1. Record Nr. UNISA996464527603316

Titolo	Security and privacy : second International Conference, ICSP 2021, Jamshedpur, India, November 16-17, 2021, proceedings / / Pantelimon Stanica, Sihem Mesnager, Sumit Kumar Debnath (editors)
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2021] ©2021
ISBN	3-030-90553-5
Descrizione fisica	1 online resource (154 pages)
Collana	Communications in Computer and Information Science ; ; 1497
Disciplina	005.8
Soggetti	Computer security Computer networks - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- Cryptanalysis and Other Attacks -- Higher Order c-Differentials -- 1 Introduction and Background -- 2 Preliminaries -- 3 Higher Order c-differentials -- 4 The Inverse Function -- 5 The Gold Function -- 6 Summary and Further Comments -- References -- First-Order Side-Channel Leakage Analysis of Masked but Asynchronous AES -- 1 Introduction -- 2 Boolean Masking Schemes Against Vertical SCAs -- 3 First-Order Vertical SCAs Against Masking Schemes -- 4 Experiments on a Real-World AES Code -- 4.1 Target Agnostic Analysis on CPU -- 4.2 Optimal Leakage Model -- 5 Discussion -- 6 Conclusions -- References -- Side-Channel Analysis of CRYSTALS-Kyber and A Novel Low-Cost Countermeasure -- 1 Introduction -- 2 Related Works and Background -- 2.1 Overview -- 2.2 Notation -- 2.3 LWE/R-LWE Problems -- 2.4 Side-Channel Attacks on Lattice-Based Cryptography -- 2.5 Countermeasures -- 3 Analysis Methodology -- 3.1 Our Objective -- 3.2 Leakage Detection Test -- 4 Experimental Results -- 4.1 Flow -- 4.2 Analysis of CRYSTALS-Kyber - Reference Implementation -- 4.3 Analysis of Masked CRYSTALS-Kyber Implementation - Additive Masking -- 4.4 Analysis of Masked CRYSTALS-Kyber Implementation - Multiplicative Masking -- 4.5 Discussion -- 5 Conclusion -- References -- Symmetric Cryptography and Hash Functions, Mathematical

Foundations of Cryptography -- A Suitable Proposal of S-Boxes (Inverse-Like) for the AES, Their Analysis and Performances -- 1 Introduction -- 2 Description of the AES -- 3 Generating Suitable S-Boxes for Block Ciphers -- 3.1 A General Approach -- 3.2 A Proposal S-Box for AES -- 4 Algebraic and Statistical Properties of the Proposed S-Box -- 4.1 Bijectivity of the Proposed S-Box -- 4.2 Fixed Points and Opposite Points -- 4.3 Strict Avalanche Criterion and Distance to SAC -- 4.4 Periodicity of the Proposed S-Box.
4.5 Algebraic Complexity -- 5 Cryptanalysis of the Proposed S-Box -- 5.1 Equivalences of Our S-Box with the Inverse Function -- 5.2 Differential Cryptanalysis -- 5.3 Boomerang Cryptanalysis -- 5.4 Linear Cryptanalysis -- 5.5 Differential-Linear Connectivity Cryptanalysis -- 6 Comparison of Cryptographic Properties Between the Proposed S-Box and Former S-Boxes -- 6.1 Security -- 6.2 Efficiency -- 7 Conclusions -- References -- A Method of Integer Factorization -- 1 Introduction -- 2 Parity Conjecture and the Rank -- 2.1 Notations -- 2.2 Torsion Subgroups -- 2.3 Parity Conjecture -- 3 Two-Descent Method and Integer Factorization -- 4 2-Selmer Group and Integer Factorization -- 5 Experiment -- References -- Embedded Systems Security, Security in Hardware -- Towards a Black-Box Security Evaluation Framework -- 1 Introduction -- 2 Background -- 2.1 Security Evaluation Modes -- 2.2 Electro-Magnetic Fault Injection Attacks -- 3 Proposed Testing Framework -- 3.1 Fingerprinting -- 3.2 Target Exploration -- 3.3 Analysis Strategy -- 3.4 Benchmark Setup -- 3.5 Exploitation and Analysis -- 3.6 Evaluation Criteria -- 4 Experiments on a Real Device: Door-Lock Unlock -- 5 Discussion -- 6 Conclusion -- References -- Multi-source Fault Injection Detection Using Machine Learning and Sensor Fusion -- 1 Introduction -- 1.1 Motivation -- 1.2 Our Contribution -- 2 Background -- 2.1 Fault Injection Attacks -- 2.2 Detecting Fault Attacks with Machine Learning -- 3 Proposed Methodology and Design Idea -- 3.1 Digital Sensor -- 3.2 Smart Monitor -- 3.3 Dataset Information -- 3.4 Machine Learning Based Evaluation Using Two-Stage Detection Framework -- 3.5 Hardware Testing of the Design Using HLS -- 4 Results -- 4.1 Threshold Optimization of Every DS -- 4.2 Classification Between EMFI and Nominal Condition -- 4.3 Classification Between CGFI and Nominal Condition.
4.4 Classification Between Combined EMFI and CGFI Against Nominal Condition -- 4.5 Classification Based on Attack Type Between EMFI and CGFI -- 5 Conclusion -- References -- Authentication, Key Management, Public Key (Asymmetric) Techniques, Information-Theoretic Techniques -- Secure Multi-Party Computation Using Pre-distributed Information from an Initializer -- 1 Introduction -- 1.1 Background -- 1.2 Our Contribution -- 1.3 Outline -- 2 Model -- 2.1 Shamir's Secret Sharing Scheme -- 2.2 Security Conditions -- 3 The Protocol -- 3.1 Pre-processing Phase -- 3.2 Computation Phase -- 4 Conclusion -- References -- Evolving Secret Sharing in Almost Semi-honest Model -- 1 Introduction -- 1.1 Threshold Evolving Secret Sharing -- 2 Hash Functions -- 3 The `Almost' Semi-honest Model -- 4 Our Construction -- 5 Concluding Remarks -- References -- Traceable and Verifier-Local Revocable Attribute-Based Signature with Constant Length -- 1 Introduction -- 1.1 Motivation -- 1.2 Related Work -- 1.3 Contribution and Strategy -- 1.4 Outline -- 2 Preliminaries -- 2.1 Bilinear Maps and Number Theoretic Assumptions -- 2.2 Access Structure ch10DBLP:confspsccsspsGoyalPSW06 -- 3 Traceable and Verifier-Local Revocable Attribute-Based Signature Scheme (TVLR-ABS): Definitions and Security -- 3.1 Oracles and Security Experiments -- 4 Cryptographic Tools -- 4.1 Two-Level Hierarchical Signature Scheme

ch10DBLP:confspspkcspsBoyenW07 -- 4.2 Access Tree Secret Values Assigned -- 4.3 GS Non-interactive Proof Systems -- 5 Construction of TVLR-ABS -- 6 Security Analysis -- 6.1 Comparison -- 7 Conclusion -- References -- Correction to: Side-Channel Analysis of CRYSTALS-Kyber and A Novel Low-Cost Countermeasure.
Correction to: Chapter "Side-Channel Analysis of CRYSTALS-Kyber and A Novel Low-Cost Countermeasure" in: P. Stnic et al. (Eds.): Security and Privacy, CCIS 1497, https://doi.org/10.1007/978-3-030-90553-8_3 -- Author Index.