1. Record Nr. UNISA996465429303316

Titolo	Cryptographic Hardware and Embedded Systems - CHES 2004 [[electronic resource]] : 6th International Workshop Cambridge, MA, USA, August 11-13, 2004, Proceedings / / edited by Marc Joye, Jean-Jaques Quisquater
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2004
ISBN	3-540-28632-2
Edizione	[1st ed. 2004.]
Descrizione fisica	1 online resource (XIV, 462 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 3156
Disciplina	005.8
Soggetti	Data encryption (Computer science) Computer communication systems Special purpose computers Logic design Operating systems (Computers) Management information systems Computer science Cryptology Computer Communication Networks Special Purpose and Application-Based Systems Logic Design Operating Systems Management of Computing and Information Systems
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 at the end of each chapters and index.
Nota di contenuto	Side Channels I -- Towards Efficient Second-Order Power Analysis -- Correlation Power Analysis with a Leakage Model -- Power Analysis of an FPGA -- Modular Multiplication -- Long Modular Multiplication for Cryptographic Applications -- Leak Resistant Arithmetic -- Efficient Linear Array for Multiplication in GF(2 m) Using a Normal Basis for Elliptic Curve Cryptography -- Low Resources I -- Low-Power Elliptic

Curve Cryptography Using Scaled Modular Arithmetic -- A Low-Cost ECC Coprocessor for Smartcards -- Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs -- Implementation Aspects -- Instruction Set Extensions for Fast Arithmetic in Finite Fields GF(p) and GF(2 m) -- Aspects of Hyperelliptic Curves over Large Prime Fields in Software Implementations -- Collision Attacks -- A Collision-Attack on AES -- Enhancing Collision Attacks -- Side Channels II -- Simple Power Analysis of Unified Code for ECC Double and Add -- DPA on n-Bit Sized Boolean and Arithmetic Operations and Its Application to IDEA, RC6, and the HMAC-Construction -- Side-Channel Attacks in ECC: A General Technique for Varying the Parametrization of the Elliptic Curve -- Switching Blindings with a View Towards IDEA -- Fault Attacks -- Fault Analysis of Stream Ciphers -- A Differential Fault Attack Against Early Rounds of (Triple-)DES -- Hardware Implementation I -- An Offset-Compensated Oscillator-Based Random Bit Source for Security Applications -- Improving the Security of Dual-Rail Circuits -- Side Channels III -- A New Attack with Side Channel Leakage During Exponent Recoding Computations -- Defeating Countermeasures Based on Randomized BSD Representations -- Pipelined Computation of Scalar Multiplication in Elliptic Curve Cryptosystems -- Efficient Countermeasures against RPA, DPA, and SPA -- Low Resources II -- Strong Authentication for RFID Systems Using the AES Algorithm -- TTS: High-Speed Signatures on a Low-Cost Smart Card -- Hardware Implementation II -- XTR Implementation on Reconfigurable Hardware -- Concurrent Error Detection Schemes for Involution Ciphers -- Authentication and Signatures -- Public Key Authentication with One (Online) Single Addition -- Attacking DSA Under a Repeated Bits Assumption -- How to Disembed a Program?.

Sommario/riassunto

These are the proceedings of CHES 2004, the 6th Workshop on Cryptographic Hardware and Embedded Systems. For the first time, the CHES Workshop was sponsored by the International Association for Cryptologic Research (IACR). This year, the number of submissions reached a new record. One hundred and twenty-five papers were submitted, of which 32 were selected for presentation. Each submitted paper was reviewed by at least 3 members of the program committee. We are very grateful to the program committee for their hard and efficient work in assembling the program. We are also grateful to the 108 external referees who helped in the review process in their area of expertise. In addition to the submitted contributions, the program included three - invited talks, by Neil Gershenfeld (Center for Bits and Atoms, MIT) about “Physical Information Security”, by Isaac Chuang (Medialab, MIT) about “Quantum Cryptography”, and by Paul Kocher (Cryptography Research) about “Phy- cal Attacks”. It also included a rump session, chaired by Christof Paar, which featured informal talks on recent results. As in the previous years, the workshop focused on all aspects of cryptographic hardware and embedded system security. We sincerely hope that the CHES Workshop series will remain a premium forum for intellectual exchange in this area.