1. Record Nr. UNINA9910767509903321

Titolo	Selected Areas in Cryptography : 7th Annual International Workshop, SAC 2000, Waterloo, Ontario, Canada, August 14-15, 2000. Proceedings / / edited by Douglas R. Stinson, Stafford Tavares
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2001
ISBN	3-540-44983-3
Edizione	[1st ed. 2001.]
Descrizione fisica	1 online resource (IX, 347 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 2012
Disciplina	005.8/2
Soggetti	Data encryption (Computer science) Computer networks Computer programming Algorithms Management information systems Computer science Application software Cryptology Computer Communication Networks Programming Techniques Algorithm Analysis and Problem Complexity Management of Computing and Information Systems Information Systems Applications (incl. Internet)
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 -- Analysis of IS-95 CDMA Voice Privacy -- Attacks on Additive Encryption of Redundant Plaintext and Implications on Internet Security -- Cryptanalysis of the “Augmented Family of Cryptographic Parity Circuits” Proposed at ISW’97 -- Block Ciphers — New Designs -- Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms — Design andAnalysis -- DFCv2 -- The Block Cipher Hierocrypt -- Symmetric Block Ciphers Based on Group Bases -- Elliptic Curves and

Efficient Implementations -- Speeding up the Arithmetic on Koblitz Curves of Genus Two -- On Complexity of Polynomial Basis Squaring in F2m -- Security Protocols and Applications -- Dynamic Multi-threshold Metering Schemes -- Chained Stream Authentication -- A Global PMI for Electronic Content Distribution -- Block Ciphers and Hash Functions -- A Polynomial-Time Universal Security Amplifier in the Class of Block Ciphers -- Decorrelation over Infinite Domains: The Encrypted CBC-MAC Case -- HAS-V: A New Hash Function with Variable Output Length -- Boolean Functions and Stream Ciphers -- On Welch-Gong Transformation Sequence Generators -- Modes of Operation of Stream Ciphers -- LILI Keystream Generator -- Improved Upper Bound on the Nonlinearity of High Order Correlation Immune Functions -- Public Key Systems -- Towards Practical Non-interactive Public Key Cryptosystems Using Non-maximal Imaginary Quadratic Orders (Extended Abstract) -- On the Implementation of Cryptosystems Based on Real Quadratic Number Fields (Extended Abstract) -- Cryptanalysis II -- Root Finding Interpolation Attack -- Differential Cryptanalysis of Reduced Rounds of GOST -- Practical Security Evaluation against Differential and Linear Cryptanalyses for Feistel Ciphers with SPN Round Function.

Sommario/riassunto

SAC 2000 was the seventh in a series of annual workshops on Selected Areas in Cryptography. PreviousworkshopswereheldatQueen'sUniversityinKingston (1994, 1996, 1998, and 1999) and at Carleton University in Ottawa (1995 and 1997). The intent of the workshops is to provide a relaxed atmosphere in which researchers in cryptography can present and discuss new work on selected areas of current interest. The themes for the SAC 2000 workshop were: - design and analysis of symmetric key cryptosystems, - primitivesforprivatekeycryptography,includingblockandstreamciphers, hash functions, and MACs, - e'cientimplementationsofcryptographicsystemsinpublicandprivatekey cryptography, - cryptographic solutions for web/internet security. Atotalof41papersweresubmittedtoSAC2000, oneofwhichwassubsequently withdrawn. After a review process that had all papers reviewed by at least 3 referees, 24 papers were accepted for presentation at the workshop. As well, we were fortunate to have the following two invited speakers at SAC 2000: - M. Bellare, UCSD (U.S.A.) "The Provable-Security Approach to Authenticated Session-Key Exchange" - D. Boneh, Stanford U. (U.S.A.) "Message Authentication in a Multicast Environment" The program committee for SAC 2000 consisted of the following members: L. Chen, H. Heys, L. Knudsen, S. Moriai, L. O'Connor, D. Stinson, S. Tavares, S. Vaudenay, A. Youssef, and R. Zuccherato. Many thanks are due to the p-gramcommitteefortheirhardwork.Also, AmrYoussefprovidedgreatassistance in making the reviewing process run smoothly. Weareappreciativeofthe'nancialsupportprovidedbyCerticomCorporation, CITO, Entrust Technologies, MITACS, and the University of Waterloo. Special thanks are due to Frances Hannigan, who was responsible for the local arran- ments, and for making sure that everything ran smoothly during the workshop.