1. Record Nr. UNINA9910337572803321

Titolo	Smart Card Research and Advanced Applications : 17th International Conference, CARDIS 2018, Montpellier, France, November 12–14, 2018, Revised Selected Papers / / edited by Begül Bilgin, Jean-Bernard Fischer
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2019
ISBN	3-030-15462-9
Edizione	[1st ed. 2019.]
Descrizione fisica	1 online resource (X, 201 p. 135 illus., 59 illus. in color.)
Collana	Security and Cryptology, , 2946-1863 ; ; 11389
Disciplina	006.246
Soggetti	Cryptography Data encryption (Computer science) Data protection Cryptology Data and Information Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Convolutional Neural Network based Side-Channel Attacks in Time-Frequency Representations -- A Systematic Study of the Impact of Graphical Models on Inference-based Attacks on AES -- Improving Side-channel Analysis through Semi-supervised Learning -- Non-profiled Mask Recovery: the impact of Independent Component Analysis -- How (not) to Use Welch’s T-test in Side-Channel Security Evaluations -- Scalable Key Rank Estimation (and Key Enumeration) Algorithm for Large Keys -- Shorter Messages and Faster Post-Quantum Encryption with Round5 on Cortex M -- Yet Another Size Record for AES: A First-Order SCA Secure AES S-box Based on GF(28) Multiplication -- Jitter Estimation with High Accuracy for Oscillator-Based TRNGs -- Electromagnetic Activity vs. Logical Activity : Near Field Scans for Reverse Engineering -- An In-depth and Black-Box Characterization of the Effects of Laser Pulses on ATmega328P -- Breaking all the Things — A Systematic Survey of Firmware Extraction Techniques for IoT Devices -- Exploiting JCVM on smart cards using forged references in the API calls.

Sommario/riassunto

This book constitutes the thoroughly refereed post-conference proceedings of the 17th International Conference on Smart Card Research and Advanced Applications, CARDIS 2018, held in Monpellier, France, in November 2018. The 13 revised full papers presented in this book were carefully reviewed and selected from 28 submissions. CARDIS has provided a space for security experts from industry and academia to exchange on security of smart cards and related applications.