1. Record Nr. UNISA996464500103316

Titolo	Cyber security cryptography and machine learning : 5th International Symposium, CSCML 2021, Be'er Sheva, Israel, July 8-9, 2021, proceedings / / editors, Shlomi Dolev [and three others]
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2021] ©2021
ISBN	3-030-78086-4
Descrizione fisica	1 online resource (520 pages)
Collana	Lecture notes in computer science : security and cryptology ; ; Volume 12716
Disciplina	005.82
Soggetti	Data encryption (Computer science)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- Programmable Bootstrapping Enables Efficient Homomorphic Inference of Deep Neural Networks -- 1 Introduction -- 2 Preliminaries -- 2.1 Torus and Torus Polynomials -- 2.2 Probability Distributions -- 3 Discretized TFHE -- 3.1 Encoding/Decoding Messages -- 3.2 Description -- 3.3 Leveled Operations -- 4 Programmable Bootstrapping -- 4.1 Blind Rotation -- 4.2 Look-Up Table Evaluation -- 5 Application to Neural Networks -- 5.1 Layers Without PBS -- 5.2 Layers with PBS -- 6 Experimental Results and Benchmarks -- 7 Conclusion -- A Complexity Assumptions Over the Real Torus -- B Algorithms -- B.1 Blind Rotation -- B.2 Sample Extraction -- B.3 Key Switching -- References -- Adversaries Strike Hard: Adversarial Attacks Against Malware Classifiers Using Dynamic API Calls as Features -- 1 Introduction -- 2 Problem Statement -- 3 Adversarial Learning Background -- 4 Related Work -- 5 Design and Implementation -- 5.1 Data Set Collection and Features Extraction -- 5.2 Target BlackBox Models -- 5.3 Malware Evasion Using GAN (MEGAN) and MEGAN with Reduced Perturbation (MEGAN-RP) -- 5.4 Malware Evasion Using Reinforcement Agents -- 6 Evaluation Results -- 7 Conclusion and Future Work -- References -- Privacy-Preserving Coupling of Vertically-Partitioned Databases and Subsequent Training with Gradient Descent -- 1 Introduction -- 1.1

Related Work -- 1.2 Outline -- 2 Hidden Set Intersection -- 3 Secure Gradient Descent -- 3.1 Regression -- 3.2 Classification -- 3.3 Gradient Descent Approach -- 3.4 MPyC -- 4 Performance -- 4.1 Run-Time -- 4.2 Accuracy -- 5 Conclusions and Future Work -- References -- Principal Component Analysis Using CKKS Homomorphic Scheme -- 1 Introduction -- 2 Preliminaries -- 2.1 CKKS Homomorphic Encryption Scheme -- 2.2 Principal Component Analysis (PCA) -- 2.3 Goldschmidt's Algorithm.
2.4 R2 Score -- 3 Vector Operations -- 3.1 Norm and Inversion by Norm -- 3.2 Ciphertext Packing -- 3.3 Vector Operations on Ciphertext and Sub-ciphertexts -- 4 Homomorphic Evaluations -- 4.1 Homomorhpic Goldschmidt's Algorithm -- 4.2 Homomorphic Power Method -- 4.3 Homomorphic PCA -- 5 Implementation Details and Results -- 5.1 Parameter Selection -- 5.2 Results -- 6 Conclusion and Future Work -- References -- DepthStAr: Deep Strange Arguments Detection -- 1 Introduction -- 2 Goals -- 3 Pattern Description -- 4 Methodology -- 4.1 A Formal Outline of the Algorithm -- 4.2 Suggested Workflow to Find Exploitable Security Weaknesses -- 5 Implementation -- 5.1 The angr Framework -- 5.2 Implementation Details -- 6 Evaluation -- 6.1 Rediscovery of Known Weaknesses in libcurl -- 6.2 Newly Detected Weaknesses -- 6.3 Synthetic Evaluation -- 7 A More General Take Away -- 8 Conclusion -- References -- Robust Multivariate Anomaly-Based Intrusion Detection System for Cyber-Physical Systems -- 1 Introduction -- 2 Threat Model -- 3 Proposed Methodology -- 3.1 Anomaly Detection Algorithm-Denoising Autoencoder (DAE) -- 3.2 Localization of the Attack Points -- 4 Experiments and Results -- 4.1 Dataset -- 4.2 Training Phase -- 4.3 Performance Evaluation Phase -- 4.4 Robustness in the Presence of Adversary During Training -- 5 Deployment of DAE in Real Time -- 6 Conclusion -- References -- Privacy-Preserving Password Strength Meters with FHE -- 1 Introduction -- 2 Fully Homomorphic Encryption -- 2.1 Privacy Preserving Search -- 2.2 Privacy Preserving Index Search -- 3 Privacy Preserving Password Strength Meters -- 3.1 Privacy Preserving Markov Model -- 3.2 Privacy Preserving PCFG Model -- 4 Conclusion and Future Work -- References -- Automatic Detection of Water Stress in Corn Using Image Processing and Deep Learning -- 1 Introduction -- 2 Proposed Approach -- 2.1 Dataset.
