1. Record Nr.   UNISA996466177403316

   Titolo   Information Security Practice and Experience [[electronic resource]] :
                         9th International Conference, ISPEC 2013, Lanzhou, China, May 12-14,
                         2013, Proceedings / / edited by Robert H. Deng, Tao Feng

   Pubbl/distr/stampa   Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer,
                         , 2013

   ISBN   3-642-38033-6

   Edizione   [1st ed. 2013.]

   Descrizione fisica   1 online resource (XIV, 388 p. 72 illus.)

   Collana   Security and Cryptology ; ; 7863

   Disciplina   005.8

   Soggetti   Computer security
                         Data encryption (Computer science)
                         Management information systems
                         Computer science
                         Systems and Data Security
                         Cryptology
                         Management of Computing and Information Systems

   Lingua di pubblicazione   Inglese

   Formato   Materiale a stampa

   Livello bibliografico Monografia

   Note generali   Bibliographic Level Mode of Issuance: Monograph

   Nota di contenuto   Enhancing False Alarm Reduction Using Pool-based Active Learning in
                         Network Intrusion Detection -- Trusted Identity Management for
                         Overlay Networks -- Situational Awareness for Improving Network
                         Resilience Management -- Optimal Defense Strategies for DDoS
                         defender using Bayesian Game Model -- Identity-Based Cryptography
                         -- Attribute Specified Identity-Based Encryption -- Leakage-resilient
                         Attribute-based Encryption with Fast Decryption: Models, Analysis and
                         Constructions -- Identity-based Multisignature with Message Recovery
                         -- Improving the Message-ciphertext Rate of Lewko's Fully Secure IBE
                         Scheme -- Cryptographic Primitives Accountable Trapdoor Sanitizable
                         Signatures -- A Conditional Proxy Broadcast Re-Encryption Scheme
                         Supporting Timed-Release -- About Hash into Montgomery Form
                         Elliptic Curves -- Secure RFID Ownership Transfer Protocols -- Leakage
                         Resilient Authenticated Key Exchange Secure in The Auxiliary Input
                         Model -- Expressing User Access Authorization Exceptions in

Conventional Role-based Access Control -- Cryptanalysis of the OKH Authenticated Encryption Scheme.

Sommario/riassunto	This book constitutes the refereed proceedings of the 9th International Conference on Information Security Practice and Experience, ISPEC 2013, held in Lanzhou, China, in May 2013. The 27 revised full papers presented were carefully reviewed and selected from 71 submissions. The papers are organized in topical sections on network security; identity-based cryptography; cryptographic primitives; security protocols; system security; software security and DRM; and cryptanalysis and side channel attacks.