1. Record Nr. UNISA996511872003316

Titolo	Information security applications : 23rd international conference, WISA 2022, Jeju Island, South Korea, August 24-26, 2022, revised selected papers / / Ilsun You, Taek-Young Youn (editors)
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2023] ©2023
ISBN	3-031-25659-X
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (361 pages)
Collana	Lecture notes in computer science ; ; Volume 13720
Disciplina	005.8
Soggetti	Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- Cryptography -- Collision-Resistant and Pseudorandom Hash Function Using Tweakable Block Cipher -- 1 Introduction -- 2 Preliminaries -- 2.1 Cryptographic Hash Function -- 2.2 Pseudorandom Function -- 2.3 Tweakable Block Cipher in TWEAKEY Framework -- 2.4 PRF and TPRP Under Related-Key Attack -- 3 Proposed Construction -- 4 Collision Resistance -- 5 Pseudorandom-Function Property -- References -- Provably Secure Password-Authenticated Key Exchange Based on SIDH -- 1 Introduction -- 2 Preliminaries -- 2.1 SIDH -- 2.2 Standard Isogeny-Based Hard Problems -- 3 The Proposed PAKE -- 3.1 Description of the Proposed PAKE -- 3.2 Comparison with Relevant Works -- 4 Security Analysis of the Proposed PAKE -- 4.1 Informal Security Analysis -- 4.2 Security in the BPR Model -- 5 Conclusion -- References -- Group Signatures with Designated Traceability over Openers' Attributes in Bilinear Groups -- 1 Introduction -- 1.1 Our Contribution -- 2 Preliminaries -- 2.1 Syntax of GSdT -- 2.2 Security Definitions of GSdT -- 3 Our Instantiation -- 3.1 Generic Constriction of GSdT in ch3AnadaFH21 -- 3.2 Key Generation and User Joining -- 3.3 Generating and Verifying a Group Signature -- 3.4 Opening and Judging -- 4 Properties -- 4.1 Security -- 4.2 Asymptotic Performance -- 5 Conclusion -- References -- Grover on SPARKLE -- 1 Introduction -- 1.1 Our Contribution and Organization -- 2 Background -- 2.1 SPARKLE -- 2.2 Quantum Gates

