1. Record Nr. UNINA9910143609103321

Titolo	Cryptographic Hardware and Embedded Systems - CHES 2000 [[electronic resource]] : Second International Workshop Worcester, MA, USA, August 17-18, 2000 Proceedings / / edited by Cetin K. Koc, Christof Paar
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2000
ISBN	3-540-44499-8
Edizione	[1st ed. 2000.]
Descrizione fisica	1 online resource (XII, 360 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 1965
Disciplina	005.8/2
Soggetti	Data encryption (Computer science) Computer communication systems Special purpose computers Logic design Computer science—Mathematics Cryptology Computer Communication Networks Special Purpose and Application-Based Systems Logic Design 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	Invited Talk -- Software Implementation of Elliptic Curve Cryptography over Binary Fields -- Implementation of Elliptic Curve Cryptosystems -- Implementation of Elliptic Curve Cryptographic Coprocessor over GF (2m) on an FPGA -- A High-Performance Reconfigurable Elliptic Curve Processor for GF(2m) -- Fast Implementation of Elliptic Curve Defined over GF(pm) on CalmRISC with MAC2424 Coprocessor -- Power and Timing Analysis Attacks -- Protecting Smart Cards from Passive Power Analysis with Detached Power Supplies -- Smartly Analyzing the Simplicity and the Power of Simple Power Analysis on Smartcards -- Power Analysis Attacks and Algorithmic Approaches to their Countermeasures for Koblitz Curve Cryptosystems -- A Timing Attack

against RSA with the Chinese Remainder Theorem -- Hardware Implementation of Block Ciphers -- A Comparative Study of Performance of AES Final Candidates Using FPGAs -- A Dynamic FPGA Implementation of the Serpent Block Cipher -- A 12 Gbps DES Encryptor/Decryptor Core in an FPGA -- A 155 Mbps Triple-DES Network Encryptor -- Hardware Architectures -- An Energy Efficient Reconfigurable Public-Key Cryptography Processor Architecture -- High-Speed RSA Hardware Based on Barret's Modular Reduction Method -- Data Integrity in Hardware for Modular Arithmetic -- A Design for Modular Exponentiation Coprocessor in Mobile Telecommunication Terminals -- Invited Talk -- How to Explain Side-Channel Leakage to Your Kids -- Power Analysis Attacks -- On Boolean and Arithmetic Masking against Differential Power Analysis -- Using Second-Order Power Analysis to Attack DPA Resistant Software -- Differential Power Analysis in the Presence of Hardware Countermeasures -- Arithmetic Architectures -- Montgomery Multiplier and Squarer in GF(2m) -- A Scalable and Unified Multiplier Architecture for Finite Fields GF(p) and GF(2m) -- Montgomery Exponentiation with no Final Subtractions: Improved Results -- Physical Security and Cryptanalysis -- Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defenses -- Software-Hardware Trade-Offs: Application to A5/1 Cryptanalysis -- New Schemes and Algorithms -- MiniPASS: Authentication and Digital Signatures in a Constrained Environment -- Efficient Generation of Prime Numbers.