1. Record Nr. UNINA9910484328403321

Titolo	Selected Areas in Cryptography : 12th International Workshop, SAC 2005, Kingston, ON, Canada, August 11-12, 2005, Revised Selected Papers / / edited by Bart Preneel, Stafford Tavares
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2006
ISBN	3-540-33109-3
Edizione	[1st ed. 2006.]
Descrizione fisica	1 online resource (XI, 371 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 3897
Altri autori (Persone)	PreneelBart <1963-> TavaresStafford <1940->
Disciplina	005.8/2
Soggetti	Cryptography Data encryption (Computer science) Operating systems (Computers) Electronic data processing - Management Algorithms Computer networks Application software Cryptology Operating Systems IT Operations Computer Communication Networks Computer and Information Systems Applications
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 index.
Nota di contenuto	Stream Ciphers I -- Conditional Estimators: An Effective Attack on A5/1 -- Cryptanalysis of the F-FCSR Stream Cipher Family -- Fault Attacks on Combiners with Memory -- Block Ciphers -- New Observation on Camellia -- Proving the Security of AES Substitution-Permutation Network -- Modes of Operation -- An Attack on CFB Mode Encryption as Used by OpenPGP -- Parallelizable Authentication Trees -- Improved Time-Memory Trade-Offs with Multiple Data -- Public Key Cryptography -- A Space Efficient Backdoor in RSA and Its Applications

-- An Efficient Public Key Cryptosystem with a Privacy Enhanced Double Decryption Mechanism -- Stream Ciphers II -- On the (Im)Possibility of Practical and Secure Nonlinear Filters and Combiners -- Rekeying Issues in the MUGI Stream Cipher -- Key Establishment Protocols and Access Control -- Tree-Based Key Distribution Patterns -- Provably Secure Tripartite Password Protected Key Exchange Protocol Based on Elliptic Curves -- An Access Control Scheme for Partially Ordered Set Hierarchy with Provable Security -- Hash Functions -- Breaking a New Hash Function Design Strategy Called SMASH -- Analysis of a SHA-256 Variant -- Impact of Rotations in SHA-1 and Related Hash Functions -- Protocols for RFID Tags -- A Scalable, Delegatable Pseudonym Protocol Enabling Ownership Transfer of RFID Tags -- Reducing Time Complexity in RFID Systems -- Efficient Implementations -- Accelerated Verification of ECDSA Signatures -- Pairing-Friendly Elliptic Curves of Prime Order -- Minimality of the Hamming Weight of the ?-NAF for Koblitz Curves and Improved Combination with Point Halving -- SPA Resistant Left-to-Right Integer Recodings -- Efficient FPGA-Based Karatsuba Multipliers for Polynomials over .

Sommario/riassunto

SAC 2005 was the 12th in a series of annual workshops on Selected Areas in Cryptography. This was the 5th time the workshop was hosted by Queen’s U- versity in Kingston (the previous workshops were held here in 1994, 1996, 1998 and 1999).Other SAC workshopshave been organizedat Carleton University in Ottawa (1995, 1997 and 2003), the Fields Institute in Toronto (2001), Memorial University of Newfoundland in St. John’s (2002) and the University of Waterloo (2000 and 2004). The workshop provided a relaxed atmosphere in which - searchers in cryptography could present and discuss new work on selected areas of current interest. The themes for SAC 2005 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 implementations of symmetric and public key algorithms; – cryptographic algorithms and protocols for ubiquitous computing (sensor networks, RFID). A total of 96 papers were submitted. Three papers were not considered - cause they were identi?ed as being multiple submissions. After an extensive double-blind reviewing process, the program committee accepted 25 papers for presentation at the workshop. We were very fortunate to have two invited speakers at SAC 2005, who both delivered thought-provoking and entertaining talks: – Alfred Menezes: Another Look at Provable Security; – Mike Wiener: The Full Cost of Cryptanalytic Attacks.