1. Record Nr. UNINA9910484204303321

Titolo	Cryptographic Hardware and Embedded Systems -- CHES 2010 : 12th International Workshop, Santa Barbara, USA, August 17-20,2010, Proceedings / / edited by Stefan Mangard, Francois-Xavier Standaert
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2010
ISBN	3-642-15031-4
Edizione	[1st ed. 2010.]
Descrizione fisica	1 online resource (XIII, 458 p. 142 illus.)
Collana	Security and Cryptology, , 2946-1863 ; ; 6225
Altri autori (Persone)	MangardStefan StandaertFrancois-Xavier
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Coding theory Information theory Data structures (Computer science) Data protection Algorithms Computer science - Mathematics Discrete mathematics Cryptology Coding and Information Theory Data Structures and Information Theory Data and Information Security Discrete Mathematics in Computer Science
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Low Cost Cryptography -- Quark: A Lightweight Hash -- PRINTcipher: A Block Cipher for IC-Printing -- Sponge-Based Pseudo-Random Number Generators -- Efficient Implementations I -- A High Speed Coprocessor for Elliptic Curve Scalar Multiplications over -- Co-Z Addition Formulæ and Binary Ladders on Elliptic Curves -- Efficient Techniques for High-Speed Elliptic Curve Cryptography -- Side-

Channel Attacks and Countermeasures I -- Analysis and Improvement of the Random Delay Countermeasure of CHES 2009 -- New Results on Instruction Cache Attacks -- Correlation-Enhanced Power Analysis Collision Attack -- Side-Channel Analysis of Six SHA-3 Candidates -- Tamper Resistance and Hardware Trojans -- Flash Memory 'Bumping' Attacks -- Self-referencing: A Scalable Side-Channel Approach for Hardware Trojan Detection -- When Failure Analysis Meets Side-Channel Attacks -- Efficient Implementations II -- Fast Exhaustive Search for Polynomial Systems in -- 256 Bit Standardized Crypto for 650 GE – GOST Revisited -- Mixed Bases for Efficient Inversion in and Conversion Matrices of SubBytes of AES -- SHA-3 -- Developing a Hardware Evaluation Method for SHA-3 Candidates -- Fair and Comprehensive Methodology for Comparing Hardware Performance of Fourteen Round Two SHA-3 Candidates Using FPGAs -- Performance Analysis of the SHA-3 Candidates on Exotic Multi-core Architectures -- XBX: eXternal Benchmarking eXtension for the SUPERCOP Crypto Benchmarking Framework -- Fault Attacks and Countermeasures -- Public Key Perturbation of Randomized RSA Implementations -- Fault Sensitivity Analysis -- PUFs and RNGs -- An Alternative to Error Correction for SRAM-Like PUFs -- New High Entropy Element for FPGA Based True Random Number Generators -- The Glitch PUF: A New Delay-PUF Architecture Exploiting Glitch Shapes.-New Designs -- Garbled Circuits for Leakage-Resilience: Hardware Implementation and Evaluation of One-Time Programs -- ARMADILLO: A Multi-purpose Cryptographic Primitive Dedicated to Hardware -- Side-Channel Attacks and Countermeasures II -- Provably Secure Higher-Order Masking of AES -- Algebraic Side-Channel Analysis in the Presence of Errors -- Coordinate Blinding over Large Prime Fields.

Sommario/riassunto

This book constitutes the refereed proceedings of the 12th International Workshop on Cryptographic Hardware and Embedded Systems, CHES 2010, held in Santa Barbara, USA during August 17-20, 2010. This year it was co-located with the 30th International Cryptology Conference (CRYPTO). The book contains 2 invited talks and 30 revised full papers which were carefully reviewed and selected from 108 submissions. The papers are organized in topical sections on low cost cryptography, efficient implementation, side-channel attacks and countermeasures, tamper resistance, hardware trojans, PUFs and RNGs.