1.

Record Nr.	UNINA9910847598403321
Autore	Homma Naofumi
Titolo	Constructive Side-Channel Analysis and Secure Design [[electronic resource]] : 15th International Workshop, COSADE 2024, Gardanne, France, April 9–10, 2024, Proceedings / / by Romain Wacquez ; edited by Naofumi Homma
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
ISBN	3-031-57543-1
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (285 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14595
Altri autori (Persone)	WacquezRomain
Disciplina	005.8
Soggetti	Data protection Computers - Law and legislation Information technology - Law and legislation Computer networks Computers, Special purpose Computer systems Microprogramming Data and Information Security Legal Aspects of Computing Computer Communication Networks Special Purpose and Application-Based Systems Computer System Implementation Control Structures and Microprogramming
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Analyses and Tools -- Characterizing and Modeling Synchronous Clock-Glitch Fault Injection -- On-chip evaluation of voltage drops and fault occurrence induced by Si backside EM injection -- EFFLUX-F2: A high performance hardware security evaluation board -- Attack Methods -- Practical Improvements to Statistical Ineffective Fault Attacks -- CAPABARA: A Combined Attack on CAPA -- Deep-Learning-Based Side-Channel Attacks -- Exploring Multi-Task Learning in the Context of Masked AES Implementations -- The Need for MORE:

Unsupervised Side-channel Analysis with Single Network Training and Multi-output Regression -- Towards Private Deep Learning-Based Side-Channel Analysis using Homomorphic Encryption -- PUF/RNG -- Leakage Sources of the ICLooPUF: Analysis of a Side-Channel Protected Oscillator-Based PUF -- Impact of Process Mismatch and Device Aging on SR-Latch Based True Random Number Generators -- Lightweight Leakage-Resilient PRNG from TBCs using Superposition -- Cryptographic Implementations -- The Impact of Hash Primitives and Communication Overhead for Hardware-Accelerated SPHINCS+ -- HaMAYO: A Fault-Tolerant Reconfigurable Hardware Implementation of the MAYO Signature Scheme -- Combining Loop Shuffling and Code Polymorphism for Enhanced AES Side-Channel Security.

Sommario/riassunto

This book constitutes the refereed proceedings of the 15th International Workshop on Constructive Side-Channel Analysis and Secure Design, COSADE 2024, held in Gardanne, France, during April 9–10, 2024. The 14 full papers included in this book were carefully reviewed and selected from 42 submissions. They were organized in topical sections as follows: Analyses and Tools; Attack Methods; Deep-Learning-Based Side-Channel Attacks; PUF/RNG; and Cryptographic Implementations.