1. Record Nr.   UNINA9910466912603321

   Autore   Naicker Sigamoney Manicka

   Titolo   Inclusive education in South Africa and the developing world : the
                      search for an inclusive pedagogy / / Sigamoney Manicka Naicker

   Pubbl/distr/stampa Bingley, UK : , : Emerald Publishing, , 2018

   ISBN   1-78743-962-3
                      1-78743-690-X

   Descrizione fisica 1 online resource (xiii, 188 pages)

   Collana   Emerald Points

   Disciplina   371.9046

   Soggetti   Inclusive education - South Africa
                      Electronic books.

   Lingua di pubblicazione Inglese

   Formato   Materiale a stampa

   Livello bibliografico Monografia

2.	Record Nr.	UNINA9910483817703321
	Titolo	Cryptology and Network Security : 7th International Conference, CANS 2008, Hong-Kong, China, December 2-4, 2008. Proceedings / / edited by Matthew Franklin, Lucas Chi-Kwong Hui, Duncan S. Wong
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2008
	ISBN	3-540-89641-4
	Edizione	[1st ed. 2008.]
	Descrizione fisica	1 online resource (XIII, 395 p.)
	Collana	Security and Cryptology, , 2946-1863 ; ; 5339
	Disciplina	005.8
	Soggetti	Cryptography
		Data encryption (Computer science)
		Computer networks
		Data protection
		Electronic data processing - Management
		Computers and civilization
		Algorithms
		Cryptology
		Computer Communication Networks
		Data and Information Security
		IT Operations
		Computers and Society
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	International conference proceedings.
	Nota di bibliografia	Includes bibliographical references and author index.
	Nota di contenuto	Cryptosystems -- Chosen-Ciphertext Secure Proxy Re-encryption without Pairings -- Hybrid Damgård Is CCA1-Secure under the DDH Assumption -- Efficient Dynamic Broadcast Encryption and Its Extension to Authenticated Dynamic Broadcast Encryption -- Cryptanalysis of Short Exponent RSA with Primes Sharing Least Significant Bits -- Signatures -- Efficient and Short Certificateless Signature -- Sanitizable Signatures Revisited -- An Efficient On-Line/Off-Line Signature Scheme without Random Oracles -- On the Security of Online/Offline Signatures and Multisignatures from ACISP'

06 -- Identification, Authentication and Key Management -- A Killer Application for Pairings: Authenticated Key Establishment in Underwater Wireless Sensor Networks -- Anonymous and Transparent Gateway-Based Password-Authenticated Key Exchange -- Cryptanalysis of EC-RAC, a RFID Identification Protocol -- Cryptographic Algorithms and Protocols -- Counting Method for Multi-party Computation over Non-abelian Groups -- Keyword Field-Free Conjunctive Keyword Searches on Encrypted Data and Extension for Dynamic Groups -- Analysis and Design of Multiple Threshold Changeable Secret Sharing Schemes -- Black-Box Constructions for Fully-Simulatable Oblivious Transfer Protocols -- Skew Frobenius Map and Efficient Scalar Multiplication for Pairing–Based Cryptography -- Stream Ciphers and Block Ciphers -- Cryptanalysis of MV3 Stream Cipher -- 3D: A Three-Dimensional Block Cipher -- Cryptographic Foundations -- Construction of Resilient Functions with Multiple Cryptographic Criteria -- Enumeration of Homogeneous Rotation Symmetric Functions over F p -- Unconditionally Reliable Message Transmission in Directed Hypergraphs -- Applications and Implementations -- An Open Framework for Remote Electronic Elections -- Conditional Payments forComputing Markets -- High-Speed Search System for PGP Passphrases -- Workload Characterization of a Lightweight SSL Implementation Resistant to Side-Channel Attacks -- Security in Ad Hoc Networks and Wireless Sensor Networks -- Authenticated Directed Diffusion -- A New Message Recognition Protocol for Ad Hoc Pervasive Networks.

| Sommario/riassunto | This book constitutes the refereed proceedings of the 7th International Conference on Cryptology and Network Security, CANS 2008, held in Hong-Kong, China, in December 2008. The 27 revised full papers presented were carefully reviewed and selected from 73 submissions. The papers are organized in topical sections on cryptosystems, signatures, identification, authentication and key management, cryptographic algorithms and protocols, stream ciphers and block ciphers, cryptographic foundations, applications and implementations, as well as security in ad hoc networks and wireless sensor networks. |