1. Record Nr. UNINA9910484014203321

Titolo	Selected areas in cryptography : 13th international workshop, SAC 2006, Montreal, Canada, August 17-18, 2006 : revised selected papers / / Eli Biham, Amr M. Youssef (editors)
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer-Verlag, , [2007] ©2007
ISBN	3-540-74462-2
Edizione	[1st ed. 2007.]
Descrizione fisica	1 online resource (XI, 395 p.)
Collana	Lecture Notes in Computer Science ; ; 4356
Disciplina	001.5436
Soggetti	Cryptography Computer security Data encryption (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	Block Cipher Cryptanalysis -- Improved DST Cryptanalysis of IDEA -- Improved Related-Key Impossible Differential Attacks on Reduced-Round AES-192 -- Related-Key Rectangle Attack on the Full SHACAL-1 -- Stream Cipher Cryptanalysis I -- Cryptanalysis of Achterbahn-Version 2 -- Cryptanalysis of the Stream Cipher ABC v2 -- The Design of a Stream Cipher LEX -- Dial C for Cipher -- Improved Security Analysis of XEX and LRW Modes -- Extended Hidden Number Problem and Its Cryptanalytic Applications -- Changing the Odds Against Masked Logic -- Advances on Access-Driven Cache Attacks on AES -- Blind Differential Cryptanalysis for Enhanced Power Attacks -- Efficient Implementations I -- Efficient Implementations of Multivariate Quadratic Systems -- Unbridle the Bit-Length of a Crypto-coprocessor with Montgomery Multiplication -- Delaying and Merging Operations in Scalar Multiplication: Applications to Curve-Based Cryptosystems -- Stream Cipher Cryptanalysis II -- On the Problem of Finding Linear Approximations and Cryptanalysis of Pomaranch Version 2 -- Multi-pass Fast Correlation Attack on Stream Ciphers -- Crossword Puzzle Attack on NLS -- Invited Talk -- When Stream Cipher Analysis Meets Public-Key Cryptography -- Efficient Implementations II -- On Redundant ?-Adic Expansions and Non-adjacent Digit Sets -- Pairing

	Calculation on Supersingular Genus 2 Curves -- Efficient Divisor Class Halving on Genus Two Curves -- Message Authentication on 64-Bit Architectures -- Some Notes on the Security of the Timed Efficient Stream Loss-Tolerant Authentication Scheme -- Constructing an Ideal Hash Function from Weak Ideal Compression Functions -- Provably Good Codes for Hash Function Design.
Sommario/riassunto	This book constitutes the thoroughly refereed post-proceedings of the 13th International Workshop on Selected Areas in Cryptography, SAC 2006, held in Montreal, Canada in August 2006. The 25 revised full papers presented together with 2 invited talks were carefully reviewed and selected from 86 submissions. The papers are organized in topical sections on block cipher cryptanalysis, stream cipher cryptanalysis, block and stream ciphers, side-channel attacks, efficient implementations, message authentication codes, and hash functions.