1.

Record Nr.	UNISA996466269403316
Titolo	Information Security and Cryptology [[electronic resource]] : 4th International Conference, Inscrypt 2008, Beijing, China, December 14-17, 2008, Revised Selected Papers / / edited by Moti Yung, Peng Liu, Dongdai Lin
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2009
ISBN	3-642-01440-2
Edizione	[1st ed. 2009.]
Descrizione fisica	1 online resource (XIII, 439 p.)
Collana	Security and Cryptology ; ; 5487
Classificazione	DAT 465f SS 4800
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Coding theory Information theory Data protection Electronic data processing—Management Computers and civilization Computer networks Cryptology Coding and Information Theory Data and Information Security IT Operations Computers and Society Computer Communication Networks
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	International conference proceedings.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Invited Talks -- The State of Hash Functions and the NIST SHA-3 Competition -- Key Evolution Systems in Untrusted Update Environments -- Secure and Privacy-Preserving Information Brokering -- Digital Signature and Signcryption Schemes -- Provably Secure Convertible Nominative Signature Scheme -- Cryptanalysis of Two Ring

Signcryption Schemes -- Efficient Signcryption Key Encapsulation without Random Oracles -- Privacy and Anonymity -- Strong Anonymous Signatures -- Publicly Verifiable Privacy-Preserving Group Decryption -- Privacy for Private Key in Signatures -- Message Authentication Code and Hash Function -- Security of Truncated MACs -- Security Analysis of Multivariate Polynomials for Hashing -- Secure Protocols -- SPVT-II: An Efficient Security Protocol Verifier Based on Logic Programming -- Batch ZK Proof and Verification of OR Logic -- Symmetric Cryptography -- Constructing Variable-Length PRPs and SPRPs from Fixed-Length PRPs -- Impossible Differential Analysis of Reduced Round CLEFIA -- Reducible Polynomial over Constructed by Trinomial ??LFSR -- Certificateless Cryptography -- Chosen Ciphertext Secure Certificateless Threshold Encryption in the Standard Model -- Further Observations on Certificateless Public Key Encryption -- Hardware Implementation and Side Channel Attack -- Efficient Hardware Architecture of SHA-256 Algorithm for Trusted Mobile Computing -- New Elliptic Curve Multi-scalar Multiplication Algorithm for a Pair of Integers to Resist SPA -- Wireless Network Security -- A Novel Marking Probability Distribution Using Probability Propagation in Hierarchical WSN -- Key Predistribution Schemes Using Codes in Wireless Sensor Networks -- Efficient Multi-PKG ID-Based Signcryption for Ad Hoc Networks -- Public Key and Identity Based Cryptography -- On the Computational Efficiency of XTR+ -- A Variant of Boneh-Gentry-Hamburg’s Pairing-Free Identity Based Encryption Scheme -- Inter-domain Identity-Based Proxy Re-encryption -- Access Control and Network Security -- Hardening Botnet by a Rational Botmaster -- Separation of Duty in Trust-Based Collaboration -- Trusted Computing and Applications -- An Integrity Assurance Mechanism for Run-Time Programs -- A Security and Performance Evaluation of Hash-Based RFID Protocols -- Correction, Optimisation and Secure and Efficient Application of PBD Shuffling.

Sommario/riassunto

This book constitutes the thoroughly refereed post-conference proceedings of the 4th International Conference on Information Security and Cryptology, Inscrypt 2008, held in Beijing, China, in December 2008. The 28 revised full papers presented together with 3 invited talks were carefully reviewed and selected from 183 submissions. The papers are organized in topical sections on digital signature and signcryption schemes, privacy and anonymity, message authentication code and hash function, secure protocols, symmetric cryptography, certificateless cryptography, hardware implementation and side channel attack, wireless network security, public key and identity based cryptography, access control and network security, as well as trusted computing and applications.