1. Record Nr. UNISA996517752103316

Titolo	Constructive side-channel analysis and secure design : 14th international workshop, COSADE 2023, Munich, Germany, April 3-4, 2023, proceedings / / edited by Elif Bilge Kavun and Michael Pehl
Pubbl/distr/stampa	Cham, Switzerland : , : Springer Nature Switzerland AG, , [2023] ©2023
ISBN	3-031-29497-1
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (268 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 13979
Disciplina	005.8
Soggetti	Computer security Data encryption (Computer science)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Fault-Injection Analyses and Countermeasures -- SAMVA: Static Analysis for Multi-Fault Attack Paths Determination -- Efficient attack-surface exploration for electromagnetic fault injection -- A CCFI verification scheme based on the RISC-V Trace Encoder -- Side-Channel Analyses and Countermeasures -- ASCA vs. SASCA - A closer look at the AES key schedule -- Removing the Field Size Loss from Duc et al.’s Conjectured Bound for Masked Encodings -- Improving Side-channel Leakage Assessment using Pre-silicon Leakage Models -- Attacks on PQC and Countermeasures -- Fast First-Order Masked NTTRU -- On the Feasibility of Single-Trace Attacks on the CDT Gaussian Sampler in FrodoKEM -- Punctured Syndrome Decoding Problem: Efficient Side-Channel Attacks Against Classic McEliece -- Analyses and Tools -- Energy Consumption of Protected Cryptographic Hardware Cores - An Experimental Study -- Whiteboxgrind - Automated Analysis of Whitebox Cryptography -- White-box cryptography with global device binding from message recoverable signatures and token-based obfuscation.
Sommario/riassunto	This book constitutes the refereed proceedings of the 14th International Workshop on Constructive Side-Channel Analysis and Secure Design, COSADE 2023, held in Munich, Germany, during April 3–

4, 2023. The 12 full papers included in this book were carefully reviewed and selected from 28 submissions. They were organized in topical sections as follows: fault-injection analyses and countermeasures; side-channel analyses and countermeasures; attacks on PQC and countermeasure; and analyses and tools.