1. Record Nr. UNISA996503471403316

Autore	Batina Lejla
Titolo	Security, Privacy, and Applied Cryptography Engineering : 12th International Conference, SPACE 2022, Jaipur, India, December 9-12, 2022, Proceedings
Pubbl/distr/stampa	Cham : , : Springer, , 2022 ©2022
ISBN	3-031-22829-4
Descrizione fisica	1 online resource (346 pages)
Collana	Lecture Notes in Computer Science ; ; v.13783
Altri autori (Persone)	PicekStjepan MondalMainack
Disciplina	005.8
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- Symmetric Cryptography -- Modeling Large S-box in MILP and a (Related-Key) Differential Attack on Full Round PIPO-64/128 -- 1 Introduction -- 2 MILP Based Differential Characteristic Search -- 2.1 Modeling Large S-box -- 2.2 Linear Inequalities for Minimization of Active S-boxes -- 2.3 Linear Inequalities for Optimization of Probability -- 3 Application to Lightweight Block Cipher PIPO-64/128 -- 3.1 Specification of PIPO-64/128 -- 3.2 MILP Modeling for PIPO-64/128 -- 3.3 Differential Cryptanalysis of PIPO-64/128 -- 3.4 Impossible Differential Cryptanalysis of PIPO-64/128 -- 3.5 Related-Key Differential Distinguisher for PIPO-64/128 -- 3.6 Related-Key Differential Attack on Full-round PIPO-64/128 -- 4 Conclusion -- Appendices -- A C = E (P,K) = E(P,K') where K' = K K K=0x6DC416DD779428D27E1D20AD2E152297 K=0x00400008010010000020000020000000 -- B MILES: MInimized Linear inEqualities for Large S-Boxes -- C Example: Linear Inequalities Generation using MILES -- References -- Light but Tight: Lightweight Composition of Serialized S-Boxes with Diffusion Layers for Strong Ciphers -- 1 Introduction -- 1.1 Related Work -- 1.2 Our Contributions -- 2 Ultra-lightweight Almost-MDS Matrix -- 3 LbT-n-: Specification and Design Rationale -- 3.1 Formal Specification of LbT-64-128 -- 3.2

Choice of the Linear Layer -- 3.3 Choice of the Key Scheduling and Add Round Key Operations -- 3.4 Choice of the Round-Constants -- 4 Security Evaluation -- 5 Threshold Implementation in Hardware -- 5.1 CA Rule Decomposition -- 5.2 TI Decomposition -- 5.3 Implementation Results of the Full Cipher -- 5.4 Resilience Against Probing Attacks -- 5.5 Test Vector Leakage Analysis (TVLA) -- 5.6 Comparative Study -- 6 Conclusion -- References -- Hardware Implementation of Masked SKINNY SBox with Application to AEAD -- 1 Introduction.
2 Background -- 2.1 Hardware Masking, Revisited ch3de2018hardware -- 2.2 SKINNY ch3beierle2016skinny -- 2.3 Romulus -- 2.4 SILVER Leakage Assessment Tool -- 3 Masking the SKINNY SBox -- 4 Formal Verification -- 5 Unit Testing -- 5.1 Accelerated Test Set-Up -- 5.2 Amplification of SNR -- 5.3 The Practical Issue with Hardware Masking and How to Address It -- 6 Implementation of the Full Romulus Modes -- 6.1 Double-Edged Implementations -- 7 Synthesis Results -- 8 Concluding Thoughts -- References -- Bias Cancellation of MixColumns -- 1 Introduction -- 2 Bias Cancellation -- 3 Applications -- 3.1 Adding an 11th Round -- 3.2 Adding Non-Linearity -- 4 Conclusion and Future Work -- References -- Big Brother Is Watching You: A Closer Look at Backdoor Construction -- 1 Introduction -- 1.1 Contribution -- 1.2 Prerequisite -- 1.3 Organisation -- 2 Background -- 2.1 Implementation Level and Cipher Level Backdoors -- 2.2 Context -- 3 Basic Concepts -- 3.1 Practical Application of a Backdoor -- 3.2 Associated Notions of Security -- 4 ZUGZWANG: Constructing a Block Cipher with a Backdoor -- 4.1 Fundamental Idea of ZUGZWANG -- 4.2 A Concrete Instance of ZUGZWANG (Using AES and SHAKE) -- 4.3 Comparison of ZUGZWANG with Malicious/LOWMC-M -- 5 Conclusion -- References -- Public-Key Cryptography, Post-quantum Cryptography, Zero Knowledge Proofs -- KEMTLS vs. Post-quantum TLS: Performance on Embedded Systems -- 1 Introduction -- 1.1 Contribution -- 2 Background -- 2.1 Post-quantum Cryptography -- 2.2 Post-quantumtls TLS -- 3 Experimental Setup -- 3.1 Implementation -- 4 Results -- 4.1 Storage and Memory Consumption -- 4.2 Handshake Times -- 5 Discussion -- 6 Conclusion and Future Work -- A Extended Benchmark Tables -- References -- Protecting the Most Significant Bits in Scalar Multiplication Algorithms*-6pt -- 1 Introduction.
