1. Record Nr. UNINA9910449985403321

Autore	Davey Sheila
Titolo	State of the world's vaccines and immunization [[electronic resource] /] / [text written by Sheila Davey]
Pubbl/distr/stampa	Geneva, : World Health Organization, 2002
Descrizione fisica	xv, 97 p
Disciplina	614.4/7/083
Soggetti	Immunization of children - Planning Communicable diseases in children - Prevention Electronic books.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph

2. Record Nr. UNIORUON00033915

Autore	LI Baojia
Titolo	Guanchang Xianxing Ji / Li Baojia
Pubbl/distr/stampa	Shenyang, : Shunfeng Wenyi Chubanshe, 1994 544 p. ; 21 cm
Classificazione	CIN VI AA
Soggetti	Letteratura cinese - Età classica - Testi
Lingua di pubblicazione	Cinese
Formato	Materiale a stampa
Livello bibliografico	Monografia

3. Record Nr. UNINA9910484083503321

Titolo	Information Security and Privacy : 12th Australasian Conference, ACISP 2007, Townsville, Australia, July 2-4, 2007, Proceedings / / edited by Josef Pieprzyk, Hossein Ghodosi, Ed Dawson
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2007
ISBN	3-540-73458-9
Edizione	[1st ed. 2007.]
Descrizione fisica	1 online resource (XIV, 476 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 4586
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Electronic data processing - Management Data protection Computer networks Coding theory Information theory Algorithms Cryptology IT Operations Data and Information Security Computer Communication Networks Coding and Information Theory

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.
Sommario/riassunto	Here is a highly relevant book that covers a wide array of key aspects in information security. It constitutes the refereed proceedings of the 12th Australasian Conference on Information Security and Privacy held in Townsville, Australia in July 2007. The 33 revised full papers presented were carefully reviewed and selected from 132 submissions. The papers are organized in topical sections on stream ciphers, hashing, biometrics, secret sharing, cryptanalysis, public key cryptography, authentication, e-commerce, and security.