

1. Record Nr.	UNISALENTO991002205529707536
Titolo	Measure theory Oberwolfach 1979 [e-book] : proceedings of the conference held at Oberwolfach, Germany, July 1–7, 1979 / edited by Dietrich Kölzow
Pubbl/distr/stampa	Berlin : Springer, 1980
ISBN	9783540392217
Descrizione fisica	1 online resource (xviii, 574 p.)
Collana	Lecture Notes in Mathematics, 0075-8434 ; 794
Classificazione	AMS 28-02 AMS 46G AMS 60-02
Altri autori (Persone)	Kölzow, Dietrich
Disciplina	515.8
Soggetti	Mathematics
Lingua di pubblicazione	Inglese
Formato	Risorsa elettronica
Livello bibliografico	Monografia

2. Record Nr.	UNINA9910484597903321
Titolo	Smart Card Research and Advanced Applications : 19th International Conference, CARDIS 2020, Virtual Event, November 18–19, 2020, Revised Selected Papers // edited by Pierre-Yvan Liardet, Nele Mentens
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2021
ISBN	3-030-68487-3
Edizione	[1st ed. 2021.]
Descrizione fisica	1 online resource (X, 197 p. 51 illus., 30 illus. in color.)
Collana	Security and Cryptology, , 2946-1863 ; ; 12609
Disciplina	006
Soggetti	Cryptography Data encryption (Computer science) Data protection Computers, Special purpose Application software Computer networks Cryptology Data and Information Security Special Purpose and Application-Based Systems Computer and Information Systems Applications Computer Communication Networks
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Post-Quantum Cryptography -- A Constant Time Full Hardware Implementation of Streamlined NTRU Prime -- Lightweight Post-Quantum Key Encapsulation for 8-bit AVR Microcontrollers -- Classic McEliece Implementation with Low Memory Footprint -- Efficient Implementations -- A Fast and Compact RISC-V Accelerator for Ascon and Friends -- Optimized Software Implementations for the Lightweight Encryption Scheme ForkAE -- Secure and Efficient Delegation of Pairings with Online Inputs -- Physical Attacks -- On the Security of Off-the-Shelf Microcontrollers: Hardware is not Enough -- A Power Side-Channel Attack on the CCA2-Secure HQC KEM -- How Deep Learning Helps Compromising USIM -- Differential Analysis and

Fingerprinting of ZombieLoads on Block Ciphers -- Low-Cost Body
Biasing Injection (BBI) Attacks on WLCSP Devices -- Let's Tessellate:
Tiling for Security Against Advanced Probe and Fault Adversaries.

Sommario/riassunto

This book constitutes the proceedings of the 19th International Conference on Smart Card Research and Advanced Applications, CARDIS 2020, which took place during November 18-20, 2020. The conference was originally planned to take place in Lübeck, Germany, and changed to an online format due to the COVID-19 pandemic. The 12 full papers presented in this volume were carefully reviewed and selected from 26 submissions. They were organized in topical sections named: post-quantum cryptography; efficient implementations; and physical attacks.
