1. Record Nr. UNINA9910483305303321

Titolo	Cryptography and Coding : 11th IMA International Conference, Cirencester, UK, December 18-20, 2007, Proceedings / / edited by Steven Galbraith
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2007
ISBN	3-540-77272-3
Edizione	[1st ed. 2007.]
Descrizione fisica	1 online resource (XI, 426 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 4887
Disciplina	003.54
Soggetti	Coding theory Information theory Cryptography Data encryption (Computer science) Data protection Computer science - Mathematics Discrete mathematics Computer networks Coding and Information Theory Cryptology Data and Information Security Discrete Mathematics in Computer Science Computer Communication Networks
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Invited Papers -- Efficient Cryptographic Protocols Based on the Hardness of Learning Parity with Noise -- Galois Rings and Pseudo-random Sequences -- Signatures I -- Finding Invalid Signatures in Pairing-Based Batches -- How to Forge a Time-Stamp Which Adobe’s Acrobat Accepts -- Efficient Computation of the Best Quadratic Approximations of Cubic Boolean Functions -- On the Walsh Spectrum of a New APN Function -- Non-linear Cryptanalysis Revisited: Heuristic Search for Approximations to S-Boxes -- Cryptanalysis of the EPBC

Authenticated Encryption Mode -- Blockwise-Adaptive Chosen-Plaintext Attack and Online Modes of Encryption -- Algebraic Cryptanalysis of the Data Encryption Standard -- Cryptographic Side-Channels from Low-Power Cache Memory -- New Branch Prediction Vulnerabilities in OpenSSL and Necessary Software Countermeasures -- Remarks on the New Attack on the Filter Generator and the Role of High Order Complexity -- Modified Berlekamp-Massey Algorithm for Approximating the k-Error Linear Complexity of Binary Sequences -- Efficient KEMs with Partial Message Recovery -- Randomness Reuse: Extensions and Improvements -- On the Connection Between Signcryption and One-Pass Key Establishment -- Optimised Versions of the Ate and Twisted Ate Pairings -- Extractors for Jacobian of Hyperelliptic Curves of Genus 2 in Odd Characteristic -- Constructing Pairing-Friendly Elliptic Curves Using Gröbner Basis Reduction -- Efficient 15,360-bit RSA Using Woop-Optimised Montgomery Arithmetic -- Toward Acceleration of RSA Using 3D Graphics Hardware -- Signatures II -- Multi-key Hierarchical Identity-Based Signatures -- Verifier-Key-Flexible Universal Designated-Verifier Signatures.

Sommario/riassunto

This book constitutes the refereed proceedings of the 11th IMA International Conference on Cryptography and Coding, held in Cirencester, UK in December 2007. The 22 revised full papers presented together with 2 invited contributions were carefully reviewed and selected from 48 submissions. The papers are organized in topical sections on signatures, boolean functions, block cipher cryptanalysis, side channels, linear complexity, public key encryption, curves, and RSA implementation.