1. Record Nr. UNINA9910144155303321

Titolo	Fast Software Encryption : 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004, Revised Papers / / edited by Bimal Kumar Roy, Willi Meier
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2004
ISBN	1-280-30780-3 9786610307807 3-540-25937-6
Edizione	[1st ed. 2004.]
Descrizione fisica	1 online resource (XII, 492 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 3017
Disciplina	005.8
Soggetti	Data encryption (Computer science) Algorithms Coding theory Information theory Computer science—Mathematics Cryptology Algorithm Analysis and Problem Complexity Coding and Information Theory 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 at the end of each chapters and index.
Nota di contenuto	New Cryptographic Primitives Based on Multiword T-Functions -- Towards a Unifying View of Block Cipher Cryptanalysis -- Algebraic Attacks on Summation Generators -- Algebraic Attacks on SOBER-t32 and SOBER-t16 without Stuttering -- Improving Fast Algebraic Attacks -- Resistance of S-Boxes against Algebraic Attacks -- Differential Attacks against the Helix Stream Cipher -- Improved Linear Consistency Attack on Irregular Clocked Keystream Generators -- Correlation Attacks Using a New Class of Weak Feedback Polynomials -- Minimum Distance between Bent and 1-Resilient Boolean Functions -- Results on Rotation Symmetric Bent and Correlation Immune Boolean

Functions -- A Weakness of the Linear Part of Stream Cipher MUGI -- Vulnerability of Nonlinear Filter Generators Based on Linear Finite State Machines -- VMPC One-Way Function and Stream Cipher -- A New Stream Cipher HC-256 -- A New Weakness in the RC4 Keystream Generator and an Approach to Improve the Security of the Cipher -- Improving Immunity of Feistel Ciphers against Differential Cryptanalysis by Using Multiple MDS Matrices -- ICEBERG : An Involutional Cipher Efficient for Block Encryption in Reconfigurable Hardware -- Related Key Differential Attacks on 27 Rounds of XTEA and Full-Round GOST -- On the Additive Differential Probability of Exclusive-Or -- Two Power Analysis Attacks against One-Mask Methods -- Nonce-Based Symmetric Encryption -- Ciphers Secure against Related-Key Attacks -- Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance -- The EAX Mode of Operation -- CWC: A High-Performance Conventional Authenticated Encryption Mode -- New Security Proofs for the 3GPP Confidentiality and Integrity Algorithms -- Cryptanalysis of a Message Authentication Code due to Cary and Venkatesan -- Fast Software-Based Attacks on SecurID -- A MAC Forgery Attack on SOBER-128 -- On Linear Approximation of Modulo Sum.

Sommario/riassunto

2.1 Di?erential Power Analysis Di?erential Power Analysis (DPA) was introduced by Kocher, Ja?e and Jun in 1998 [13] and published in 1999 [14]. The basic idea is to make use of potential correlations between the data handled by the micro-controller and the electric consumption measured values. Since these correlations are often very low, s- tistical methods must be applied to deduce su?cient information from them. Theprinciple ofDPAattacksconsistsincomparingconsumptionvalues m-suredonthe real physical device (for instance a GSM chip or a smart card)with values computed in an hypothetical model of this device (the hypotheses being made among others on the nature of the implementation, and chie?y on a part of the secret key). By comparing these two sets of values, the attacker tries to recover all or part of the secret key. The initial target of DPA attacks was limited to symmetric algorithms. V- nerability of DES – ?rst shown by Kocher, Ja?e and Jun [13, 14]–wasfurther studied by Goubin and Patarin [11, 12], Messerges, Dabbish, Sloan [16]and Akkar, B´ evan, Dischamp, Moyart [2]. Applications of these attacks were also largely taken into account during the AES selection process, notably by Biham, Shamir [4], Chari, Jutla, Rao, Rohatgi [5] and Daemen, Rijmen [8].