1. Record Nr. UNISA996466026803316

Titolo	Selected Areas in Cryptography [[electronic resource]] : 11th International Workshop, SAC 2004, Waterloo, Canada, August 9-10, 2004, Revised Selected Papers / / edited by Helena Handschuh, Anwar Hasan
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2005
ISBN	3-540-30564-5
Edizione	[1st ed. 2005.]
Descrizione fisica	1 online resource (XI, 354 p.)
Collana	Security and Cryptology ; ; 3357
Disciplina	005.8/2
Soggetti	Data encryption (Computer science) Operating systems (Computers) Management information systems Computer science Algorithms Computer communication systems Application software Cryptology Operating Systems Management of Computing and Information Systems Algorithm Analysis and Problem Complexity Computer Communication Networks 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 and author index.
Nota di contenuto	Stream Cipher Cryptanalysis -- An Improved Correlation Attack on A5/1 -- Extending the Resynchronization Attack -- A New Simple Technique to Attack Filter Generators and Related Ciphers -- Side-Channel Analysis -- On XTR and Side-Channel Analysis -- Provably Secure Masking of AES -- Block Cipher Design -- Perfect Diffusion Primitives for Block Ciphers -- Security of the MISTY Structure in the Luby-Rackoff Model: Improved Results -- FOX : A New Family of Block

Ciphers -- Efficient Implementations -- A Note on the Signed Sliding Window Integer Recoding and a Left-to-Right Analogue -- Fast Irreducibility Testing for XTR Using a Gaussian Normal Basis of Low Complexity -- Modular Number Systems: Beyond the Mersenne Family -- Efficient Doubling on Genus Two Curves over Binary Fields -- Secret Key Cryptography I -- About the Security of Ciphers (Semantic Security and Pseudo-Random Permutations) -- A Subliminal Channel in Secret Block Ciphers -- Blockwise Adversarial Model for On-line Ciphers and Symmetric Encryption Schemes -- Cryptanalysis -- Cryptanalysis of a White Box AES Implementation -- Predicting Subset Sum Pseudorandom Generators -- Collision Attack and Pseudorandomness of Reduced-Round Camellia -- Cryptographic Protocols -- Password Based Key Exchange with Mutual Authentication -- Product Construction of Key Distribution Schemes for Sensor Networks -- Deterministic Key Predistribution Schemes for Distributed Sensor Networks -- On Proactive Secret Sharing Schemes -- Secret Key Cryptography II -- Efficient Constructions of Variable-Input-Length Block Ciphers -- A Sufficient Condition for Optimal Domain Extension of UOWHFs.

Sommario/riassunto

SAC 2004 was the eleventh in a series of annual workshops on Selected Areas in Cryptography. This was the second time that the workshop was hosted by the University of Waterloo, Ontario, with previous workshops being held at Queen’sUniversityinKingston(1994,1996,1998 and1999),CarletonUniversity in Ottawa (1995, 1997 and 2003), the Fields Institute in Toronto (2001) and Memorial University of Newfoundland in St. John’s (2002). The primary intent of the workshop was to provide a relaxed atmosphere in which researchers in cryptography could present and discuss new work on selected areas of current interest. This year’s themes for SAC were: – Design and analysis of symmetric key cryptosystems. – Primitives for symmetric key cryptography, including block and stream - phers, hash functions, and MAC algorithms. – E?cient implementation of cryptographic systems in public and symmetric key cryptography. – Cryptographic solutions for mobile (web) services. A record of 117 papers were submitted for consideration by the program committee. After an extensive review process, 25 papers were accepted for p- sentation at the workshop (two of these papers were merged). Unfortunately, many good papers could not be accommodated this year. These proceedings contain the revised versions of the 24 accepted papers. The revised versions were not subsequently checked for correctness. Also, we were very fortunate to have two invited speakers at SAC 2004. • Eli Biham arranged for some breaking news in his talk on “New Results on SHA-0 and SHA-1.” This talk was designated as the Sta?ord Tavares L- ture.