1. Record Nr. UNINA9910410056003321

Titolo	Smart Card Research and Advanced Applications : 18th International Conference, CARDIS 2019, Prague, Czech Republic, November 11–13, 2019, Revised Selected Papers / / edited by Sonia Belaïd, Tim Güneysu
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2020
ISBN	3-030-42068-X
Edizione	[1st ed. 2020.]
Descrizione fisica	1 online resource (X, 269 p. 106 illus., 50 illus. in color.)
Collana	Security and Cryptology ; ; 11833
Disciplina	005.82 006.246
Soggetti	Data encryption (Computer science) Computer security Application software Computer communication systems Microprogramming Cryptology Systems and Data Security Information Systems Applications (incl. Internet) Computer Communication Networks Control Structures and Microprogramming
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	System-on-a-Chip Security -- In-situ Extraction of Randomness from Computer Architecture through Hardware Performance Counters -- Optimized Threshold Implementations: Securing Cryptographic Accelerators for Low-Latency and Low-Energy Applications -- Breaking the Lightweight Secure PUF: Understanding the Relation of Input Transformations and Machine Learning Resistance -- Post-Quantum Cryptography -- Improving Speed of Dilithium's Signing Procedure -- An efficient and provable masked implementation of qtesla -- Side-Channel Analysis -- Side-channel attacks on blinded scalar multiplications revisited -- Remote Side-Channel Attacks on Heterogeneous SoC -- Optimal Collision Side-Channel Attacks --

Microarchitectural Attacks -- A Bit-Level Approach to Side Channel Based Disassembling -- CCCiCC: A Cross-core Cache-independent Covert Channel on AMD Family 15h CPUs -- Design Considerations for EM Pulse Fault Injection -- Cryptographic Primitives -- Lightweight MACs from Universal Hash Functions -- FELICS-AEAD: Benchmarking of Lightweight Authenticated Encryption Algorithms -- Advances in Side-Channel Analysis -- A Comparison of Chi^2-Test and Mutual Information as Distinguisher for Side-Channel Analysis -- Key Enumeration from the Adversarial Viewpoint. When to Stop Measuring and Start Enumerating?.

Sommario/riassunto

This book constitutes the thoroughly refereed post-conference proceedings of the 18th International Conference on Smart Card Research and Advanced Applications, CARDIS 2019, held in Prague, Czech Republic, in November 2019. The 15 revised full papers presented in this book were carefully reviewed and selected from 31 submissions. The papers are organized in the following topical sections: system-on-a-chip security; post-quantum cryptography; side-channel analysis; microarchitectural attacks; cryptographic primitives; advances in side-channel analysis. CARDIS has provided a space for security experts from industry and academia to exchange on security of smart cards and related applications.