2.2 Proposed Method -- 3 Results -- 4 Conclusions -- References -- Tortoise and Hares Consensus: The Meshcash Framework for Incentive-Compatible, Scalable Cryptocurrencies -- 1 Introduction -- 1.1 Consensus, Money, and Contracts -- 1.2 Permissionless Consensus via PoW -- 1.3 Importance of Incentive-Compatibility -- 1.4 Drawbacks of Leader Election -- 1.5 Our Contributions -- 1.6 Related Works -- 2 Informal Protocol Overview -- 3 Meshcash Security -- 3.1 Security Proof Overview -- References -- Game of Drones - Detecting Spying Drones Using Time Domain Analysis -- 1 Introduction -- 2 Background -- 2.1 Video Coding Algorithms -- 3 Related Work -- 4 Adversary Model and Proposed Detection Scheme -- 4.1 Detection Model -- 4.2 Detecting FPV Channels -- 5 Influence of Physical Stimulus -- 5.1 Lab Experiments -- 6 Evaluation -- 7 Conclusions and Future Work -- References -- Privacy Vulnerability of NeNDS Collaborative Filtering -- 1 Introduction -- 2 The NeNDS Algorithm -- 3 Privacy Attack on NeNDS -- 4 NeNDS Shortcomings -- 5 Conclusions -- References -- Lawful Interception in WebRTC Peer-To-Peer Communication -- 1 Introduction -- 2 Background and Related Work -- 2.1 Browsers' Support and Open Source WebRTC Libraries -- 2.2 ETSI Reference Model for Lawful Interception -- 2.3 Current Solutions for Intercepting VoIP Calls -- 3 WebRTC -- 3.1 Connection Initiation -- 3.2 Encryption -- 3.3 P2P

Communication -- 3.4 Multi-party Conversations -- 4 The Interception Model -- 4.1 Signaling Services -- 4.2 Web Applications -- 5 Showcase -- 5.1 Signaling Services -- 5.2 Web Applications -- 5.3 LEA Management Console -- 6 Limitation of the Current Work -- 7 Conclusion -- References -- Hierarchical Ring Signatures Immune to Randomness Injection Attacks -- 1 Introduction -- 2 Hierarchical Signature Scheme -- 2.1 Preliminaries and Notation.
