1.

Record Nr.	UNISA996465992403316
Titolo	Information security practice and experience : 4th international conference, ispec 2008 sydney, australia, april 21-23, 2008 proceedings / / edited by Liqun Chen, Yi Mu, Willy Susilo
Pubbl/distr/stampa	Germany : , : Springer, , [2008] Â©2008
ISBN	3-540-79104-3
Edizione	[1st ed. 2008.]
Descrizione fisica	1 online resource (XIII, 420 p.)
Collana	Security and Cryptology ; ; 4991
Disciplina	005.8
Soggetti	Computer security Data protection Computer networks - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Verification of Integrity and Secrecy Properties of a Biometric Authentication Protocol -- An On-Line Secure E-Passport Protocol -- Secure Multi-Coupons for Federated Environments: Privacy-Preserving and Customer-Friendly -- 1-out-of-n Oblivious Signatures -- A Formal Study of the Privacy Concerns in Biometric-Based Remote Authentication Schemes -- Private Query on Encrypted Data in Multi-user Settings -- Towards Tamper Resistant Code Encryption: Practice and Experience -- A New Public Key Broadcast Encryption Using Boneh-Boyen-Goh’s HIBE Scheme -- RSA Moduli with a Predetermined Portion: Techniques and Applications -- Variants of the Distinguished Point Method for Cryptanalytic Time Memory Trade-Offs -- Secure Cryptographic Precomputation with Insecure Memory -- Securing Peer-to-Peer Distributions for Mobile Devices -- Unified Rate Limiting in Broadband Access Networks for Defeating Internet Worms and DDoS Attacks -- Combating Spam and Denial-of-Service Attacks with Trusted Puzzle Solvers -- PROBE: A Process Behavior-Based Host Intrusion Prevention System -- Towards the World-Wide Quantum Network -- Synthesising Monitors from High-Level Policies for the Safe Execution of Untrusted Software -- Mediator-Free Secure Policy Interoperation of Exclusively-Trusted Multiple Domains -- Privacy of

Recent RFID Authentication Protocols -- A New Hash-Based RFID Mutual Authentication Protocol Providing Enhanced User Privacy Protection -- An Efficient Countermeasure against Side Channel Attacks for Pairing Computation -- Efficient Arithmetic on Subfield Elliptic Curves over Small Finite Fields of Odd Characteristic -- Secure Computation of the Vector Dominance Problem -- Rational Secret Sharing with Repeated Games -- Distributed Private Matching and Set Operations -- Computational Soundness of Non-Malleable Commitments -- Square Attack on Reduced-Round Zodiac Cipher -- Analysis of Zipper as a Hash Function -- On the Importance of the Key Separation Principle for Different Modes of Operation.