1. Record Nr. UNISA996465933803316

Titolo	Fast software encryption : 15th International Workshop, FSE 2008, Lausanne, Switzerland, February 10-13, 2008 : revised selected papers / / Kaisa Nyberg (editor)
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer, , [2008] ©2008
ISBN	3-540-71039-6
Edizione	[1st ed. 2008.]
Descrizione fisica	1 online resource (XI, 489 p.)
Collana	Lecture Notes in Computer Science ; ; 5086
Disciplina	005.8
Soggetti	Computers - Access control 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	SHA Collisions -- Collisions for Step-Reduced SHA-256 -- Collisions on SHA-0 in One Hour -- New Hash Function Designs -- The Hash Function Family LAKE -- SWIFFT: A Modest Proposal for FFT Hashing -- Block Cipher Cryptanalysis (I) -- A Unified Approach to Related-Key Attacks -- Algebraic and Slide Attacks on KeeLoq -- A Meet-in-the-Middle Attack on 8-Round AES -- Implementation Aspects -- Block Ciphers Implementations Provably Secure Against Second Order Side Channel Analysis -- SQUASH – A New MAC with Provable Security Properties for Highly Constrained Devices Such as RFID Tags -- Differential Fault Analysis of Trivium -- Accelerating the Whirlpool Hash Function Using Parallel Table Lookup and Fast Cyclical Permutation -- Hash Function Cryptanalysis (I) -- Second Preimage Attack on 3-Pass HAVAL and Partial Key-Recovery Attacks on HMAC/NMAC-3-Pass HAVAL -- Cryptanalysis of LASH -- A (Second) Preimage Attack on the GOST Hash Function -- Stream Cipher Cryptanalysis (I) -- Guess-and-Determine Algebraic Attack on the Self-Shrinking Generator -- New Form of Permutation Bias and Secret Key Leakage in Keystream Bytes of RC4 -- Efficient Reconstruction of RC4 Keys from Internal States -- Security Bounds -- An Improved Security Bound for HCTR -- How to Encrypt with a Malicious Random Number Generator -- A One-Pass Mode of Operation for Deterministic Message

Authentication— Security beyond the Birthday Barrier -- Entropy -- Post-Processing Functions for a Biased Physical Random Number Generator -- Entropy of the Internal State of an FCSR in Galois Representation -- Block Cipher Cryptanalysis (II) -- Bit-Pattern Based Integral Attack -- Experiments on the Multiple Linear Cryptanalysis of Reduced Round Serpent -- Impossible Differential Cryptanalysis of CLEFIA -- Hash Function Cryptanalysis (II) -- MD4 is Not One-Way -- Improved Indifferentiability Security Analysis of chopMD Hash Function -- New Techniques for Cryptanalysis of Hash Functions and Improved Attacks on Snefru -- Stream Cipher Cryptanalysis (II) -- On the Salsa20 Core Function -- New Features of Latin Dances: Analysis of Salsa, ChaCha, and Rumba.

Sommario/riassunto

This book constitutes the thoroughly refereed proceedings of the 15th International Workshop on Fast Software Encryption, FSE 2008, held in Lausanne, Switzerland in February 2008. The 26 revised full papers presented together with 4 short papers were carefully reviewed and selected from 72 submissions. The papers address all current aspects of fast and secure primitives for symmetric cryptology and are organized in topical sections on SHA collisions, new hash function designs, block cipher cryptanalysis, implementation aspects, hash function cryptanalysis, stream cipher cryptanalysis, security bounds, and entropy.