1. Record Nr. UNINA9910484083503321

Titolo	Information security and privacy : 12th Australasian conference, ACISP 2007, Townsville, Australia, July 2-4, 2007 : proceedings / / Josef Pieprzyk, Hossein Ghodosi, Ed Dawson (eds.)
Pubbl/distr/stampa	Berlin, Germany ; ; New York, New York : , : Springer, , [2007] ©2007
ISBN	3-540-73458-9
Edizione	[1st ed. 2007.]
Descrizione fisica	1 online resource (XIV, 476 p.)
Collana	Security and Cryptology ; ; 4586
Disciplina	005.8
Soggetti	Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Stream Ciphers -- An Analysis of the Hermes8 Stream Ciphers -- On the Security of the LILI Family of Stream Ciphers Against Algebraic Attacks -- Strengthening NLS Against Crossword Puzzle Attack -- Hashing -- A New Strategy for Finding a Differential Path of SHA-1 -- Preimage Attack on the Parallel FFT-Hashing Function -- Second Preimages for Iterated Hash Functions and Their Implications on MACs -- On Building Hash Functions from Multivariate Quadratic Equations -- Biometrics -- An Application of the Goldwasser-Micali Cryptosystem to Biometric Authentication -- Soft Generation of Secure Biometric Keys -- Secret Sharing -- Flaws in Some Secret Sharing Schemes Against Cheating -- Efficient (k,n) Threshold Secret Sharing Schemes Secure Against Cheating from n???1 Cheaters -- Cryptanalysis -- Related-Key Amplified Boomerang Attacks on the Full-Round Eagle-64 and Eagle-128 -- Analysis of the SMS4 Block Cipher -- Forgery Attack to an Asymptotically Optimal Traitor Tracing Scheme -- Public Key Cryptography -- : A Hardware-Oriented Trapdoor Cipher -- Anonymity on Paillier's Trap-Door Permutation -- Generic Certificateless Key Encapsulation Mechanism -- Double-Size Bipartite Modular Multiplication -- Affine Precomputation with Sole Inversion in Elliptic Curve Cryptography -- Construction of Threshold (Hybrid) Encryption in the Random Oracle Model: How to Construct Secure Threshold Tag-KEM from Weakly Secure Threshold KEM -- Efficient Chosen-Ciphertext

Secure Identity-Based Encryption with Wildcards -- Authentication -- Combining Prediction Hashing and MDS Codes for Efficient Multicast Stream Authentication -- Certificateless Signature Revisited -- Identity-Committable Signatures and Their Extension to Group-Oriented Ring Signatures -- Hash-and-Sign with Weak Hashing Made Secure -- “Sandwich” Is Indeed Secure: How to Authenticate a Message with Just One Hashing -- Threshold Anonymous Group Identification and Zero-Knowledge Proof -- Non-interactive Manual Channel Message Authentication Based on eTCR Hash Functions -- E-Commerce -- A Practical System for Globally Revoking the Unlinkable Pseudonyms of Unknown Users -- Efficient and Secure Comparison for On-Line Auctions -- Practical Compact E-Cash -- Security -- Use of Dempster-Shafer Theory and Bayesian Inferencing for Fraud Detection in Mobile Communication Networks -- On Proactive Perfectly Secure Message Transmission.