1.

Record Nr.	UNINA9910647396303321
Titolo	Smart Card Research and Advanced Applications : 21st International Conference, CARDIS 2022, Birmingham, UK, November 7–9, 2022, Revised Selected Papers / / edited by Ileana Buhan, Tobias Schneider
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2023
ISBN	9783031253195 3031253191
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (311 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 13820
Disciplina	332.76
Soggetti	Cryptography Data encryption (Computer science) Computer networks Computer systems Coding theory Information theory Computer networks - Security measures Computer science - Mathematics Cryptology Computer Communication Networks Computer System Implementation Coding and Information Theory Mobile and Network Security Mathematics of Computing
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Physical Attacks -- Time’s a Thief of Memory: Breaking Multi-tenant Isolation in TrustZones through Timing based Bidirectional Covert Channels -- Combined Fault Injection and Real-Time Side-Channel Analysis for Android Secure-Boot Bypassing -- A Practical Introduction to Side-Channel Extraction of Deep Neural Network Parameters -- Physical Countermeasures -- A Nearly Tight Proof of Duc et al.s

Conjectured Security Bound for Masked Implementations -- Short-Iteration Constant-Time GCD and Modular Inversion -- Protecting AES -- Guarding the First Order: The Rise of AES Maskings -- Rivain-Prouff on Steroids: Faster and Stronger Masking of the AES -- Self-Timed Masking: Implementing Masked S-Boxes Without Registers -- Evaluation Methodologies -- An Evaluation Procedure for Comparing Clock Jitter Measurement Methods -- Comparing Key Rank Estimation Methods -- Cycle-Accurate Power Side-Channel Analysis Using the ChipWhisperer: a Case Study on Gaussian Sampling -- Attacking NTRU -- Reveal the Invisible Secret: Chosen-Ciphertext Side-Channel Attacks on NTRU -- Security Assessment of NTRU Against Non-Profiled SCA -- Next-Generation Cryptography -- Post-Quantum Protocols for Banking Applications -- Analyzing the Leakage Resistance of the NIST’s Lightweight Crypto Competition’s Finalists.

Sommario/riassunto

This book constitutes the proceedings of the 21st International Conference on Smart Card Research and Advanced Applications, CARDIS 2022, which took place in November 2022. The conference took place in Birmingham, United Kingdom. The 15 full papers presented in this volume were carefully reviewed and selected from 29 submissions. They were organized in topical sections named: physical attacks; physical countermeasures; protecting AES; evaluation methodologies; attacking NTRU; next-generation cryptography.