1. Record Nr. UNINA9910484450503321

Titolo	Progress in Cryptology – INDOCRYPT 2007 : 8th International Conference on Cryptology in India, Chennai, India, December 9-13, 2007, Proceedings / / edited by K. Srinathan, C. Pandu Rangan, Moti Yung
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2007
ISBN	3-540-77026-7
Edizione	[1st ed. 2007.]
Descrizione fisica	1 online resource (XI, 428 p.)
Collana	Security and Cryptology ; ; 4859
Classificazione	004 DAT 465f SS 4800
Disciplina	001.5436
Soggetti	Cryptography Data encryption (Computer science) Algorithms Computer science—Mathematics Discrete mathematics Data protection Computer networks Electronic data processing—Management Cryptology Discrete Mathematics in Computer Science Data and Information Security Computer Communication Networks IT Operations
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Hashing -- Linearization Attacks Against Syndrome Based Hashes -- A Meet-in-the-Middle Collision Attack Against the New FORK-256 -- Multilane HMAC— Security beyond the Birthday Limit -- Elliptic Curve -- On the Bits of Elliptic Curve Diffie-Hellman Keys -- A Result on the Distribution of Quadratic Residues with Applications to Elliptic Curve

Cryptography -- Cryptoanalysis -- Related-Key Attacks on the Py-Family of Ciphers and an Approach to Repair the Weaknesses -- Related-Key Differential-Linear Attacks on Reduced AES-192 -- Improved Meet-in-the-Middle Attacks on Reduced-Round DES -- Information Theoretic Security -- Probabilistic Perfectly Reliable and Secure Message Transmission – Possibility, Feasibility and Optimality -- Secret Swarm Unit Reactive k??Secret Sharing -- Elliptic Curve Cryptography -- New Formulae for Efficient Elliptic Curve Arithmetic -- A Graph Theoretic Analysis of Double Base Number Systems -- Optimizing Double-Base Elliptic-Curve Single-Scalar Multiplication -- Signature -- Transitive Signatures from Braid Groups -- Proxy Re-signature Schemes Without Random Oracles -- Side Channel Attack -- First-Order Differential Power Analysis on the Duplication Method -- Solving Discrete Logarithms from Partial Knowledge of the Key -- Symmetric Cryptosystem -- New Description of SMS4 by an Embedding overGF(28) -- Tweakable Enciphering Schemes from Hash-Sum-Expansion -- A Framework for Chosen IV Statistical Analysis of Stream Ciphers -- Asymmetric Cryptosystem -- Public Key Encryption with Searchable Keywords Based on Jacobi Symbols -- A Certificate-Based Proxy Cryptosystem with Revocable Proxy Decryption Power -- Short Presentation -- Computationally-Efficient Password Authenticated Key Exchange Based on Quadratic Residues -- On the k-Operation Linear Complexity of Periodic Sequences -- Trade-Off Traitor Tracing -- X-FCSR – A New Software Oriented Stream Cipher Based Upon FCSRs -- Efficient Window-Based Scalar Multiplication on Elliptic Curves Using Double-Base Number System -- Extended Multi-Property-Preserving and ECM-Construction -- Design of a Differential Power Analysis Resistant Masked AES S-Box -- LFSR Based Stream Ciphers Are Vulnerable to Power Attacks -- An Update on the Side Channel Cryptanalysis of MACs Based on Cryptographic Hash Functions -- Attacking the Filter Generator by Finding Zero Inputs of the Filtering Function -- Efficient Implementations of Some Tweakable Enciphering Schemes in Reconfigurable Hardware.

Sommario/riassunto

This book constitutes the refereed proceedings of the 8th International Conference on Cryptology in India, INDOCRYPT 2007, held in Chennai, India, in December 2007. The 22 revised full papers and 11 revised short papers presented together with 3 invited lectures were carefully reviewed and selected from 104 submissions. The papers are organized in topical sections on hashing, elliptic curve, cryptoanalysis, information theoretic security, elliptic curve cryptography, signature, side channel attack, symmetric cryptosystem, asymmetric cryptosystem, and short papers.