1.	Record Nr.	UNINA9910483541303321
	Titolo	Progress in Cryptology - INDOCRYPT 2010 : 11th International Conference on Cryptology in India, Hyderabad, India, December 12-15, 2010, Proceedings / / edited by Guang Gong, Kishan Chand Gupta
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2010
	ISBN	1-280-39054-9 9786613568465 3-642-17401-9
	Edizione	[1st ed. 2010.]
	Descrizione fisica	1 online resource (XVI, 366 p. 63 illus.)
	Collana	Security and Cryptology, , 2946-1863 ; ; 6498
	Altri autori (Persone)	GongGuang <1956-> GuptaKishan Chand
	Disciplina	005.82
	Soggetti	Cryptography Data encryption (Computer science) Computer networks Algorithms Electronic data processing - Management Data protection Computer science - Mathematics Discrete mathematics Cryptology Computer Communication Networks IT Operations Data and Information Security Discrete Mathematics in Computer Science
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Includes index.
	Nota di contenuto	Invited Talk -- Getting a Few Things Right and Many Things Wrong -- Security of RSA and Multivariate Schemes -- Partial Key Exposure Attack on RSA – Improvements for Limited Lattice Dimensions -- Towards Provable Security of the Unbalanced Oil and Vinegar Signature Scheme under Direct Attacks -- CyclicRainbow – A Multivariate

Signature Scheme with a Partially Cyclic Public Key -- Security Analysis, Pseudorandom Permutations and Applications -- Combined Security Analysis of the One- and Three-Pass Unified Model Key Agreement Protocols -- Indifferentiability beyond the Birthday Bound for the Xor of Two Public Random Permutations -- The Characterization of Luby-Rackoff and Its Optimum Single-Key Variants -- Versatile Prêt à Voter: Handling Multiple Election Methods with a Unified Interface -- Invited Talk -- Cryptographic Hash Functions: Theory and Practice -- Hash Functions -- Cryptanalysis of Tav-128 Hash Function -- Near-Collisions for the Reduced Round Versions of Some Second Round SHA-3 Compression Functions Using Hill Climbing -- Speeding Up the Wide-Pipe: Secure and Fast Hashing -- Attacks on Block Ciphers and Stream Ciphers -- New Boomerang Attacks on ARIA -- Algebraic, AIDA/Cube and Side Channel Analysis of KATAN Family of Block Ciphers -- The Improbable Differential Attack: Cryptanalysis of Reduced Round CLEFIA -- Greedy Distinguishers and Nonrandomness Detectors -- Fast Cryptographic Computation -- Polynomial Multiplication over Binary Fields Using Charlier Polynomial Representation with Low Space Complexity -- Random Euclidean Addition Chain Generation and Its Application to Point Multiplication -- Cryptanalysis of AES -- Attack on a Higher-Order Masking of the AES Based on Homographic Functions -- Improved Impossible Differential Cryptanalysis of 7-Round AES-128 -- Cryptanalysis ofa Perturbated White-Box AES Implementation -- Efficient Implementation -- A Program Generator for Intel AES-NI Instructions -- ECC2K-130 on NVIDIA GPUs -- One Byte per Clock: A Novel RC4 Hardware.

Sommario/riassunto

The LNCS series reports state-of-the-art results in computer science research, development, and education, at a high level and in both printed and electronic form. Enjoying tight cooperation with the R & D community, with numerous individuals, as well as with prestigious organizations and societies, LNCS has grown into the most comprehensive computer science research forum available. The scope of LNCS, including its subseries LNAI and LNBI, spans the whole range of computer science and information technology including interdisciplinary topics in a variety of application fields. The type of material published traditionally includes proceedings (published in time for the respective conference) post-proceedings (consisting of thoroughly revised final full papers) research monographs (which may be based on outstanding PhD work, research projects, technical reports, etc.) More recently, several color-cover sublines have been added featuring, beyond a collection of papers, various added-value components; these sublines include tutorials (textbook-like monographs or collections of lectures given at advanced courses) state-of-the-art surveys (offering complete and mediated coverage of a topic) hot topics (introducing emergent topics to the broader community) Book jacket.