1.	Record Nr.	UNINA9910482979003321
	Titolo	Advances in Information and Computer Security : 4th International Workshop on Security, IWSEC 2009 Toyama, Japan, October 28-30, 2009 Proceedings / / edited by Tsuyoshi Takagi, Masahiro Mambo
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2009
	ISBN	3-642-04846-3
	Edizione	[1st ed. 2009.]
	Descrizione fisica	1 online resource (XII, 229 p.)
	Collana	Security and Cryptology, , 2946-1863 ; ; 5824
	Classificazione	DAT 465f SS 4800
	Altri autori (Persone)	MamboMasahiro TakagiTsuyoshi
	Disciplina	005.8
	Soggetti	Data protection Computer networks Computer programming Operating systems (Computers) Electronic data processing - Management Computers and civilization Data and Information Security Computer Communication Networks Programming Techniques Operating Systems 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 index.
	Nota di contenuto	Invited Talk -- The Future of Cryptographic Algorithms -- Block Cipher -- Bit-Free Collision: Application to APOP Attack -- Impossible Boomerang Attack for Block Cipher Structures -- Improved Distinguishing Attacks on HC-256 -- Cryptographic Protocols -- A Generic Construction of Timed-Release Encryption with Pre-open Capability -- An Efficient Identity-Based Signcryption Scheme for Multiple Receivers -- Universal Designated Verifier Signatures with

Threshold-Signers -- Reducing Complexity Assumptions for Oblivious Transfer -- Protection and Intrusion Detection -- Tamper-Tolerant Software: Modeling and Implementation -- An Error-Tolerant Variant of a Short 2-Secure Fingerprint Code and Its Security Evaluation -- Efficient Intrusion Detection Based on Static Analysis and Stack Walks -- Authentication -- Strongly Secure Authenticated Key Exchange without NAXOS' Approach -- ID-Based Group Password-Authenticated Key Exchange -- A Proposal of Efficient Remote Biometric Authentication Protocol.

Sommario/riassunto	This book constitutes the refereed proceedings of the 4th International Workshop on Security, IWSEC 2009, held in Toyama, Japan, in October 2009. The 13 revised full papers presented together with 1 invited talk were carefully reviewed and selected from 46 submissions. The papers are organized in topical sections on block cipher, cryptographic protocols, contents protection and intrusion detection, as well as authentication.