1.1 Software Implementations of Curve25519 -- 1.2 Hardware Implementations of the Complete Addition Formulas -- 2 Background and Experimental Setup -- 2.1 Experimental Setup and Side-Channel Evaluation -- 3 Leakage on Curve25519 -- 3.1 Initial Loop Iterations -- 3.2 Experimental Verification -- 4 Protecting the Most Significant Bits in Curve25519 -- 4.1 Implementing Our Proposed Modification -- 4.2 Implementations of the Ladder Step -- 4.3 Evaluation of Our Countermeasures -- 5 Leakage on the Complete Addition Formulas -- 6 Conclusions and Future Work -- References -- Combining Montgomery Multiplication with Tag Tracing for the Pollard Rho Algorithm in Prime Order Fields -- 1 Introduction -- 2 Background -- 3 Combining Montgomery Multiplication with Tag Tracing -- References -- Card-Based Zero-Knowledge Proof for the Nearest Neighbor Property: Zero-Knowledge Proof of ABC End View -- 1 Introduction -- 2 Definition of Problem -- 3 Protocol for ABC End View -- 4 Conclusion -- References -- Hardware Security and AI -- What Do You See? Transforming Fault Injection Target Characterizations -- 1 Introduction -- 2 Background -- 2.1 Fault Injection and Target Characterization -- 2.2 Polynomial Functions -- 2.3 Kullback-Leibler Divergence (KLD) -- 2.4 Canonical Correlation Analysis (CCA) -- 3 Motivation and Application -- 4 Proposed Transformations -- 4.1 2D Transformations

-- 4.2 Polynomial Transformations -- 5 Utilized Data Examples -- 6 Experimental Results -- 6.1 Electromagnetic Fault Injection (EMFI) Case -- 6.2 Simulated Case -- 6.3 Voltage Glitching Case -- 6.4 Evaluating the Effect of Transformations -- 7 Conclusion and Future Work -- References -- Dual-Tone Multi-Frequency Assisted Acoustic Side Channel Attack to Retrieve Dialled Call Log -- 1 Introduction -- 1.1 Main Intuition and Contributions -- 2 Background.
