1.

Record Nr.	UNINA9910485140003321
Titolo	Selected areas in cryptography : 15th International Workshop, SAC 2008, Sackville, New Brunswick, Canada, August 14-15, revised selected papers / / Roberto Avanzi, Liam Keliher, Francesco Sica (eds.)
Pubbl/distr/stampa	Berlin ; ; Heidelberg, : Springer-Verlag, c2009
ISBN	3-642-04159-0
Edizione	[1st ed. 2009.]
Descrizione fisica	1 online resource (XI, 457 p.)
Collana	Lecture notes in computer science ; ; 5381
Altri autori (Persone)	AvanziRoberto KeliherLiam SicaFrancesco
Disciplina	005.8
Soggetti	Data encryption (Computer science) Cryptography
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	Elliptic and Hyperelliptic Curve Arithmetic -- Faster Halvings in Genus 2 -- Efficient Pairing Computation on Genus 2 Curves in Projective Coordinates -- On Software Parallel Implementation of Cryptographic Pairings -- Block Ciphers I -- The Cryptanalysis of Reduced-Round SMS4 -- Building Secure Block Ciphers on Generic Attacks Assumptions -- First Invited Talk -- Lifting and Elliptic Curve Discrete Logarithms -- Hash Functions I -- Preimage Attacks on One-Block MD4, 63-Step MD5 and More -- Preimage Attacks on 3-Pass HAVAL and Step-Reduced MD5 -- Cryptanalysis of Tweaked Versions of SMASH and Reparation -- Mathematical Aspects of Applied Cryptography I -- Counting Functions for the k-Error Linear Complexity of 2 n -Periodic Binary Sequences -- On the Exact Success Rate of Side Channel Analysis in the Gaussian Model -- Stream Ciphers Cryptanalysis -- Algebraic and Correlation Attacks against Linearly Filtered Non Linear Feedback Shift Registers -- A Cache Timing Analysis of HC-256 -- An Improved Fast Correlation Attack on Stream Ciphers -- Hash Functions II -- A Three-Property-Secure Hash Function -- Analysis of the Collision Resistance of RadioGatúnUsing Algebraic Techniques -- A Scheme to Base a Hash Function on a Block Cipher -- Collisions and Other Non-random Properties for Step-Reduced SHA-256 -- Cryptography with Algebraic