1. Record Nr. UNISA996495571503316

Titolo	Innovative security solutions for information technology and communications : 14th international conference, SecITC 2021, virtual event, November 25-26, 2021, revised selected papers / / edited by Peter Y. A. Ryan and Cristian Toma
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2022] ©2022
ISBN	3-031-17510-7
Descrizione fisica	1 online resource (345 pages)
Collana	Lecture Notes in Computer Science ; ; v.13195
Disciplina	005.8
Soggetti	Computer security Telecommunication systems
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 -- KRAKEN: A Knowledge-Based Recommender System for Analysts, to Kick Exploration up a Notch -- 1 Introduction -- 2 Related Work -- 3 Visualising and Investigating -- 3.1 Log Investigation -- 3.2 ZeroKit -- 3.3 Recommendation -- 4 Recommender System -- 4.1 Recommendation Process -- 4.2 Recommendation Triggers -- 4.3 Knowledge Base -- 4.4 Decision-Making -- 5 Evaluation -- 5.1 Datasets -- 5.2 Experimental Setup -- 5.3 User Feedback -- 5.4 Recommendation Relevance -- 5.5 Providing Assistance to Investigations -- 6 Conclusion -- References -- ADAM: Automatic Detection of Android Malware -- 1 Introduction -- 2 Related Works -- 3 ADAM: The Proposed Android Malware Detection -- 3.1 Dataset -- 3.2 Feature-Set Extraction -- 3.3 MRMR-Based Feature Selection -- 3.4 Training the Model -- 4 Performance Analysis -- 4.1 Discussion -- 4.2 Model Deployment -- 5 Conclusion -- References -- Attack on the Common Prime Version of Murru and Saettone's RSA Cryptosystem -- 1 Introduction -- 1.1 Background -- 1.2 Our Contributions -- 1.3 Organization of the Paper -- 2 Preliminaries -- 2.1 Murru and Saettone's RSA Cryptosystem -- 2.2 Lattice -- 2.3 Finding Small Roots -- 3 Attack on the Common Prime Variant of Murru and Saettone's RSA

Cryptosystem -- 4 Extended Attack on the Common Prime Variant of Murru and Saettone's RSA Cryptosystem -- 5 Experimental Results -- 6 Conclusion -- References -- Identification of Data Breaches from Public Forums -- 1 Introduction -- 2 Related Work -- 2.1 Novelty of this Paper -- 3 Preliminaries -- 3.1 Global Vectors for Word Representation -- 3.2 TF-IDF Vectorizer -- 4 System Model and Model Construction -- 5 Experimental Setup and Performance Evaluation -- 5.1 Datasets -- 5.2 Testbed -- 5.3 Score Evaluation Metric -- 5.4 Performance Evaluation -- 6 Conclusion -- References.
A Forensic Framework for Webmail Threat Detection Using Log Analysis -- 1 Introduction -- 2 Literature Review -- 2.1 Webmail Challenge: Malicious Insider -- 2.2 Assumptions -- 3 Proposed Framework -- 3.1 Start Web Browsing Activity -- 3.2 Memory Capture -- 3.3 Evidence Extraction -- 3.4 Logging -- 3.5 Logging Tool Workflow -- 4 Evaluation and Results -- 4.1 Experimental Setup -- 4.2 Results and Performance -- 4.3 Performance Evaluation and Results -- 5 Benefits of the Proposed Scheme -- 6 Conclusion -- 7 Limitations and Future Work -- References -- An Evaluation of the Multi-platform Efficiency of Lightweight Cryptographic Permutations -- 1 Introduction -- 2 Overview of the Permutations -- 3 Implementation and Evaluation -- 4 Experimental Results -- 5 Conclusions -- References -- Optimized Implementation of SHA-512 for 16-Bit MSP430 Microcontrollers -- 1 Introduction -- 2 SHA-512 -- 2.1 Preprocessing -- 2.2 Hash Computation -- 3 Implementation and Optimization for MSP430 -- 4 Experimental Results -- 5 Concluding Remarks -- A Optimized Rotation of 64-Bit Words -- References -- Limitations of the Use of Neural Networks in Black Box Cryptanalysis -- 1 Introduction -- 2 Preliminaries -- 2.1 Neural Networks -- 2.2 Boolean Functions and Block Ciphers -- 3 On the Hardness of Emulating Boolean Functions -- 3.1 Related Work -- 3.2 Block Ciphers and Permutations -- 3.3 Emulating the Behaviour of a Boolean Function -- 3.4 Noisy Bits -- 4 Analysis of Previous Results -- 5 Emulating Boolean Functions Using Neural Networks -- 5.1 Experimental Results When Varying Number of Samples and Neurons -- 6 Emulating AES Using Neural Networks -- 6.1 AES Specifications -- 6.2 AES Emulation -- 7 Conclusion -- A Preliminaries on Boolean Functions -- B Neural Networks in Black Box Cryptanalysis: Previous Results -- B.1 Cipher Identification -- B.2 Cipher Emulation.
