1. Record Nr. UNINA9910483360103321

Titolo	Provable security : first international conference, provsec 2007, wollongong, australia, november 1-2, 2007. Proceedings / / edited by Willy Susilo, Joseph K. Liu, Yi Mu
Pubbl/distr/stampa	Berlin, Germany : , : Springer, , [2007] Â©2007
ISBN	3-540-75670-1
Edizione	[1st ed. 2007.]
Descrizione fisica	1 online resource (X, 246 p.)
Collana	Security and Cryptology ; ; 4784
Disciplina	005.8
Soggetti	Computer systems - Access control Cryptography Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Authentication -- Stronger Security of Authenticated Key Exchange -- An Hybrid Approach for Efficient Multicast Stream Authentication over Unsecured Channels -- Asymmetric Encryption -- CCA2-Secure Threshold Broadcast Encryption with Shorter Ciphertexts -- Construction of a Hybrid HIBE Protocol Secure Against Adaptive Attacks -- Signature -- A CDH-Based Strongly Unforgeable Signature Without Collision Resistant Hash Function -- Two Notes on the Security of Certificateless Signatures -- A Provably Secure Ring Signature Scheme in Certificateless Cryptography -- Protocol and Proving Technique -- Complex Zero-Knowledge Proofs of Knowledge Are Easy to Use -- Does Secure Time-Stamping Imply Collision-Free Hash Functions? -- Formal Proof of Provable Security by Game-Playing in a Proof Assistant -- Authentication and Symmetric Encryption (Short Papers) -- Security of a Leakage-Resilient Protocol for Key Establishment and Mutual Authentication -- An Approach for Symmetric Encryption Against Side Channel Attacks in Provable Security -- On the Notions of PRP-RKA, KR and KR-RKA for Block Ciphers -- Signature (Short Papers) -- Practical Threshold Signatures Without Random Oracles -- Aggregate Proxy Signature and Verifiably Encrypted Proxy Signature -- Asymmetric Encryption (Short Papers) -- Formal Security Treatments for Signatures

from Identity-Based Encryption -- Decryptable Searchable Encryption.

Sommario/riassunto

This book constitutes the refereed proceedings of the First International Conference on Provable Security, ProvSec 2007, held in Wollongong, Australia, October 31 - November 2, 2007. The 10 revised full papers presented together with 7 short papers were carefully reviewed and selected from 51 submissions. The papers are organized in topical sections on Authentication, Asymmetric Encryption, Signature, Protocol and Proving Technique, Authentication and Symmetric Encryption, Signature and Asymmetric Encryption.