2.2 Definition of Hierarchical-Signature Scheme -- 3 New Security Model -- 3.1 Anonymity Model -- 3.2 Strong Unforgeability Model -- 4 Modified Specific HRS Scheme -- 4.1 Unforgeability Analysis -- 4.2 Anonymity Analysis -- 5 Implementation -- 6 Conclusion -- References -- Theoretical Aspects of a Priori On-Line Assessment of Data Predictability in Applied Tasks -- 1 Introduction -- 2 Description and Problem Definitions -- 3 Metrics of Predictability: Related Work -- 3.1 Selection of a Predictor Based on the Model of Losses from Erroneous Predictions -- 4 Model and Procedure for Choosing a Predictor -- 5 "Ontological" Factors in Probabilistic Models of Prediction -- 6 Conclusion -- References -- Randomly Rotate Qubits, Compute and Reverse for Weak Measurements Resilient QKD and Securing Entanglement -- 1 Introduction -- 2 The Random Basis Encryption Scheme -- 3 Securing Entanglement -- 4 WM and the Random Basis CNOT QKD Scheme -- References -- Warped Input Gaussian Processes for Time Series Forecasting -- 1 Introduction -- 2 Preliminaries -- 3 Warped Input Gaussian Process Model -- 3.1 Model -- 3.2 Training -- 3.3 Forecasting -- 3.4 Modelling Seasonality -- 3.5 Time and Space Complexity -- 4 Empirical Evaluation -- 4.1 Synthetic Datasets -- 4.2 Real-World Datasets -- 5 Related Work -- 6 Conclusion -- References -- History Binding Signature -- 1 Introduction -- 2 Preliminaries -- 2.1 Verifiable Secret Sharing -- 2.2 Verifiable Secret Public Sharing -- 2.3 Verifiable Random Functions -- 3 History Binding Signature -- 4 Conditions for a Valid Signature -- 4.1 Unforgeability -- 4.2 Security -- 4.3 Correctness (Signing) -- 4.4 Correctness (Key-Revealing) -- 5 Conclusion and Future Work -- References -- Effective Enumeration of Infinitely Many Programs that Evade Formal Malware Analysis -- 1 Introduction -- 2 Foundations of Computation Theory.
3 Recursive Function Theory -- 4 Theoretical Impossibility of a Complete formal Malware/Non-malware Program Classification -- 5 Discussion and Directions for Further Research -- References -- DNS-Morph: UDP-Based Bootstrapping Protocol for Tor -- 1 Introduction -- 1.1 Our Contribution -- 2 Related Work -- 3 Threat Model -- 4 Obfsproxy Design -- 5 DNS-Morph Design -- 6 DNS-Morph Reliability -- 6.1 Received Packets Acknowledgments -- 6.2 Sorting Received Packets -- 6.3 DNS-Morph Identifiers' Encryption and Decryption -- 6.4 DNS-Morph Multiple Sessions Support -- 7 DNS-Morph Encoded Packets -- 8 DNS-Morph: Security Analysis -- 8.1 Censor's DPI Capabilities -- 8.2 DNS-Morph DPI Resistance -- 8.3 Additional Attacks and Resistance -- 8.4 Active Probing and Replay Attack Resistance -- 8.5 Domain Names' Entropy -- 9 DNS-Morph Design Considerations -- 9.1 Choice of DNS -- 9.2 Choice of Base32 -- 9.3 Query Types -- 9.4 Recursive DNS -- 10 Tests and Results -- 10.1 Test Setup -- 10.2 Client's Testing Environment -- 10.3 Deep Packet Inspection Tools -- 11 Summary -- 11.1 Future Works -- References -- Polynomial Time k-Shortest Multi-criteria Prioritized and All-Criteria-Disjoint Paths -- 1 Introduction and Related Work -- 2 Finding Prioritized Multi-criteria k-Shortest Paths in Polynomial Time -- 3 Prioritized Multi-criteria 2-Disjoint (Node/Edge) Shortest Paths -- 4 k-Disjoint All-Criteria-Shortest Paths -- References -- Binding BIKE Errors to a Key Pair -- 1 Introduction -- 2 Specific Proposals for BIKE -- 3 Practical

Considerations and the BIKE Additional Implementation Package -- 4 Conclusion -- References -- Fast and Error-Free Negacyclic Integer Convolution Using Extended Fourier Transform -- 1 Introduction -- 2 Preliminaries -- 3 Efficient Negacyclic Convolution -- 3.1 Redundant Approach -- 3.2 Non-redundant Approach -- 4 Analysis of Error Propagation.
4.1 Error Propagation Through FFT and FFNT.