

1. Record Nr.	UNINA9910483449803321
Titolo	Cryptology and Network Security [[electronic resource]] : 4th International Conference, CANS 2005, Xiamen, China, December 14-16, 2005, Proceedings // edited by Yvo G. Desmedt, Huaxiong Wang, Yi Mu, Yongqing Li
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2005
Edizione	[1st ed. 2005.]
Descrizione fisica	1 online resource (XII, 352 p.)
Collana	Security and Cryptology ; ; 3810
Disciplina	005.8
Soggetti	Computer communication systems Data encryption (Computer science) Operating systems (Computers) Management information systems Computer science Computers and civilization Algorithms Computer Communication Networks Cryptology Operating Systems Management of Computing and Information Systems Computers and Society Algorithm Analysis and Problem Complexity
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	Cryptanalysis -- The Second-Preimage Attack on MD4 -- On the Security of Certificateless Signature Schemes from Asiacrypt 2003 -- On the Security of a Group Signcryption Scheme from Distributed Signcryption Scheme -- Cryptanalysis of Two Group Key Management Protocols for Secure Multicast -- Security Analysis of Password-Authenticated Key Agreement Protocols -- Intrusion Detection and Viruses -- An Immune-Based Model for Computer Virus Detection -- A

New Model for Dynamic Intrusion Detection -- Self Debugging Mode for Patch-Independent Nullification of Unknown Remote Process Infection -- A New Unsupervised Anomaly Detection Framework for Detecting Network Attacks in Real-Time -- Authentication and Signature -- ID-Based Aggregate Signatures from Bilinear Pairings -- Efficient Identity-Based Signatures and Blind Signatures -- How to Authenticate Real Time Streams Using Improved Online/Offline Signatures -- New Authentication Scheme Based on a One-Way Hash Function and Diffie-Hellman Key Exchange -- Signcryption -- Two Proxy Signcryption Schemes from Bilinear Pairings -- Constructing Secure Warrant-Based Proxy Signcryption Schemes -- E-mail Security -- Design and Implementation of an Inline Certified E-mail Service -- Efficient Identity-Based Protocol for Fair Certified E-mail Delivery -- Cryptosystems -- Similar Keys of Multivariate Quadratic Public Key Cryptosystems -- A Note on Signed Binary Window Algorithm for Elliptic Curve Cryptosystems -- Constructions of Almost Resilient Functions -- Privacy and Tracing -- A Novel Method to Maintain Privacy in Mobile Agent Applications -- Non-expanding Transaction Specific Pseudonymization for IP Traffic Monitoring -- Information Hiding -- Reevaluation of Error Correcting Coding in Watermarking Channel -- Firewalls, Denial of Service and DNS Security -- On the Performance and Analysis of DNS Security Extensions -- On Securing RTP-Based Streaming Content with Firewalls -- Safeguard Information Infrastructure Against DDoS Attacks: Experiments and Modeling -- Trust Management -- Distributed Credential Chain Discovery in Trust-Management with Parameterized Roles.