-- 2.3 Grover's Algorithm for Key Search -- 3 Quantum Implementation of SPARKLE -- 3.1 SPARKLE Permutation -- 3.2 SCHWAEMM -- 4 Performance -- 5 Cost Estimation for Grover Key Search -- 6 Conclusion -- References -- Network Security -- Quality-of-Service Degradation in Distributed Instrumentation Systems Through Poisoning of 5G Beamforming Algorithms -- 1 Introduction.
2 Techniques for Poisoning 5G Beamforming Algorithms -- 3 A Reconfigurable Surface for Poisoning 5G Beamforming Algorithms -- 3.1 Reconfigurable Surface Modeling -- 3.2 Considered Beamforming Algorithms and Proposed Poisoning Algorithm -- 3.3 Physical Implementation and 5G Radio Channel Characteristics -- 4 Experimental Validation: Simulation and Results -- 5 Conclusions and Future Work -- References -- An Effective Approach for Stepping-Stone Intrusion Detection Using Packet Crossover -- 1 Introduction -- 2 Preliminaries -- 2.1 Definitions of Send/Echo Packets -- 2.2 Packet Crossover -- 2.3 The Distribution of Packets' RTTs in a Connection Chain -- 2.4 The Rationale to Detect SSI Based on the Length of a Connection Chain -- 3 Estimate the Length of a Downstream Connection Chain Using Packet Crossover -- 4 Network Experiments and Performance Analysis -- 5 Conclusion -- References -- Software-Defined Network Based Secure Internet-Enabled Video Surveillance System -- 1 Introduction -- 1.1 Problem Background -- 1.2 Contribution of the Paper -- 1.3 Significance of the Study -- 2 Related Literature Review -- 2.1 Application of an IoT-Based System -- 2.2 Security and Prevention Features -- 3 Secure Internet-Enabled Video Surveillance System -- 3.1 Environment Setup -- 3.2 Network Management Tool -- 3.3 DDOS Attack and Mitigation -- 4 Results and Discussion -- 5 Conclusion and Future Works -- References -- TLS Goes Low Cost: When TLS Meets Edge -- 1 Introduction -- 2 Related Works -- 3 TLS-EC (TLS with Edge Computing) Protocol -- 3.1 Our Approach -- 3.2 TLS-EC Protocol -- 4 Security Evaluation -- 5 Performance Evaluation -- 5.1 Discussion -- 6 Conclusion -- References -- 5G-AKA, Revisited -- 1 Introduction -- 1.1 Motivation and Our Contributions -- 2 Preliminaries -- 2.1 Notation -- 2.2 Computational Assumption.
2.3 Exponential Challenge-Response Signature Schemes -- 3 A Secure AKA Protocol for 5G and Beyond Networks -- 3.1 Initialization -- 3.2 Authentication and Key Agreement -- 4 Security Model -- 5 Security Proof of AKA -- 6 Discussions -- 6.1 UE Anonymity -- 6.2 Forward Secrecy -- 6.3 Explicit Mutual Authentication -- 6.4 UE Unlinkability -- 6.5 Efficiency -- 6.6 Implementation Perspective -- 6.7 Comparison -- References -- Privacy Enhancing Technique -- Membership Privacy for Asynchronous Group Messaging -- 1 Introduction -- 2 Cohn-Gordon et al. SGM Protocol (ART) -- 3 Proposed Protocol -- 4 Conclusion -- References -- On Membership Inference Attacks to Generative Language Models Across Language Domains -- 1 Introduction -- 2 Background of Language Modeling -- 3 Methodology -- 3.1 Threat Model -- 3.2 Text Generation -- 3.3 Membership Inference -- 3.4 Verification -- 4 Evaluation -- 4.1 Environments -- 4.2 Target System -- 4.3 Effectiveness of Membership Inference Across Language Domains -- 4.4 Improving Uniqueness of Inferred Samples -- 5 Discussion -- 6 Related Work -- 7 Conclusion -- References -- A Joint Framework to Privacy-Preserving Edge Intelligence in Vehicular Networks -- 1 Introduction -- 2 Background -- 2.1 Distributed Ledger Technology -- 2.2 Federated Learning -- 2.3 Differential Privacy -- 3 Related Work -- 4 Towards Secure Edge Intelligence -- 5 Numerical Results and Discussion -- 6 Conclusion and Future Work -- References -- Vulnerability Analysis -- Recovering Yaw Rate from Signal Injection