B.3 Key Recovery Attacks -- B.4 Key-Schedule Inversion -- C A Tiny Example -- D Emulating Boolean Functions with Different Cryptographic Properties -- References -- Improved Polynomial Multiplication Algorithms over Characteristic Three Fields and Applications to NTRU Prime -- 1 Introduction -- 2 Notation and Preliminaries -- 3 A New 4-Way Multiplication Method (N3) -- 4 Unbalanced Split 5-Way Polynomial Multiplication Method (U1) -- 5 Application of the New Algorithms to NTRU Prime Decapsulation and the Implementation Results -- 5.1 B1-Hybrid1 Multiplication Method for n = 653 -- 5.2 B1-Hybrid2 Multiplication Method for n = 761 -- 5.3 U1-Hybrid1 Multiplication Method for n = 653 -- 5.4 U1-Hybrid2 Multiplication Method for n = 761 -- 6 Conclusion -- A NTRU Prime Decapsulation and the Flowcharts of the New Hybrid Methods: U1-Hybrid1 and U1-Hybrid2 -- B Tables -- References -- An Optimization of Bleichenbacher's Oracle Padding Attack -- 1 Introduction -- 2 Preliminaries -- 2.1 The PKCS #1 v1.5 and PKCS #11 Standards -- 2.2 Padding Oracles -- 2.3 Bleichenbacher's Attack -- 2.4 Performance Analysis Depending on the Oracle Type -- 3 Already Known Improvements -- 4 Our Proposed Improvement -- 4.1 Description of the Attack -- 4.2 Analysis of the Attack -- 5 Implementation Results --

6 Conclusions and Future Work -- References -- UC Analysis of the Randomized McEliece Cryptosystem -- 1 Introduction -- 2 The Universal Composability Framework -- 3 Coding Theory Background -- 4 The McEliece Cryptosystem -- 5 Main Result -- References -- Using Five Cards to Encode Each Integer in Z/6Z -- 1 Introduction -- 1.1 Protocols of Boolean Functions -- 1.2 Protocols of Non-boolean Functions -- 1.3 Our Contribution -- 2 Preliminaries -- 2.1 Sequence of Cards -- 2.2 Matrix -- 2.3 Pile-Shifting Shuffle -- 3 Encoding Scheme of Shinagawa et al. -- 3.1 Copy Protocol.
