1.	Record Nr.	UNISA996466296903316
	Titolo	Information Security and Privacy [[electronic resource]] : 15th Australasian Conference, ACISP 2010, Sydney, Australia, July 5-7, 2010, Proceedings / / edited by Ron Steinfeld, Philip Hawkes
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2010
	ISBN	1-280-38765-3 9786613565570 3-642-14081-5
	Edizione	[1st ed. 2010.]
	Descrizione fisica	1 online resource (XII, 403 p. 40 illus.)
	Collana	Security and Cryptology ; ; 6168
	Disciplina	005.8
	Soggetti	Computer security Data encryption (Computer science) Computer communication systems Management information systems Computer science Algorithms Computer science—Mathematics Systems and Data Security Cryptology Computer Communication Networks Management of Computing and Information Systems Algorithm Analysis and Problem Complexity Discrete Mathematics in Computer Science Sydney <2010>
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Bibliographic Level Mode of Issuance: Monograph
	Nota di bibliografia	Includes bibliographical references and index.
	Nota di contenuto	Symmetric Key Encryption -- Cryptanalysis of a Generalized Unbalanced Feistel Network Structure -- Improved Algebraic Cryptanalysis of QUAD, Bivium and Trivium via Graph Partitioning on Equation Systems -- On Multidimensional Linear Cryptanalysis -- Side-Channel Analysis of the K2 Stream Cipher -- On Unbiased Linear

Approximations -- Hash Functions -- Distinguishers for the Compression Function and Output Transformation of Hamsi-256 -- Second-Preimage Analysis of Reduced SHA-1 -- Some Observations on Indifferentiability -- Public Key Cryptography -- Adaptive and Composable Non-committing Encryptions -- Relations among Notions of Complete Non-malleability: Indistinguishability Characterisation and Efficient Construction without Random Oracles -- Strong Knowledge Extractors for Public-Key Encryption Schemes -- A Multi-trapdoor Commitment Scheme from the RSA Assumption -- Identity-Based Chameleon Hash Scheme without Key Exposure -- The Security Model of Unidirectional Proxy Re-Signature with Private Re-Signature Key -- Security Estimates for Quadratic Field Based Cryptosystems -- Solving Generalized Small Inverse Problems -- Protocols -- One-Time-Password-Authenticated Key Exchange -- Predicate-Based Key Exchange -- Attribute-Based Authenticated Key Exchange -- Optimally Tight Security Proofs for Hash-Then-Publish Time-Stamping -- Additive Combinatorics and Discrete Logarithm Based Range Protocols -- Proof-of-Knowledge of Representation of Committed Value and Its Applications -- Network Security -- Pattern Recognition Techniques for the Classification of Malware Packers -- Repelling Sybil-Type Attacks in Wireless Ad Hoc Systems.