2.1 Dual-Tone Multi-Frequency (DTMF) Signals -- 2.2 Fast Fourier Transform (FFT) -- 2.3 Machine Learning Models -- 3 Proposed Acoustic Side Channel Attack Methodology -- 3.1 Data Collection and Feature Extraction -- 3.2 Training ML Models with Extracted Features -- 3.3 Inference of Dialed Digits by Attacker -- 4 Experimental Setup and Results -- 4.1 Experimental Setup for Data Collection, Feature Extraction and Training -- 4.2 Experimental Set-up for Inferring the Digits of a Phone Number -- 4.3 Accuracy of Prediction of the Dialed Digits Using the Proposed Acoustic SCA Methodology -- 4.4 Implementation Complexity (Estimated Attack Time) of the Proposed Methodology -- 5 Conclusion -- References -- Machine Learning Attacks on Low-Cost Reconfigurable XRRO and XRBR PUF Designs -- 1 Introduction -- 2 Background -- 2.1 CRO PUFs and BR PUFs -- 2.2 ML Attacks on CRO PUFs and BR PUFs -- 3 Modelling XOR-Based Reconfigurable PUFs -- 3.1 Mechanism of XRBR PUF -- 3.2 Modelling XRBR PUF -- 3.3 Mechanism of XRRO PUF -- 3.4 Modelling XRRO PUF -- 4 Machine Learning Attacks on XOR-Based Reconfigurable PUFs -- 5 Conclusion -- References -- HWGN2: Side-Channel Protected NNs Through Secure and Private Function Evaluation -- 1 Introduction -- 2 Adversary Model -- 3 Related Work -- 3.1 SCA Against NNs -- 3.2 Security-Preserving DL Accelerators -- 3.3 Garbled Accelerators -- 4 Background -- 4.1 SFE/PFE Protocols -- 4.2 Neural Networks (NNs) -- 5 Foundations of HWGN2 -- 5.1 Implementation of HWGN2 -- 6 Evaluation of HWGN2 -- 6.1 Resource Utilization -- 6.2 Side-Channel Evaluation -- 7 Conclusion -- References -- How Many Cameras Do You Need? Adversarial Attacks and Countermeasures for Robust Perception in Autonomous Vehicles -- 1 Introduction -- 2 Background -- 2.1 Adversarial Attacks on Image Recognition -- 2.2 Motivation -- 2.3 Contributions.
3 Spoofing Multiple Cameras with Overlapping FOV -- 3.1 Object Detection Output -- 3.2 Formulation of Attack Objective -- 3.3 Robust Adversarial Object Generation -- 3.4 Spoofing Multiple Cameras -- 4 Additional Countermeasures -- 4.1 Dimensionality Reduction -- 4.2 Feature Squeezing: Color Depth Reduction -- 5 Experiments -- 5.1 Dataset -- 5.2 Choice of Objects -- 5.3 Experimental Setup -- 5.4 Evaluation -- 6 Limitations -- 7 Conclusions -- References -- Network Security, Authentication, and Privacy -- SMarT: A SMT Based Privacy Preserving Smart Meter Streaming Methodology -- 1 Introduction -- 2 Related Work -- 3 System Assumptions -- 3.1 System Model -- 3.2 Adversarial Model -- 4 Privacy Preserving Streaming Model of ch15TIFFspsPrivacy -- 4.1 Description of the Privacy Preserving Streaming Model -- 4.2 Drawbacks of Privacy Preserving Streaming Model of ch15TIFFspsPrivacy -- 5 Proposed Privacy Preserving Smart Meter Streaming Algorithm -- 5.1 Privacy Formulation -- 5.2 Detailed Description of the Proposed Algorithm -- 5.3 Privacy Analysis -- 6 Experimental Results -- 6.1 Experimental Setup -- 6.2 Platform -- 6.3 Evaluation of ``Obfuscate-Load-Signature'' Scheme -- 7 Conclusion and Future Work -- References -- An Analysis of the Hardware-Friendliness of AMQ Data Structures for Network Security -- 1 Introduction -- 1.1 Challenges in Membership Query Data Structures on Hardware -- 2 An Insight into AMQ Data Structures -- 2.1 Hash

	Table and Its Variants -- 2.2 Bloom Filter and Its Variants -- 2.3 Cuckoo Filter and Its Variants -- 3 Hardware Architectures -- 3.1 Choosing a Suitable Architecture -- 3.2 Implementation Details -- 4 Evaluation -- 4.1 Evaluation of Lookup Architectures -- 4.2 Evaluation of Key-Value Stores -- 5 Conclusion -- A Hardware Architectures -- A. 1 Cuckoo Hash Table and Cuckoo Filter -- A.2 Peacock Hash Table. B Additional Analysis.
Sommario/riassunto	This book constitutes the refereed proceedings of the 12th International Conference on Security, Privacy, and Applied Cryptography Engineering, SPACE 2022 held in Jaipur, India, during December 9-12, 2022.The 18 full papers included in this book were carefully reviewed and selected from 61 submissions. They were organized in topical sections as follows: symmetric cryptography; public-key cryptography, post-quantum cryptography, zero knowledge proofs; hardware security and AI; and network security, authentication, and privacy.