1. Record Nr. UNINA9910508446903321

Titolo	E-business and telecommunications : 17th International Conference on E-Business and Telecommunications, ICETE 2020, online event, July 8-10, 2020 : revised selected papers / / Mohammad S. Obaidat, Jalel Ben-Othman (editors)
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2021] ©2021
ISBN	3-030-90428-8
Descrizione fisica	1 online resource (243 pages)
Collana	Communications in computer and information science ; ; 1484
Disciplina	621.382
Soggetti	Telecommunication systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- An Improved Bit Masking Technique to Enhance Covert Channel Attacks in Everyday IT Systems -- 1 Introduction -- 1.1 Contribution -- 1.2 Structure -- 2 Related Work -- 3 Building Blocks -- 3.1 Bit-Masking -- 3.2 Acquiring White Traffic -- 3.3 Matching Algorithm -- 4 Methodology -- 5 Attack Implementations -- 5.1 Improved Version 1 -- 5.2 Improved Version 2 -- 6 Experiments and Results -- 6.1 Performance Tests -- 6.2 Attack Evasion Tests -- 7 Conclusion -- References -- Security and Complexity of a New Variant of the McEliece Cryptosystem Using Non-linear Convolutional Codes -- 1 Introduction -- 2 A New Non-linear Convolutional Encoding/Decoding Algorithm -- 2.1 Non-linear Convolutional Cryptosystem -- 2.2 New Encoding/Decoding Algorithm Using Non-linear Convolutional Code -- 3 A New Variant of the Mceliece Cryptosystem -- 3.1 The Classical McEliece Cryptosystem -- 3.2 The New Variant of the McEliece Cryptosystem [14] -- 4 Cryptographic Algorithm Metrics -- 4.1 Key Size Analysis -- 4.2 Complexity Analysis -- 5 Cryptanalysis -- 5.1 Structural Attack [14] -- 5.2 Decoding Attack [14] -- 6 Results and Discussion -- 6.1 Structural Attack -- 6.2 Decoding Attack -- 6.3 Comparison with Existing McEliece Cryptosystems -- 7 Conclusion -- Appendix -- Transition Tables -- References -- A Secure Distributed Hash-Based

Encryption Mode of Operation Suited for Big Data Systems -- 1 Introduction -- 2 Related Work -- 3 Proposed Solution -- 3.1 Distributed Cipher Block Chaining: DCBC -- 3.2 Target Criteria -- 3.3 How Does DCBC Work? -- 3.4 Encryption and Decryption in DCBC -- 3.5 IV Generator -- 4 Security Properties -- 4.1 CPA Security -- 4.2 Blockwise Adaptive Chosen Plaintext Attack Security -- 5 Theoretical Performance Cost -- 5.1 Assumptions -- 5.2 Cost Function C -- 5.3 Theoretical Performance Comparison.
6 Theoretical Diffusion -- 6.1 The Probability of a Bit Flipping -- 6.2 Probability of at Least M Bits Flipping -- 7 Conclusion and Future Work -- References -- An Assurance Framework and Process for Hybrid Systems -- 1 Introduction -- 2 Assurance Requirements -- 3 Assurance Framework -- 4 REST Interface -- 4.1 OpenAPI Document -- 4.2 Component REST API -- 5 Assurance Process -- 5.1 Building Blocks -- 5.2 Assurance Process -- 6 Walkthrough and Experiments -- 6.1 Process in Execution -- 6.2 Experiments -- 7 Comparison with Existing Solutions -- 8 Conclusions -- References -- PakeMail: Authentication and Key Management in Decentralized Secure Email and Messaging via PAKE -- 1 Introduction -- 1.1 Motivation -- 1.2 Contributions and Structure -- 1.3 Related Work -- 2 Framework and Preliminaries -- 3 Pitfalls in Out-of-Band Authentication -- 3.1 Inattentive Users and Partial Preimage Attacks -- 3.2 Case Study -- 4 Authentication in Secure Email and Messaging via PAKE -- 4.1 Public Key Authentication via PAKE -- 4.2 An Instantiation Based on SPAKE2 -- 4.3 Selecting a PAKE Protocol -- 4.4 Transport Mechanism -- 5 Enhancements to Secure Email and Messaging by PAKE -- 5.1 Key Management and Authentication Improvements -- 5.2 Cryptographic Properties Enabled by PAKE -- 5.3 Cryptographic Enhancements to Email and Messaging -- 5.4 Comparison -- 6 Implementation: PakeMail -- 6.1 Cryptographic Details -- 6.2 PAKE Protocol Carried Out over Email -- 6.3 Implemented Scenarios -- 6.4 Performance -- 6.5 Further Design and Security Considerations -- 7 Security and Low-Entropy Secrets -- 8 Further Directions -- References -- Practically Efficient Attribute-Based Encryption for Compartmented and Multilevel Access Structures -- 1 Introduction -- 2 Preliminaries -- 3 Our Contribution -- 3.1 Motivation and Main Goal -- 3.2 Our Scheme for CASs.
3.3 Variations on the Same Theme: The Case of MASs -- 4 Extension to Multiple-Input Boolean Trees -- 5 Implementation -- 6 Conclusions -- References -- Analysis of In-Place Randomized Bit-Flipping Decoders for the Design of LDPC and MDPC Code-Based Cryptosystems -- 1 Introduction -- 2 Notation and Background -- 3 In-Place Randomized Bit-Flipping Decoder -- 3.1 An In-Place, Randomized Bit-Flipping Decoder -- 3.2 Modeling of the Bit-Flipping Probabilities -- 4 Validation of DFR Models and Cryptosystem Design -- 4.1 Experimental Validation of DFR Models -- 4.2 Design of Code-Based Cryptosystems -- 5 Related Work and Discussion -- 6 Conclusion -- References -- Business Analyst Tasks for Requirement Elicitation -- 1 Introduction -- 2 Systematic Literature Review -- 3 Business Analyst for Agile Method Driven Requirement Elicitation -- 4 Business Analyst in Ontology Driven Requirement Engineering -- 5 Case Study on Non-formal Education System Development -- 6 Conclusions -- References -- Chained Transaction Protocol Automated Verification Using Cl-AtSe -- 1 Introduction -- 2 Chained Transaction Protocol -- 2.1 Exchange Sub-protocol -- 2.2 Resolution 1 Sub-protocol -- 2.3 Resolution 2 Sub-protocol -- 3 Overview of AVISPA Tool -- 3.1 AVISPA Tool -- 3.2 High Level Protocol Specification Language -- 4 Automated Verification of Chained Transaction Protocol -- 4.1 Agent's Basic Roles -- 4.2 Protocol's Sessions Composed Roles -- 4.3 Environment Role -- 4.4

Security Requirements -- 4.5 Verification Results -- 5 Conclusions -- References -- Overall Feasibility of RF Energy Harvesting for IoT -- 1 Introduction -- 2 Constraints -- 2.1 Ambient Energy -- 2.2 Energy Consumption -- 3 Choice of Storage Capacitor -- 4 Rectifier -- 5 Overall System Feasibility -- 5.1 Theoretical Model -- 5.2 Application of the Model -- 6 Conclusion -- References -- Author Index.