3.2 Addition Protocol -- 3.3 Multiplication Protocol -- 4 Encoding Scheme of Nishida et al. -- 4.1 Copy Protocol -- 4.2 Addition Protocol -- 4.3 Multiplication Protocol -- 5 Our Encoding Scheme -- 5.1 Copy Protocol -- 5.2 Addition Protocol -- 5.3 Multiplication Protocol -- 6 Encoding Integers in Other Congruent Classes -- 7 Future Work -- References -- Conditional Differential Cryptanalysis on Bagua -- 1 Introduction -- 1.1 Our Contributions -- 2 Preliminaries -- 2.1 A Brief Description of Bagua -- 2.2 Framework of CDC -- 3 CDC on Bagua -- 3.1 Input Difference Choosing Strategy -- 3.2 Analysis of 182-Round Bagua -- 3.3 Analysis of 204-Round Bagua -- 4 Conclusion -- References -- Perfect Anonymous Authentication and Secure Communication in Internet-of-Things -- 1 Introduction -- 1.1 Case Study: Offline Finding and Privacy -- 2 Contribution and Paper Structure -- 3 Related Work -- 4 Notation and Preliminaries -- 4.1 Notation -- 4.2 Cryptographic Primitives -- 4.3 Ring Signatures -- 5 New AAKE Protocols -- 6 AAKE Protocols and Security Model -- 6.1 Security Model -- 6.2 Security and Anonymity of New AAKE -- 7 Performance Evaluation -- 8 Conclusion and Future Work -- A AAKE Protocol and Security Model -- A.1 Security Model -- B Proof of Theorems -- References -- Flexible Group Non-interactive Key Exchange in the Standard Model -- 1 Introduction -- 1.1 Scalable and Flexible Key Exchange -- 1.2 Group Non-interactive Key Exchange With and Without iO -- 1.3 Our Contribution and the Outline of the Paper -- 1.4 Other Related Works -- 2 Preliminaries -- 2.1 Chameleon Hash Functions -- 2.2 Multilinear Maps -- 2.3 The n-Exponent Multilinear Decision Diffie-Hellman Assumption -- 3 Group Non-interactive Key Exchange and Security Models -- 3.1 Group Non-interactive Key Exchange -- 3.2 Security Models for GNIKE -- 4 A Flexible GNIKE Protocol from Multilinear Maps.
4.1 Protocol Description -- 4.2 Security Analysis -- 5 Proof of Theorem 1 -- 6 Conclusion and Future Works -- A Intractability Analysis of n-Exponent Multilinear Diffie-Hellman Assumption -- B Cases in Game 2 in the Proof of Theorem 1 -- References -- A Multifunctional Modular Implementation of Grover's Algorithm -- 1 Introduction -- 2 Discussion of Grover's Algorithm -- 2.1 An Inductive Approach -- 2.2 A More Accurate Approach -- 3 Qiskit Implementation: Examples and Analysis -- 3.1 Simulation -- 3.2 Execution on Real Devices -- 4 Conclusion -- A Qiskit Source Code -- References -- Lightweight Swarm Authentication -- 1 Introduction -- 2 Preliminaries -- 2.1 Hardness Assumptions -- 2.2 Zero-Knowledge Protocols -- 2.3 A Distributed Unified Protocol -- 3 Computational Diffie-Hellman Swarm Protocol -- 3.1 Description -- 3.2 Security Analysis -- 3.3 Complexity Analysis -- 3.4 Hash Based Variant -- 4 Conclusions -- A Computational Bilinear Diffie-Hellman Swarm Protocol -- References -- New Configurations of Grain Ciphers: Security Against Slide Attacks -- 1 Introduction -- 2 Preliminaries -- 2.1 Grain Family -- 3 Generic Grain Attacks -- 4 Proposed Ideas -- 4.1 Compact Padding -- 4.2 Fragmented Padding -- 5 Conclusion -- A Grain V1 -- B Grain-128 -- C Grain-128a -- D Examples -- E Propagation of Single Bit Differentials

-- F Algorithms -- References -- Improved Security Solutions for DDoS Mitigation in 5G Multi-access Edge Computing -- 1 Introduction -- 2 Background -- 2.1 MEC Architecture -- 2.2 Network Flow Analysis and Deep Packet Inspection -- 2.3 Anomaly Detection System in 5G MEC -- 3 Improved Solutions -- 3.1 Concernes and Solutions -- 3.2 Architectural Proposals -- 4 The Orchestration Process -- 5 Conclusions -- References -- Long-Term Secure Asymmetric Group Key Agreement -- 1 Introduction -- 2 Preliminaries.
2.1 Bilinear Maps and the Bilinear Diffie Hellman Assumption.