1.	Record Nr.	UNINA9910484022703321
	Titolo	Cryptographic ahrdware and embedded systems, CHES 2008 : 10th International Workshop, Washington, D.C., USA, August 10-13, 2008 : proceedings / / Edited by Elisabeth Oswald and Pankaj Rohatgi
	Pubbl/distr/stampa	Berlin, Germany ; ; New York, New York : , : Springer, , [2008] ©2008
	ISBN	3-540-85053-8
	Edizione	[1st ed. 2008.]
	Descrizione fisica	1 online resource (XIII, 445 p.)
	Collana	Security and Cryptology ; ; 5154
	Disciplina	005.82
	Soggetti	Computer science Computers, Special purpose Computer networks
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Includes index.
	Nota di bibliografia	Includes bibliographical references and author index.
	Nota di contenuto	Side-Channel Analysis 1 -- Attack and Improvement of a Secure S-Box Calculation Based on the Fourier Transform -- Collision-Based Power Analysis of Modular Exponentiation Using Chosen-Message Pairs -- Multiple-Differential Side-Channel Collision Attacks on AES -- Implementations 1 -- Time-Area Optimized Public-Key Engines: -Cryptosystems as Replacement for Elliptic Curves? -- Ultra High Performance ECC over NIST Primes on Commercial FPGAs -- Exploiting the Power of GPUs for Asymmetric Cryptography -- Fault Analysis 1 -- High-Performance Concurrent Error Detection Scheme for AES Hardware -- A Lightweight Concurrent Fault Detection Scheme for the AES S-Boxes Using Normal Basis -- RSA with CRT: A New Cost-Effective Solution to Thwart Fault Attacks -- Random Number Generation -- A Design for a Physical RNG with Robust Entropy Estimators -- Fast Digital TRNG Based on Metastable Ring Oscillator -- Efficient Helper Data Key Extractor on FPGAs -- Side-Channel Analysis 2 -- The Carry Leakage on the Randomized Exponent Countermeasure -- Recovering Secret Keys from Weak Side Channel Traces of Differing Lengths -- Attacking State-of-the-Art Software Countermeasures—A Case Study for AES -- Cryptography and Cryptanalysis -- Binary Edwards Curves -- A Real-World Attack Breaking A5/1 within Hours -- Hash Functions and

RFID Tags: Mind the Gap -- Implementations 2 -- A New Bit-Serial Architecture for Field Multiplication Using Polynomial Bases -- A Very Compact Hardware Implementation of the MISTY1 Block Cipher -- Light-Weight Instruction Set Extensions for Bit-Sliced Cryptography -- Fault Analysis 2 -- Power and Fault Analysis Resistance in Hardware through Dynamic Reconfiguration -- RFID and Its Vulnerability to Faults -- Perturbating RSA Public Keys: An Improved Attack -- Side-Channel Analysis 3 -- Divided Backend Duplication Methodology for Balanced Dual Rail Routing -- Using Subspace-Based Template Attacks to Compare and Combine Power and Electromagnetic Information Leakages -- Mutual Information Analysis -- Invited Talks -- RSA—Past, Present, Future -- A Vision for Platform Security.

Sommario/riassunto

This book constitutes the refereed proceedings of the 10th Interntaional Workshop on Cryptographic Hardware and Embedded Systems, CHES 2008, held in Washington, D.C., USA, during August 10-13, 2008. The book contains 2 invited talks and 27 revised full papers which were carefully reviewed and selected from 107 submissions. The papers are organized in topical sections on side channel analysis, implementations, fault analysis, random number generation, and cryptography and cryptanalysis.