1. Record Nr. UNISA996466125503316

Titolo	Selected areas in cryptography : 5th annual international workshop, SAC'98, Kingston, Ontario, Canada, August 17-18, 1998, proceedings / / Stafford Tavares, Henk Meijer (editors)
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer, , [1999] Â©1999
ISBN	3-540-48892-8
Edizione	[1st ed. 1999.]
Descrizione fisica	1 online resource (X, 386 p.)
Collana	Lecture Notes in Computer Science ; ; 1556
Disciplina	005.8
Soggetti	Computer security Data encryption (Computer science)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Design of Secret Key Cryptosystems -- Feistel Ciphers with L 2-Decorrelation -- Key-Dependent S-Box Manipulations -- On the Twofish Key Schedule -- Towards Provable Security of Substitution-Permutation Encryption Networks -- Randomness and Computational Issues -- An Accurate Evaluation of Maurer's Universal Test -- Computational Alternatives to Random Number Generators -- Storage-Efficient Finite Field Basis Conversion -- Verifiable Partial Sharing of Integer Factors -- Analysis of Secret Key Cryptosystems -- Higher Order Differential Attack Using Chosen Higher Order Differences -- On Maximum Non-averaged Differential Probability -- Cryptanalysis of RC4-like Ciphers -- Cryptographic Systems -- Key Preassigned Traceability Schemes for Broadcast Encryption -- Mix-Based Electronic Payments -- Over the Air Service Provisioning -- Public Key Cryptosystems -- Faster Attacks on Elliptic Curve Cryptosystems -- Improved Algorithms for Elliptic Curve Arithmetic in GF(2n) -- Cryptanalysis of a Fast Public Key Cryptosystem Presented at SAC '97 -- A Lattice- Based Public-Key Cryptosystem -- Design and Implementation of Secret Key Cryptosystems -- Fast DES Implementations for FPGAs and Its Application to a Universal Key-Search Machine -- IDEA: A Cipher for Multimedia Architectures? -- A Strategy for Constructing Fast Round Functions with Practical Security

	Against Differential and Linear Cryptanalysis -- The Nonhomomorphicity of Boolean Functions -- Attacks on Secret Key Cryptosystems -- Cryptanalysis of ORYX -- A Timing Attack on RC5 -- Cryptanalysis of SPEED -- Invited Talks -- Authenticated Diffe-Hellman Key Agreement Protocols -- Initial Observations on Skipjack: Cryptanalysis of Skipjack-3XOR.
Sommario/riassunto	AC’98 A C - . AC’94 AC’96 ’ ! K AC’95 AC’97 C ! O . & . I - * . & * AC’98 : • D A ** K C * • E? I* * C * • C I • /M N O 39 * AC’98,26 - * .& ! , A M K A * E B * I O ! J :C J -3.