1. Record Nr. UNINA9910483405503321

Titolo	Provable Security : Second International Conference, ProvSec 2008, Shanghai, China, October 30 - November 1, 2008. Proceedings / / edited by Joon Sang Baek, Feng Bao, Kefei Chen, Xuejia Lai
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2008
ISBN	3-540-88733-4
Edizione	[1st ed. 2008.]
Descrizione fisica	1 online resource (XI, 361 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 5324
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Computer science - Mathematics Data protection Coding theory Information theory Computer science Machine theory Cryptology Mathematics of Computing Data and Information Security Coding and Information Theory Theory of Computation Formal Languages and Automata Theory
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	Encryption -- Generalized ElGamal Public Key Cryptosystem Based on a New Diffie-Hellman Problem -- Tweakable Pseudorandom Permutation from Generalized Feistel Structure -- Timed-Release Encryption Revisited -- Efficient and Provably Secure Certificateless Multi-receiver Signcryption -- A CCA Secure Hybrid Damgård's ElGamal Encryption -- Signature -- Construction of Yet Another Forward Secure Signature Scheme Using Bilinear Maps -- Optimal Online/Offline Signature: How

to Sign a Message without Online Computation -- Round-Optimal Blind Signatures from Waters Signatures -- Secure Proxy Multi-signature Scheme in the Standard Model -- Server-Aided Verification Signatures: Definitions and New Constructions -- Analysis -- On Proofs of Security for DAA Schemes -- Cryptanalysis of Vo-Kim Forward Secure Signature in ICISC 2005 -- Computationally Sound Symbolic Analysis of Probabilistic Protocols with Ideal Setups -- On the Equivalence of Generic Group Models -- The Analysis of an Efficient and Provably Secure ID-Based Threshold Signcryption Scheme and Its Secure Version -- Application of Hash Functions -- Leaky Random Oracle (Extended Abstract) -- How to Use Merkle-Damgård — On the Security Relations between Signature Schemes and Their Inner Hash Functions -- Can We Construct Unbounded Time-Stamping Schemes from Collision-Free Hash Functions? -- Universal Composability -- Relationship of Three Cryptographic Channels in the UC Framework -- A Universally Composable Framework for the Analysis of Browser-Based Security Protocols -- Threshold Homomorphic Encryption in the Universally Composable Cryptographic Library -- Universally Composable Security Analysis of TLS -- Round Optimal Universally Composable Oblivious Transfer Protocols -- Applications -- A Tamper-Evident Voting Machine Resistant to CovertChannels -- Self-healing Key Distribution with Revocation and Resistance to the Collusion Attack in Wireless Sensor Networks.

Sommario/riassunto

This book constitutes the refereed proceedings of the Second International Conference on Provable Security, ProvSec 2008, held in Shanghai, China, October 30 - November 1, 2008. The 25 revised full papers presented were carefully reviewed and selected from 79 submissions. The papers are organized in topical sections on Encryption, Signature, Analysis, Application of Hash Functions, Universal Composability, and Applications.