1. Record Nr. UNINA9910484216603321

Titolo	Information Security : 12th International Conference, ISC 2009 Pisa, Italy, September 7-9, 2009 Proceedings / / edited by Pierangela Samarati, Moti Yung, Fabio Martinelli, Claudio Agostino Ardagna
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2009
ISBN	3-642-04474-3
Edizione	[1st ed. 2009.]
Descrizione fisica	1 online resource (XIV, 508 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 5735
Classificazione	DAT 050f DAT 460f SS 4800
Altri autori (Persone)	SamaratiPierangela ArdagnaClaudio A MartinelliFabio YungMoti
Disciplina	005.822gerDNB
Soggetti	Computer science - Mathematics Computer programming Cryptography Data encryption (Computer science) Data protection Algorithms Mathematics of Computing Programming Techniques Cryptology Data and Information Security Mathematical Applications in Computer Science
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	Analysis Techniques -- A New Approach to ? 2 Cryptanalysis of Block Ciphers -- Analysis and Optimization of Cryptographically Generated Addresses -- Security Analysis of the PACE Key-Agreement Protocol -- Towards Security Notions for White-Box Cryptography -- A Calculus to Detect Guessing Attacks -- Hash Functions -- Structural Attacks on

Two SHA-3 Candidates: Blender-n and DCH-n -- Meet-in-the-Middle Attacks Using Output Truncation in 3-Pass HAVAL -- On Free-Start Collisions and Collisions for TIB3 -- Database Security and Biometrics -- Detection of Database Intrusion Using a Two-Stage Fuzzy System -- Combining Consistency and Confidentiality Requirements in First-Order Databases -- Cancelable Iris Biometrics Using Block Re-mapping and Image Warping -- Iris Recognition in Nonideal Situations -- Algebraic Attacks and Proxy Re-Encryption -- Efficient Conditional Proxy Re-encryption with Chosen-Ciphertext Security -- Practical Algebraic Attacks on the Hitag2 Stream Cipher -- A New Construction of Boolean Functions with Maximum Algebraic Immunity -- Distributed System Security -- A2M: Access-Assured Mobile Desktop Computing -- Automated Spyware Collection and Analysis -- Towards Unifying Vulnerability Information for Attack Graph Construction -- Traitor Tracing without A Priori Bound on the Coalition Size -- SISR – A New Model for Epidemic Spreading of Electronic Threats -- Identity Management and Authentication -- An Efficient Distance Bounding RFID Authentication Protocol: Balancing False-Acceptance Rate and Memory Requirement -- Robust Authentication Using Physically Unclonable Functions -- Risks of the CardSpace Protocol -- Applied Cryptography -- Fair E-Cash: Be Compact, Spend Faster -- On the Security of Identity Based Ring Signcryption Schemes -- A Storage Efficient Redactable Signature inthe Standard Model -- Generic Construction of Stateful Identity Based Encryption -- Access Control -- Privacy-Aware Attribute-Based Encryption with User Accountability -- Hardware-Assisted Application-Level Access Control -- Towards Trustworthy Delegation in Role-Based Access Control Model -- Secure Interoperation in Multidomain Environments Employing UCON Policies -- Specification and Enforcement of Static Separation-of-Duty Policies in Usage Control -- MAC and Nonces -- Nonce Generators and the Nonce Reset Problem -- MAC Precomputation with Applications to Secure Memory -- HMAC without the “Second” Key -- P2P and Web Services -- Adding Trust to P2P Distribution of Paid Content -- Peer-to-Peer Architecture for Collaborative Intrusion and Malware Detection on a Large Scale -- F3ildCrypt: End-to-End Protection of Sensitive Information in Web Services.

Sommario/riassunto

This book constitutes the refereed proceedings of the 12th International Conference on Information Security Conference, ISC 2009, held in Pisa, Italy, September 7-9, 2009. The 29 revised full papers and 9 revised short papers presented were carefully reviewed and selected from 105 submissions. The papers are organized in topical sections on analysis techniques, hash functions, database security and biometrics, algebraic attacks and proxy re-encryption, distributed system security, identity management and authentication, applied cryptography, access control, MAC and nonces, and P2P and Web services.