1. Record Nr. UNINA9910484964003321

Titolo	Cryptographic Hardware and Embedded Systems - CHES 2007 : 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings / / edited by Pascal Paillier, Ingrid Verbauwhede
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2007
ISBN	3-540-74735-4
Edizione	[1st ed. 2007.]
Descrizione fisica	1 online resource (XIV, 468 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 4727
Disciplina	004.16
Soggetti	Cryptography Data encryption (Computer science) Computer networks Computers, Special purpose Logic design Operating systems (Computers) Electronic data processing - Management Cryptology Computer Communication Networks Special Purpose and Application-Based Systems Logic Design Operating Systems IT Operations
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Differential and Higher Order Attacks -- A First-Order DPA Attack Against AES in Counter Mode with Unknown Initial Counter -- Gaussian Mixture Models for Higher-Order Side Channel Analysis -- Side Channel Cryptanalysis of a Higher Order Masking Scheme -- Random Number Generation and Device Identification -- High-Speed True Random Number Generation with Logic Gates Only -- FPGA Intrinsic PUFs and Their Use for IP Protection -- Logic Styles: Masking and Routing -- Evaluation of the Masked Logic Style MDPL on a Prototype

Chip -- Masking and Dual-Rail Logic Don’t Add Up -- DPA-Resistance Without Routing Constraints? -- Efficient Algorithms for Embedded Processors -- On the Power of Bitslice Implementation on Intel Core2 Processor -- Highly Regular Right-to-Left Algorithms for Scalar Multiplication -- MAME: A Compression Function with Reduced Hardware Requirements -- Collision Attacks and Fault Analysis -- Collision Attacks on AES-Based MAC: Alpha-MAC -- Secret External Encodings Do Not Prevent Transient Fault Analysis -- Two New Techniques of Side-Channel Cryptanalysis -- High Speed AES Implementations -- AES Encryption Implementation and Analysis on Commodity Graphics Processing Units -- Multi-gigabit GCM-AES Architecture Optimized for FPGAs -- Public-Key Cryptography -- Arithmetic Operators for Pairing-Based Cryptography -- FPGA Design of Self-certified Signature Verification on Koblitz Curves -- How to Maximize the Potential of FPGA Resources for Modular Exponentiation -- Implementation Cost of Countermeasures -- TEC-Tree: A Low-Cost, Parallelizable Tree for Efficient Defense Against Memory Replay Attacks -- Power Analysis Resistant AES Implementation with Instruction Set Extensions -- Security Issues for RF and RFID -- Power and EM Attacks on Passive RFID Devices -- RFID Noisy Reader How toPrevent from Eavesdropping on the Communication? -- RF-DNA: Radio-Frequency Certificates of Authenticity -- Special Purpose Hardware for Cryptanalysis -- CAIRN 2: An FPGA Implementation of the Sieving Step in the Number Field Sieve Method -- Collision Search for Elliptic Curve Discrete Logarithm over GF(2 m) with FPGA -- A Hardware-Assisted Realtime Attack on A5/2 Without Precomputations -- Side Channel Analysis -- Differential Behavioral Analysis -- Information Theoretic Evaluation of Side-Channel Resistant Logic Styles -- Problems and Solutions for Lightweight Devices -- On the Implementation of a Fast Prime Generation Algorithm -- PRESENT: An Ultra-Lightweight Block Cipher -- Cryptographic Hardware and Embedded Systems - CHES 2007.

Sommario/riassunto

CHES2007,theninthworkshoponCryptographicHardwareandEmbeddedS-tems, was sponsored by the International Association for Cryptologic Research (IACR) and held in Vienna, Austria, September 10–13, 2007. The workshop - ceived 99 submissions from 24 countries, of which the Program Committee (39 members from 15 countries) selected 31 for presentation. For the ?rst time in the history of CHES, each submission was reviewed by at least four reviewers instead of three (and at least ? ve for submissions by PC members, those now being limited to two per member) and many submitted papers have received plenty of extra reviews (some papers received up to nine reviews), thus totalling the unprecedented record of 483 reviews overall. Thepaperscollectedinthisvolumerepresentcutting-edgeworldwideresearch in the rapidly evolving ?elds of crypto-hardware, fault-based and side-channel cryptanalysis, and embedded cryptography, at the crossing of academic and - dustrial research. The wide diversity of subjects appearing in these proceedings covers virtually all related areas and shows our e?orts to extend the scope of CHES more than usual. Although a relatively young workshop, CHES is now ?rmlyestablishedasascienti? ceventofreferenceappreciatedbymoreandmore renowned experts of theory and practice: many high-quality works were subm- ted, all of which, sadly, could not be accepted. Selecting from so many good worksis no easy task and our deepest thanks go to the members of the Program Committee for their involvement, excellence, and team spirit. We are grateful to the numerous external reviewers listed below for their expertise and assistance in our deliberations.