1. Record Nr. UNINA9910616393803321

Titolo	Applied cryptography in computer and communications : Second EAI International Conference, AC3 2022, virtual event, May 14-15, 2022, proceedings / / edited by Jingqiang Lin, Qiang Tang
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2022] ©2022
ISBN	3-031-17081-4
Descrizione fisica	1 online resource (229 pages)
Collana	Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering ; ; v.448
Disciplina	929.605
Soggetti	Computer security
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 -- Quantum-Safe Cryptographic Solution -- DU-QS22: A Dataset for Analyzing QC-MDPC-Based Quantum-Safe Cryptosystems -- 1 Introduction -- 2 QC-MDPC-Based Cryptosystem -- 3 Importance of Decoder -- 4 Overview of Our Implementation -- 4.1 Key-Generation Module -- 4.2 Encryption Module -- 4.3 Decryption Modules -- 5 DU-QS22 Dataset -- 6 Conclusion -- References -- Quantum-Safe Signing of Notification Messages in Intelligent Transport Systems -- 1 Introduction -- 2 Previous Work -- 3 Test Program -- 3.1 Implementing the Digital Signature Algorithms -- 3.2 Performance Tests -- 4 Results -- 5 Discussion -- 6 Future Research -- 7 Summary -- References -- Applied Cryptography for IoT -- WB-GWS: An IoT-Oriented Lightweight Gateway System Based on White-Box Cryptography -- 1 Introduction -- 2 Preliminaries -- 3 The Construction of WB-GWS -- 3.1 The Framework of WB-GWS -- 3.2 The Protocols of WB-GWS -- 4 Gateway Addition -- 5 Gateway Removal -- 6 Security Analysis -- 7 Experiment -- 7.1 The Experiment Base on Temperature and Humidity Sensor System -- 7.2 The Performance Comparison -- 8 Conclusions -- References -- Symmetric Key Based Scheme for Verification Token Generation in Internet of Things Communication Environment -- 1 Introduction -- 2 Related Work -- 3 System Model -- 3.1 System Setup

Phase -- 3.2 Registration Phase -- 3.3 Authentication and Session Key Negotiation Phase -- 4 Comparative Analysis and Evaluation -- 4.1 Security Evaluation -- 4.2 Performance Evaluation -- 5 Conclusion and Future Work -- References -- Resource Consumption Evaluation of C++ Cryptographic Libraries on Resource-Constrained Devices -- 1 Introduction -- 2 Related Work -- 3 Methodology -- 4 Evaluation -- 4.1 Selected Algorithms -- 4.2 Experimental Setup -- 4.3 Discussion of Results -- 4.4 Limitations.
5 Conclusions and Future Work -- References -- Authentication Protocol -- A Secure Lightweight RFID Mutual Authentication Protocol Without Explicit Challenge-Response Pairs -- 1 Introduction -- 1.1 Structure of the Paper -- 2 Preliminaries -- 3 The Proposed Protocol -- 3.1 Notations -- 3.2 Assumptions of Our Proposed Protocol -- 3.3 Authentication Process -- 4 BAN Logic Analysis and Simulation Using the Scyther -- 4.1 BAN Logical Analysis -- 4.2 Simulation Using the Scyther -- 5 Security Analysis -- 6 Performance Evaluation -- 7 Conclusion -- A Analysis of the Gope et al.'s Scheme -- A.1 Performance and Security Analysis of Gope's Scheme -- B Physical Unclonable Functions -- C Feldman's (t,n)-threshold Verifiable Secret Sharing Scheme -- D Basic Notations and Logical Postulates of BAN Logical -- D.1 Basic Notations -- D.2 Logical Postulates -- E Security Simulation Using Scyther -- References -- bisAUTH: A Blockchain-Inspired Secure Authentication Protocol for IoT Nodes -- 1 Introduction -- 2 Related Works -- 3 bisAUTH: A New Blockchain-Inspired Secure Authentication Protocol for IoT Nodes -- 3.1 Main Components of the bisAUTH Protocol -- 3.2 Main Phases of the bisAUTH Protocol -- 3.3 bisAUTH Protocol Assessment -- 4 Conclusion -- References -- Real-World Applied Cryptography -- X-FTPC: A Fine-Grained Trust Propagation Control Scheme for Cross-Certification Utilizing Certificate Transparency -- 1 Introduction -- 2 Background and Challenges -- 2.1 Cross-Certification -- 2.2 Trust Propagation Challenge -- 2.3 Certificate Transparency -- 3 X-FTPC: Fine-Grained Trust Propagation Control for Cross-Certification -- 3.1 Overview -- 3.2 Fine-Grained Control Based on Mandatory-Log in X-FTPC -- 3.3 Different Scenarios in X-FTPC -- 3.4 Potential Threats in X-FTPC -- 4 Discussion in Feasibility of X-FTPC -- 5 Related Work -- 6 Conclusion -- References.
The Block-Based Mobile PDE Systems are Not Secure - Experimental Attacks -- 1 Introduction -- 2 Background -- 2.1 Flash Memory -- 2.2 Flash Translation Layer -- 2.3 Plausibly Deniable Encryption -- 3 Model and Assumptions -- 4 Experimentally Attacking the Block-Layer PDE Systems -- 4.1 Experimental Setup -- 4.2 Experimental Attacks -- 5 Discussion -- 6 Related Work -- 6.1 The Hidden Volume-Based PDE Systems -- 6.2 The Steganographic File Systems -- 7 Conclusion -- References -- Black-Box Testing of Cryptographic Algorithms Based on Data Characteristics -- 1 Introduction -- 2 Preliminaries -- 3 Design and Implementation -- 3.1 Overview -- 3.2 Characteristic Data Extraction and Data Set Construction -- 3.3 Characteristic Data Matching Strategy -- 3.4 Cryptographic Algorithm Determination -- 4 Evaluation -- 4.1 Experiments Setup -- 4.2 Effectiveness -- 4.3 Performance -- 4.4 Limitations -- 5 Summary -- A Cryptographic Algorithm Supports -- B Test File Information -- References -- Network Attack and Defense -- IoT Devices Classification Base on Network Behavior Analysis -- 1 Introduction -- 2 Related Work -- 3 Network Behavior Analysis Based IoT Devices Classification -- 3.1 Motivation an Analysis -- 3.2 Overview -- 3.3 Session Feature Extraction -- 3.4 Session Feature Preprocess -- 3.5 LSTM Based Sequence Feature Extraction -- 3.6 Multilayer Perceptron Classifier -- 4 Evaluation -- 4.1 IoT Testbed Construction and Traffic Collection --