1. Record Nr. UNINA9910482972503321

Titolo	Cryptographic hardware and embedded systems - CHES 2009 : 11th international workshop Lausanne, Switzerland, September 6-9, 2009 proceedings / / Christophe Clavier, Kris Gaj (eds.)
Pubbl/distr/stampa	Berlin ; ; Heidelberg, : Springer-Verlag, 2009
ISBN	3-642-04138-8
Edizione	[1st ed. 2009.]
Descrizione fisica	1 online resource (XVI, 472 p.)
Collana	Lecture notes in computer science, , 0302-9743 ; ; 5747
Classificazione	DAT 130f DAT 260f DAT 465f SS 4800
Altri autori (Persone)	ClavierChristophe GajKris
Disciplina	005.8/2
Soggetti	Data encryption (Computer science) Cryptography
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	Software Implementations -- Faster and Timing-Attack Resistant AES-GCM -- Accelerating AES with Vector Permute Instructions -- SSE Implementation of Multivariate PKCs on Modern x86 CPUs -- MicroEliece: McEliece for Embedded Devices -- Invited Talk 1 -- Physical Unclonable Functions and Secure Processors -- Side Channel Analysis of Secret Key Cryptosystems -- Practical Electromagnetic Template Attack on HMAC -- First-Order Side-Channel Attacks on the Permutation Tables Countermeasure -- Algebraic Side-Channel Attacks on the AES: Why Time also Matters in DPA -- Differential Cluster Analysis -- Side Channel Analysis of Public Key Cryptosystems -- Known–Plaintext–Only Attack on RSA–CRT with Montgomery Multiplication -- A New Side-Channel Attack on RSA Prime Generation -- Side Channel and Fault Analysis Countermeasures -- An Efficient Method for Random Delay Generation in Embedded Software -- Higher-Order Masking and Shuffling for Software Implementations of Block Ciphers -- A Design Methodology for a DPA-Resistant Cryptographic LSI with RSL Techniques -- A Design Flow and Evaluation

Framework for DPA-Resistant Instruction Set Extensions -- Invited Talk 2 -- Crypto Engineering: Some History and Some Case Studies -- Pairing-Based Cryptography -- Hardware Accelerator for the Tate Pairing in Characteristic Three Based on Karatsuba-Ofman Multipliers -- Faster -Arithmetic for Cryptographic Pairings on Barreto-Naehrig Curves -- Designing an ASIP for Cryptographic Pairings over Barreto-Naehrig Curves -- New Ciphers and Efficient Implementations -- KATAN and KTANTAN — A Family of Small and Efficient Hardware-Oriented Block Ciphers -- Programmable and Parallel ECC Coprocessor Architecture: Tradeoffs between Area, Speed and Security -- Elliptic Curve Scalar Multiplication Combining Yao's Algorithm and Double Bases -- TRNGs and Device Identification -- The Frequency Injection Attack on Ring-Oscillator-Based True Random Number Generators -- Low-Overhead Implementation of a Soft Decision Helper Data Algorithm for SRAM PUFs -- CDs Have Fingerprints Too -- Invited Talk 3 -- The State-of-the-Art in IC Reverse Engineering -- Hot Topic Session: Hardware Trojans and Trusted ICs -- Trojan Side-Channels: Lightweight Hardware Trojans through Side-Channel Engineering -- MERO: A Statistical Approach for Hardware Trojan Detection -- Theoretical Aspects -- On Tamper-Resistance from a Theoretical Viewpoint -- Mutual Information Analysis: How, When and Why? -- Fault Analysis -- Fault Attacks on RSA Signatures with Partially Unknown Messages -- Differential Fault Analysis on DES Middle Rounds.

Sommario/riassunto

This book constitutes the refereed proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems, CHES 2009, held in Lausanne, Switzerland during September 6-9, 2009. The book contains 3 invited talks and 29 revised full papers which were carefully reviewed and selected from 148 submissions. The papers are organized in topical sections on software implementations, side channel analysis of secret key cryptosystems, side channel analysis of public key cryptosystems, side channel and fault analysis countermeasures, pairing-based cryptography, new ciphers and efficient implementations, TRNGs and device identification, hardware trojans and trusted ICs, theoretical aspects, and fault analysis.