1. Record Nr. UNINA9910144196803321

Titolo	Selected Areas in Cryptography : 10th Annual International Workshop, SAC 2003, Ottawa, Canada, August 14-15, 2003, Revised Papers / / edited by Mitsuru Matsui, Robert Zuccherato
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2004
ISBN	1-280-30723-4 9786610307234 3-540-24654-1
Edizione	[1st ed. 2004.]
Descrizione fisica	1 online resource (XII, 368 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 3006
Disciplina	005.8
Soggetti	Data encryption (Computer science) Computer networks Operating systems (Computers) Algorithms Application software Management information systems Computer science Cryptology Computer Communication Networks Operating Systems Algorithm Analysis and Problem Complexity Information Systems Applications (incl. Internet) 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	Elliptic and Hyperelliptic Curves -- Low Cost Security: Explicit Formulae for Genus-4 Hyperelliptic Curves -- On the Selection of Pairing-Friendly Groups -- Counting Points for Hyperelliptic Curves of Type y 2=x 5+ax over Finite Prime Fields -- Side Channel Attacks -- Longer Keys May Facilitate Side Channel Attacks -- On Randomizing Private

Keys to Counteract DPA Attacks -- Security Protocols and Applications -- Zero Common-Knowledge Authentication for Pervasive Networks -- Multiple-Time Signature Schemes against Adaptive Chosen Message Attacks -- Broadcast Enforced Threshold Schemes with Disenrollment -- Cryptanalysis I -- A New Meet-in-the-Middle Attack on the IDEA Block Cipher -- Cryptanalysis of the Alleged SecurID Hash Function -- Authenticated On-Line Encryption -- Five Practical Attacks for “Optimistic Mixing for Exit-Polls” -- Cryptanalysis II -- Security Analysis of SHA-256 and Sisters -- A Chosen IV Attack Against Turing -- Related-Key Differential Cryptanalysis of 192-bit Key AES Variants -- A Distinguishing Attack of SNOW 2.0 with Linear Masking Method -- Cryptographic Primitives -- On the Use of GF-Inversion as a Cryptographic Primitive -- Cryptographic Applications of T-Functions -- Stream Ciphers -- On the Success of the Embedding Attack on the Alternating Step Generator -- Additive Autocorrelation of Resilient Boolean Functions -- On a New Notion of Nonlinearity Relevant to Multi-output Pseudo-random Generators -- Efficient Implementation -- Alternative Digit Sets for Nonadjacent Representations -- Generic Efficient Arithmetic Algorithms for PAFFs (Processor Adequate Finite Fields) and Related Algebraic Structures -- More Generalized Mersenne Numbers -- Lower Bound on Linear Authenticated Encryption.

Sommario/riassunto

This book constitutes the thoroughly refereed postproceedings of the 10th Annual International Workshop on Selected Areas in Cryptography, SAC 2003, held in Ottawa, Canada, in August 2003. The 25 revised full papers presented were carefully selected from 85 submissions during two rounds of reviewing and improvement. The papers are organized in topical sections on elliptic and hyperelliptic curves, side channel attacks, security protocols and applications, cryptanalysis, cryptographic primitives, stream ciphers, and efficient implementations.