious Key Management System for Cloud Storage -- 1 Introduction -- 2 Preliminaries -- 2.1 Technical Background -- 2.2 System Model -- 2.3 Adversarial Model -- 2.4 Design Goals -- 3 The Proposed Scheme -- 3.1 Description of PUOKMS -- 3.2 Correctness Proof -- 3.3 Further Discussion -- 4 Security Analysis -- 4.1 Impersonation Attacks and Password Guessing Attacks -- 4.2 Collusion Attacks -- 4.3 Perpetual Leakage Attacks -- 5 Performance Evaluation -- 5.1 Communication Overhead -- 5.2 Computation Overhead -- 6 Conclusion -- References -- OblivShare: Towards Privacy-Preserving File Sharing with Oblivious Expiration Control -- 1 Introduction -- 1.1 Motivation -- 1.2 Summary of Contributions -- 2 Related Work -- 2.1 Existing Secure File Sharing -- 2.2 ORAM for File Storage -- 3 Preliminaries -- 3.1 Secure Computation -- 3.2 ORAM -- 3.3 Synchronised Inside-Outside ORAM Trees -- 4 System Overview -- 4.1 System Architecture -- 4.2 Threat Model -- 5 Detailed Construction -- 5.1 Synchronised ORAM Trees -- 5.2 OblivExp for Expiration Control -- 5.3 OblivData for File Access -- 5.4 Security Guarantees -- 5.5 Performance -- 6 Conclusion -- A METAL's Synchronised Inside-Outside ORAM Trees -- A.1 Secret-

Shared Doubly Oblivious Transfer -- A.2 Distributed Permutation -- References -- Automatic Key Recovery of Feistel Ciphers: Application to SIMON and SIMECK -- 1 Introduction -- 2 Preliminaries -- 2.1 Notations -- 2.2 Linear Cryptanalysis -- 2.3 Description of SIMON and SIMECK -- 3 Efficient Key Recovery with FWHT -- 3.1 Efficient Arbitrary-Round Key Recovery.
3.2 Extended Algorithm - Efficient Arbitrary-Round Key Recovery of Feistel Ciphers -- 4 Getting Attack Complexity Automatically -- 4.1 The Automatic Model of Detecting Guessed Subkeys -- 4.2 The Strategy of Reducing Guessed Subkeys' Size -- 5 Application -- 6 Conclusion -- A Active Subkeys of SIMON and SIMECK -- References -- Efficient Fully Anonymous Public-Key Trace and Revoke with Adaptive IND-CCA Security -- 1 Introduction -- 2 Preliminaries -- 2.1 Asymmetric Bilinear Pairings and Hardness Assumption ch11ren2014fully,ch11lai2016anonymous -- 2.2 Tardos Codes ch11tardos2008optimal -- 2.3 Identity-Based Fully Anonymous Public-Key Trace and Revoke -- 3 Our Construction -- 4 Security Analysis -- 5 Conclusion -- A Proof of the Theorem 4 -- B Proof of the Theorem 5 -- References -- Ring Trapdoor Redactable Signatures from Lattice -- 1 Introduction -- 2 Preliminaries -- 3 Ring Trapdoor Preimage Sampleable Functions -- 4 Ring Trapdoor Redactable Signatures -- 4.1 A Simplified Version of RTRS Scheme -- 4.2 A Full Version of RTRS Scheme -- 5 Conclusion -- References -- WADS: A Webshell Attack Defender Assisted by Software-Defined Networks -- 1 Introduction -- 1.1 Basic Information -- 1.2 Contribution -- 2 Background -- 2.1 Webshells -- 2.2 Webshell Detection -- 2.3 Software-Defined Network -- 3 Machine Learning Method and Techniques -- 3.1 N-Gram Method -- 3.2 TF-IDF Method -- 3.3 Model Training -- 3.4 Experimental and Analysis -- 4 Design -- 4.1 System Architecture -- 4.2 Machine Learning Framework -- 4.3 SDN Controller Framework -- 5 Experiment -- 6 Conclusion -- References -- Cloud-Assisted LLL: A Secure and Efficient Outsourcing Algorithm for Approximate Shortest Vector Problem -- 1 Introduction -- 2 System Model and Security Definitions -- 2.1 System Model -- 2.2 Threat Models -- 2.3 Correctness and Security Definitions.
3 Notations and Preliminaries -- 3.1 Lattice -- 3.2 LLL Reduction Algorithm and Its Properties -- 4 Our Outsourcing Algorithm for SVP -- 4.1 Design Rationale -- 4.2 Detailed Algorithm -- 4.3 Some Remarks -- 5 Correctness, Security, Verifiability and Efficiency -- 5.1 Correctness -- 5.2 Input/Output Privacy -- 5.3 Verifiability -- 5.4 Efficiency -- 6 Practical Performance Evaluation -- 6.1 Evaluation Methodology -- 6.2 Evaluation Results -- 7 Applications -- 8 Conclusion -- References -- Privacy-Preserving Support Vector Machines with Flexible Deployment and Error Correction -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Our Techniques -- 1.3 Organization -- 2 Preliminaries -- 2.1 Support Vector Machines -- 2.2 Shamir's Secret Sharing -- 3 Security Definition for Privacy-Preserving SVM -- 4 Building Blocks of Our Protocol -- 4.1 Secure Fixed-Point Calculation ch15Catrina18 and ch15OS10 -- 4.2 Error-Message Recovery via the Berlekamp-Welch Algorithm -- 5 Privacy-Preserving SVM -- 5.1 Protocol Overview -- 5.2 Protocol Details -- 6 Evaluation -- 6.1 Theoretical Analysis -- 6.2 Experimental Analysis -- 6.3 Comparison -- 7 Conclusion -- A Preliminaries -- A.1 Error-Correcting Codes and Berlekamp-Welch Algorithm -- B Details of Protocols in ch15OS10 and ch15Catrina18 -- B.1 Truncation -- B.2 Fixed-Point Multiplication -- B.3 Batch Calculation -- B.4 The Less-Than-Zero Protocol -- References -- Lightweight EdDSA Signature Verification for the Ultra-Low-Power Internet of Things -- 1

Introduction -- 2 Preliminaries -- 3 Implementation Options for EdDSA Verification -- 3.1 Simultaneous Double-Scalar Multiplication -- 3.2 Two Separate Scalar Multiplications -- 3.3 Compatibility with Other ECC Libraries -- 4 Experimental Results -- 5 Conclusions -- References --
A Dummy Location Selection Algorithm Based on Location Semantics and Physical Distance.
1 Introduction.