1. Record Nr. UNISA996465295403316

| | |
|---|---|
| Titolo | Selected Areas in Cryptography [[electronic resource] ] : 8th Annual International Workshop, SAC 2001 Toronto, Ontario, Canada, August 16-17, 2001. Revised Papers / / edited by Serge Vaudenay, Amr M. Youssef |
| Pubbl/distr/stampa | Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2001 |
| ISBN | 3-540-45537-X |
| Edizione | [1st ed. 2001.] |
| Descrizione fisica | 1 online resource (XII, 364 p.) |
| Collana | Lecture Notes in Computer Science, , 0302-9743 ; ; 2259 |
| Disciplina | 005.82 |
| Soggetti | Data encryption (Computer science)<br>Operating systems (Computers)<br>Computers and civilization<br>Algorithms<br>Computer communication systems<br>Computer mathematics<br>Cryptology<br>Operating Systems<br>Computers and Society<br>Algorithm Analysis and Problem Complexity<br>Computer Communication Networks<br>Computational Science and Engineering |
| 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 | Cryptanalysis I -- Weaknesses in the Key Scheduling Algorithm of RC4 -- A Practical Cryptanalysis of SSC2 -- Analysis of the E 0 Encryption System -- Boolean Functions -- Boolean Functions with Large Distance to All Bijective Monomials: N Odd Case -- Linear Codes in Constructing Resilient Functions with High Nonlinearity -- New Covering Radius of Reed-Muller Codes for t-Resilient Functions -- Generalized Zig-zag Functions and Oblivious Transfer Reductions -- Rijndael -- A Simple Algebraic Representation of Rijndael -- Improving the Upper Bound on |

the Maximum Average Linear Hull Probability for Rijndael -- Invited Talk I -- Polynomial Reconstruction Based Cryptography -- Elliptic Curves and Efficient Implementation I -- An Improved Implementation of Elliptic Curves over GF(2 n ) when Using Projective Point Arithmetic -- Fast Generation of Pairs (k, [k]P) for Koblitz Elliptic Curves -- Algorithms for Multi-exponentiation -- Two Topics in Hyperelliptic Cryptography -- Cryptanalysis II -- A Differential Attack on Reduced-Round SC2000 -- On the Complexity of Matsui's Attack -- Random Walks Revisited: Extensions of Pollard's Rho Algorithm for Computing Multiple Discrete Logarithms -- Elliptic Curves and Efficient Implementation II -- Fast Normal Basis Multiplication Using General Purpose Processors -- Fast Multiplication of Integers for Public-Key Applications -- Fast Simultaneous Scalar Multiplication on Elliptic Curve with Montgomery Form -- On the Power of Multidoubling in Speeding Up Elliptic Scalar Multiplication -- Public Key Systems -- The GH Public-Key Cryptosystem -- XTR Extended to GF(p 6m ) -- Invited Talk II -- The Two Faces of Lattices in Cryptology -- Protocols and Mac -- New (Two-Track-)MAC Based on the Two Trails of RIPEMD -- Key Revocation with Interval Cover Families -- Timed-Release Cryptography.