1. Record Nr. UNISA996466296803316

Titolo	Progress in Cryptology - INDOCRYPT 2012 [[electronic resource]] : 12th International Conference on Cryptology in India, Chennai, India, December 11-14, 2011, Proceedings13th International Conference on Cryptology in India, Kolkata, India, December 9-12, 2012, Proceedings / / edited by Steven Galbraith, Mridul Nandi
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2012
ISBN	3-642-34931-5
Edizione	[1st ed. 2012.]
Descrizione fisica	1 online resource (XIV, 566 p. 118 illus.)
Collana	Security and Cryptology ; ; 7668
Disciplina	005.82
Soggetti	Data encryption (Computer science) Computer communication systems Algorithms Management information systems Computer science Computer security Computer science—Mathematics Cryptology Computer Communication Networks Algorithm Analysis and Problem Complexity Management of Computing and Information Systems Systems and Data Security Discrete Mathematics in 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	How to Compute on Encrypted Data -- Using the Cloud to Determine Key Strengths -- On the Non-malleability of the Fiat-Shamir Transform -- Another Look at Symmetric Incoherent Optimal Eavesdropping against BB84 -- Leakage Squeezing of Order Two -- Hash Functions and Stream Cipher -- Collision Attack on the Hamsi-256 Compression Function -- Generalized Iterated Hash Functions Revisited: New

Complexity Bounds for Multicollision Attacks -- A Di_erential Fault Attack on the Grain Family under Reasonable Assumptions -- Faster Chosen-Key Distinguishers on Reduced-Round AES -- High-Speed Parallel Implementations of the Rainbow Method in a Heterogeneous System -- Computing Small Discrete Logarithms Faster -- Embedded Syndrome-Based Hashing -- Compact Hardware Implementations of the Block Ciphers mCrypton, NOEKEON, and SEA -- A New Model of Binary Elliptic Curves -- Symmetric Key Design and Provable Security SipHash: a fast short-input PRF.

Sommario/riassunto

This book constitutes the refereed proceedings of the 12th International Conference on Cryptology in India, INDOCRYPT 2011, held in Chennai, India, in December 2011. The 22 revised full papers presented together with the abstracts of 3 invited talks and 3 tutorials were carefully reviewed and selected from 127 submissions. The papers are organized in topical sections on side-channel attacks, secret-key cryptography, hash functions, pairings, and protocols.