1.

Record Nr.	UNISA996465754303316
Titolo	Provable Security [[electronic resource]] : 7th International Conference, ProvSec 2013, Melaka, Malaysia, October 23-25, 2013, Proceedings / / edited by Willy Susilo, Reza Reyhanitabar
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2013
ISBN	3-642-41227-0
Edizione	[1st ed. 2013.]
Descrizione fisica	1 online resource (X, 347 p. 36 illus.)
Collana	Security and Cryptology ; ; 8209
Disciplina	005.8
Soggetti	Data encryption (Computer science) Computer security Computers and civilization E-commerce Application software Computer science Cryptology Systems and Data Security Computers and Society e-Commerce/e-business Computer Appl. in Administrative Data Processing Computer Science, general
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	On Modeling Terrorist Frauds: Addressing Collusion in Distance Bounding Protocols -- Authenticated Key Exchange Protocols Based on Factoring Assumption -- Efficient, Pairing-Free, Authenticated Identity Based Key Agreement in a Single Round -- CIL Security Proof for a Password-Based Key Exchange -- Non Observability in the Random Oracle Model -- Indistinguishability against Chosen Ciphertext Verification Attack Revisited: The Complete Picture -- Input-Aware Equivocable Commitments and UC-secure Commitments with Atomic Exchanges -- Towards Anonymous Ciphertext Indistinguishability with

Sommario/riassunto

This book constitutes the refereed proceedings of the 7th International Conference on Provable Security, ProvSec 2013, held in Melaka, Malaysia, in October 2013. The 18 full papers presented together with 1 invited talk were carefully reviewed and selected from 44 submissions. The papers cover the following topics: key exchange protocols, security models, signature and signcryption schemes, authenticated encryption, theory, and public key encryption.