1.

Record Nr.	UNINA9910484070403321
Titolo	Progress in cryptology : INDOCRYPT 2009 : 10th International Conference on Cryptology in India, New Delhi, India, December 13-16, 2009 ; proceedings / / Bimal Roy, Nicolas Sendrier (eds.)
Pubbl/distr/stampa	Berlin ; ; New York, : Springer-Verlag, c2009
ISBN	1-280-38330-5 9786613561220 3-642-10628-5
Edizione	[1st ed. 2009.]
Descrizione fisica	1 online resource (XV, 443 p.)
Collana	Lecture notes in computer science, , 0302-9743 ; ; 5922
Classificazione	DAT 465f SS 4800
Altri autori (Persone)	RoyBimal SendrierNicolas
Disciplina	004n/a
Soggetti	Computer security Cryptography
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	Post-Quantum Cryptology -- Secure Parameters for SWIFFT -- FSBday -- Key Agreement Protocols -- Reusing Static Keys in Key Agreement Protocols -- A Study of Two-Party Certificateless Authenticated Key-Agreement Protocols -- Side Channel Attacks -- Fault Analysis of Rabbit: Toward a Secret Key Leakage -- On Physical Obfuscation of Cryptographic Algorithms -- Cache Timing Attacks on Clefia -- Symmetric Cryptology -- Software Oriented Stream Ciphers Based upon FCSRs in Diversified Mode -- On the Symmetric Negabent Boolean Functions -- Improved Meet-in-the-Middle Attacks on AES -- Hash Functions -- Related-Key Rectangle Attack of the Full HAS-160 Encryption Mode -- Second Preimage Attack on SHAMATA-512 -- Towards Secure and Practical MACs for Body Sensor Networks -- Indifferentiability Characterization of Hash Functions and Optimal Bounds of Popular Domain Extensions -- A Distinguisher for the Compression Function of SIMD-512 -- Number Theoretic Cryptology -- Sampling from Signed Quadratic Residues: RSA Group Is Pseudofree -- Software Implementation of Pairing-Based Cryptography on Sensor

Networks Using the MSP430 Microcontroller -- A New Hard-Core Predicate of Paillier’s Trapdoor Function -- Lightweight Cryptology -- Private Interrogation of Devices via Identification Codes -- RFID Distance Bounding Multistate Enhancement -- Two Attacks against the F f RFID Protocol -- Signature Protocols -- Efficient Constructions of Signcryption Schemes and Signcryption Composability -- On Generic Constructions of Designated Confirmer Signatures -- Verifiably Encrypted Signatures from RSA without NIZKs -- Identity Based Aggregate Signcryption Schemes -- Multiparty Computation -- Round Efficient Unconditionally Secure MPC and Multiparty Set Intersection with Optimal Resilience -- Non-committing Encryptions Based on Oblivious Naor-Pinkas Cryptosystems -- Oblivious Multi-variate Polynomial Evaluation.

Sommario/riassunto

This book constitutes the refereed proceedings of the 10th International Conference on Cryptology in India, INDOCRYPT 2009, held in New Dehli, India, in December 2009. The 28 revised full papers were carefully reviewed and selected from 104 submissions. The papers are organized in topical sections on post-quantum cryptology, key agreement protocols, side channel attacks, symmetric cryptology, hash functions, number theoretic cryptology, lightweight cryptology, signature protocols, and multiparty computation.