1.	Record Nr.	UNISA996465527903316
	Titolo	Advances in cryptology, ASIACRYPT 2008 : 14th International Conference on the Theory and Application of Cryptology and Information Security, Melbourne, Australia, December 7-11, 2008, proceedings / / Josef Pieprzyk (editor)
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer-Verlag, , [2008] ©2008
	ISBN	3-540-89255-9
	Edizione	[1st ed. 2008.]
	Descrizione fisica	1 online resource (XIV, 572 p.)
	Collana	Lecture Notes in Computer Science ; ; 5350
	Disciplina	005.82
	Soggetti	Data encryption (Computer science) Computer security
	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	Multi-Party Computation -- MPC vs. SFE : Unconditional and Computational Security -- Strongly Multiplicative and 3-Multiplicative Linear Secret Sharing Schemes -- Graph Design for Secure Multiparty Computation over Non-Abelian Groups -- Invited Talk -- Some Perspectives on Complexity-Based Cryptography -- Cryptographic Protocols I -- A Modular Security Analysis of the TLS Handshake Protocol -- Ambiguous Optimistic Fair Exchange -- Compact Proofs of Retrievability -- On the Security of HB# against a Man-in-the-Middle Attack -- Cryptographic Hash Functions I -- Hash Functions from Sigma Protocols and Improvements to VSH -- Slide Attacks on a Class of Hash Functions -- Basing PRFs on Constant-Query Weak PRFs: Minimizing Assumptions for Efficient Symmetric Cryptography -- Cryptographic Protocols II -- Universally Composable Adaptive Oblivious Transfer -- A Linked-List Approach to Cryptographically Secure Elections Using Instant Runoff Voting -- Towards Robust Computation on Encrypted Data -- Efficient Protocols for Set Membership and Range Proofs -- Cryptographic Hash Functions II -- Preimage Attacks on 3, 4, and 5-Pass HAVAL -- How to Fill Up Merkle-Damgård Hash Functions -- Limits of Constructive Security Proofs -- Public-Key Cryptography I -- Efficient Chosen Ciphertext Secure Public

Key Encryption under the Computational Diffie-Hellman Assumption -- Twisted Edwards Curves Revisited -- On the Validity of the ?-Hiding Assumption in Cryptographic Protocols -- Chosen Ciphertext Security with Optimal Ciphertext Overhead -- Lattice-Based Cryptography -- Concurrently Secure Identification Schemes Based on the Worst-Case Hardness of Lattice Problems -- Rigorous and Efficient Short Lattice Vectors Enumeration -- Solving Linear Equations Modulo Divisors: On Factoring Given Any Bits -- Private-Key Cryptography -- An Infinite Class of Balanced Functions with Optimal Algebraic Immunity, Good Immunity to Fast Algebraic Attacks and Good Nonlinearity -- An Improved Impossible Differential Attack on MISTY1 -- Public-Key Cryptography II -- Generalized Identity Based and Broadcast Encryption Schemes -- Speeding Up the Pollard Rho Method on Prime Fields -- Sufficient Conditions for Intractability over Black-Box Groups: Generic Lower Bounds for Generalized DL and DH Problems -- OAEP Is Secure under Key-Dependent Messages -- Analysis of Stream Ciphers -- Cryptanalysis of Sosemanuk and SNOW 2.0 Using Linear Masks -- A New Attack on the LEX Stream Cipher -- Breaking the F-FCSR-H Stream Cipher in Real Time.

Sommario/riassunto

This book constitutes the refereed proceedings of the 14th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2008, held in Melbourne, Australia, in December 2008. The 33 revised full papers presented together with the abstract of 1 invited lecture were carefully reviewed and selected from 208 submissions. The papers are organized in topical sections on muliti-party computation, cryptographic protocols, cryptographic hash functions, public-key cryptograhy, lattice-based cryptography, private-key cryptograhy, and analysis of stream ciphers.