1.	Record Nr.	UNINA9910484329303321
	Titolo	Selected Areas in Cryptography : 16th International Workshop, SAC 2009, Calgary, Alberta, Canada, August 13-14, 2009, Revised Selected Papers / / edited by Michael J. Jacobson, Vincent Rijmen, Rei Safavi-Naini
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2009
	ISBN	3-642-05445-5
	Edizione	[1st ed. 2009.]
	Descrizione fisica	1 online resource (XIII, 467 p.)
	Collana	Security and Cryptology, , 2946-1863 ; ; 5867
	Classificazione	DAT 465f SS 4800
	Altri autori (Persone)	JacobsonMichael J RijmenVincent <1970-> Safavi-NainiReihanah
	Disciplina	004n/a
	Soggetti	Cryptography Data encryption (Computer science) Computer programming Data protection Data structures (Computer science) Information theory Coding theory Computer science - Mathematics Discrete mathematics Cryptology Programming Techniques Data and Information Security Data Structures and Information Theory 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 and index.
	Nota di contenuto	Hash Functions I -- Practical Collisions for SHAMATA-256 -- Improved

Cryptanalysis of the Reduced Grøstl Compression Function, ECHO Permutation and AES Block Cipher -- Cryptanalyses of Narrow-Pipe Mode of Operation in AURORA-512 Hash Function -- Miscellaneous Techniques -- More on Key Wrapping -- Information Theoretically Secure Multi Party Set Intersection Re-visited -- Real Traceable Signatures -- Hash Functions II -- Cryptanalysis of Hash Functions with Structures -- Cryptanalysis of the LANE Hash Function -- Practical Pseudo-collisions for Hash Functions ARIRANG-224/384 -- Hardware Implementation and Cryptanalysis -- A More Compact AES -- Optimization Strategies for Hardware-Based Cofactorization -- More on the Security of Linear RFID Authentication Protocols -- Differential Fault Analysis of Rabbit -- An Improved Recovery Algorithm for Decayed AES Key Schedule Images -- Block Ciphers -- Cryptanalysis of the Full MMB Block Cipher -- Weak Keys of Reduced-Round PRESENT for Linear Cryptanalysis -- Improved Integral Attacks on MISTY1 -- New Results on Impossible Differential Cryptanalysis of Reduced–Round Camellia–128 -- Modes of Operation -- Format-Preserving Encryption -- BTM: A Single-Key, Inverse-Cipher-Free Mode for Deterministic Authenticated Encryption -- Implementation of Public Key Cryptography -- On Repeated Squarings in Binary Fields -- Highly Regular m-Ary Powering Ladders -- An Efficient Residue Group Multiplication for the ? T Pairing over -- Compact McEliece Keys from Goppa Codes -- Hash Functions and Stream Ciphers -- Herding, Second Preimage and Trojan Message Attacks beyond Merkle-Damgård -- Cryptanalysis of Dynamic SHA(2) -- A New Approach for FCSRs -- New Cryptanalysis of Irregularly Decimated Stream Ciphers.

Sommario/riassunto

This volume constitutes the selected papers of the 16th Annual International Workshop on Selected Areas in Cryptography, SAC 2009, held in Calgary, Alberta, Canada, in August 13-14 2009. From a total of 99 technical papers, 27 papers were accepted for presentation at the workshop. They cover the following topics: hash functions, on block and stream ciphers, public key schemes, implementation, and privacy-enhancing cryptographic systems.