

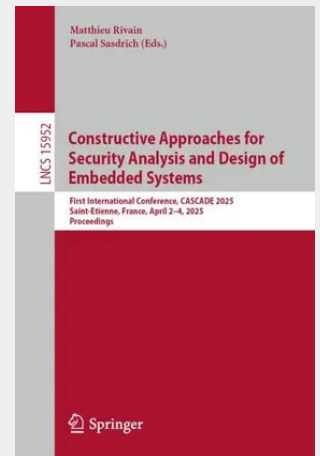
Constructive Approaches for Security Analysis and Design of Embedded Systems

First International Conference, CASCADE 2025, Saint-Etienne, France, April 2-4, 2025, Proceedings

This book constitutes the refereed proceedings of the First International Conference on Constructive Approaches for Security Analysis and Design of Embedded Systems, CASCADE 2025, held in Saint-Etienne, France, during April 2–4, 2025.

The 24 full papers included in this book were carefully reviewed and selected from 51 submissions. They are organized in topical sections as follows: Attacks on Symmetric Cryptography; Side-Channel Attacks; Physical Security; RISC-V ; Machine Learning; Attacks on Post-Quantum Cryptography; Securing Post-Quantum Cryptography; Homomorphic Encryption and White-Box Cryptography; Attacks on Symmetric Cryptography; Side-Channel Attacks; Physical Security; RISC-V; and Machine Learning.

..Attacks on Symmetric Cryptography..- The Dangerous Message/Key Swap in HMAC..- Practical Second-Order CPA Attack on Ascon with Proper SelectionFunction..- Side-Channel Attacks..- On the Success Rate of Simple Side-Channel Attacks against Maskingwith Unlimited Attack Traces..- A Comparison of Graph-Inference Side-Channel Attacks Against SKINNY. .- Physical Security..- Robust and Reliable PUF Protocol Exploiting Non-MonotonicQuantization and Neyman-Pearson Lemma..- Towards Package Opening Detection at Power-up by MonitoringThermal Dissipation..- Partial Key Overwrite Attacks in Microcontrollers: a Survey..- RISC-V..- Combined Masking and Shuffling for Side-Channel Secure Ascon onRISC-V..- A Hardware Design Methodology to Prevent MicroarchitecturalTransition Leakages..- Machine Learning..- Taking AI-Based Side-Channel Attacks to a New Dimension..- Avenger Ensemble: Genetic Algorithm-Driven Ensemble Selection forDeep Learning-based Side-Channel Analysis..- Improving Leakage Exploitability in Horizontal Side Channel Attacksthrough Anomaly Mitigation with Unsupervised Neural Networks..- Profiling Side-Channel Attack on HQC Polynomial MultiplicationUsing Machine Learning Methods..- Attacks on Post-Quantum Cryptography..- Simple Power Analysis assisted Chosen Cipher-Text Attack on ML-KEM..- A Horizontal Attack on the Codes and Restricted Objects SignatureScheme (CROSS)..- Vladimir Sarde and Nicolas Debande..- Message-Recovery Horizontal Correlation Attack on Classic McEliece..- Breaking HuFu with 0 Leakage: A Side-Channel Analysis..- Securing Post-Quantum Cryptography..- X2X: Low-Randomness and High-Throughput A2B and B2Aconversions for d+1 shares in Hardware..- Area Efficient Polynomial Arithmetic Accelerator for Post-QuantumDigital Signatures and KEMs..- Efficient Error Detection Methods for the Number Theoretic Transformsin Lattice-Based Algorithms..- A Fault-Resistant NTT by Polynomial Evaluation and Interpolation..- Homomorphic Encryption and White-Box Cryptography..- Hybrid Homomorphic Encryption Resistance to Side-channel Attacks..- White-Box Implementation Techniques for the HFE Family.



79,17 €

73,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783032014047

Medium: Buch

ISBN: 978-3-032-01404-7

Verlag: Birkhäuser

Erscheinungstermin: 21.10.2025

Sprache(n): Englisch

Auflage: Erscheinungsjahr 2025

Serie: Lecture Notes in Computer Science

Produktform: Kartoniert

Gewicht: 920 g

Seiten: 604

Format (B x H): 155 x 235 mm