Attack to Protect RV's Direction -- 1 Introduction -- 2 Related Works -- 2.1 Attack on Gyroscopes -- 2.2 Signal Injection Detection Methods -- 2.3 Recovery Methods -- 3 Background -- 3.1 Resonant Frequencies of MEMS Gyroscopes and Accelerometers -- 3.2 Relation Between Accelerometer X, Y-Axis and Gyroscope Z-Axis -- 4 Attack Model -- 5 Our Method.
5.1 Dataset Collection -- 5.2 Linear System Identification -- 5.3 Estimation of Gyroscope Z-Axis -- 6 Evaluation -- 6.1 Experiment Setup -- 6.2 Impacts of Acoustic Signal Injection -- 6.3 Yaw Rates Estimation -- 6.4 Recovery of Odometry System -- 7 Conclusion -- References -- A Survey on Sensor False Data Injection Attacks and Countermeasures in Cyber-Physical and Embedded Systems -- 1 Introduction -- 2 Background -- 3 Threat Model -- 4 Sensor False Data Injection (SFDI) Attacks -- 4.1 Message Broadcasting -- 4.2 Inertial Measurement Unit (IMU) -- 4.3 Microphone -- 4.4 Active Sensors -- 4.5 Other Sensors -- 5 Countermeasures -- 5.1 Receiver Layer -- 5.2 Signal Processing Layer -- 5.3 Control Layer -- 6 Research Challenges -- 7 Conclusion -- References -- Dazzle-attack: Anti-Forensic Server-side Attack via Fail-Free Dynamic State Machine -- 1 Introduction -- 2 Motivating Example -- 3 Design -- 3.1 Identifying Input Words via Profiling -- 3.2 Dazzle-attack Creator -- 4 Evaluation -- 4.1 Reliability of Dazzle-attack -- 4.2 Anti-forensic Capability of Dazzle-attack -- 4.3 Comparison with Existing Obfuscators -- 5 Discussion -- 6 Related Work -- 7 Conclusion -- A Appendix -- A.1 Payload types -- References -- vkTracer: Vulnerable Kernel Code Tracing to Generate Profile of Kernel Vulnerability -- 1 Introduction -- 2 Background -- 2.1 Kernel Vulnerability and PoC Code -- 3 Precondition of Environment and Scenario -- 4 Design -- 4.1 Concept -- 4.2 Approach -- 4.3 Profile of Vulnerable Kernel Codes -- 5 Implementation -- 5.1 Profile Generation -- 5.2 Kernel Code Tracing and Virtual Address Range Identification -- 5.3 Termination Condition -- 6 Evaluation -- 6.1 Evaluation Environment -- 6.2 Tracing and Identification Consideration -- 6.3 Performance Measurement -- 7 Discussion -- 7.1 Evaluation Result Consideration -- 7.2 Limitation -- 7.3 Portability.
8 Related Work -- 8.1 Comparison -- 9 Conclusion -- References -- Security Engineering -- ARMing-Sword: Scabbard on ARM -- 1 Introduction -- 1.1 Contributions -- 1.2 Organization of the Paper -- 2 Backgrounds -- 2.1 Scabbard: A Suite of Post-quantum Key-Encapsulation Mechanisms -- 2.2 Target Processor: Apple M1 Processor -- 2.3 Optimized Implementations of Post-Quantum Cryptography on ARM Processors -- 3 Proposed Techniques -- 3.1 Instruction Set -- 3.2 Evaluation: Direct Mapping -- 3.3 Multiplication: Sliding Window -- 4 Evaluation -- 5 Conclusion -- References -- Optimized Implementation of Quantum Binary Field Multiplication with Toffoli Depth One -- 1 Introduction -- 1.1 Our Contribution -- 2 Background -- 2.1 Binary Field Multiplication -- 2.2 Karatsuba Multiplication -- 2.3 Quantum Gates -- 3 Optimized Implementation of Quantum Binary Field Multiplication -- 3.1 Parallel Quantum Multiplication with the Karatsuba Algorithm -- 3.2 Toffoli Depth Optimization with Recursive Karatsuba Algorithm -- 3.3 Recycling Qubits with Reverse Operation -- 3.4 Optimized Implementation of Quantum Multiplication of T-Depth One -- 3.5 Quantum Modular Reduction -- 4 Performance -- 5 Conclusion -- References -- Time-Optimal Design of Finite Field Arithmetic for SIKE on Cortex-M4 -- 1 Introduction -- 2 Related Work -- 3 Preliminaries -- 3.1 SIKE -- 3.2 ARMv7-M Architecture -- 4 Proposed Design for SIKE Field Arithmetic -- 4.1 Notation -- 4.2 Multi-precision Multiplication -- 4.3 Multi-precision Squaring -- 4.4 Multi-precision Reduction -- 4.5

Performance Evaluation -- 5 SIKE Performance Speedup -- 6 Conclusions -- References -- Analysis of Radioactive Decay Based Entropy Generator in the IoT Environments -- 1 Introduction -- 2 Background -- 2.1 Random Number Generator -- 2.2 Quantum Random Number Generator -- 3 Materials and Method -- 3.1 Digital Data Harvesting.
3.2 Analysis of Pulse Collector for IoT Devices.

Sommario/riassunto

This book constitutes the revised selected papers from the 23rd International Conference on Information Security Applications, WISA 2022, which took place on Jeju Island, South Korea, during August 2022. The 25 papers included in this book were carefully reviewed and selected from 76 submissions. They were organized in topical sections as follows: network security; cryptography; vulnerability analysis; privacy enhancing technique; security management; security engineering.