1.	Record Nr.	UNINA9910484835503321
	Titolo	Provable Security : 8th International Conference, ProvSec 2014, Hong Kong, China, October 9-10, 2014. Proceedings / / edited by Sherman S.M. Chow, Joseph K. Liu, Lucas C.K. Hui, Siu Ming Yiu
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2014
	ISBN	3-319-12475-7
	Edizione	[1st ed. 2014.]
	Descrizione fisica	1 online resource (XVIII, 351 p. 41 illus.)
	Collana	Security and Cryptology ; ; 8782
	Disciplina	005.82
	Soggetti	Data encryption (Computer science) Computer security Computers and civilization Application software Management information systems Computer science Cryptology Systems and Data Security Computers and Society Computer Appl. in Administrative Data Processing 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	Invited Paper -- Password-Based Authenticated Key Exchange: An Overview -- Practical and Provably Secure Attribute Based Encryption -- Fundamental -- Adaptive versus Static Security in the UC Model -- Impossibility of Surjective Icart-Like Encodings -- Symmetric Key Encryption -- On the practical security bound of GF-NLFSR structure with SPN round function -- Misuse-Resistant Variants of the OMD Authenticated Encryption Mode -- A Block-Cipher-Based Hash Function Using an MMO-Type Double-Block Compression Function -- Authentication.-Forward-Secure Sequential Aggregate Message Authentication Revisited: Formalization and a Provably Secure Scheme -- A Provable Secure Batch Authentication Scheme for EPCGen2 Tags --

Signatures -- Generic Transformation to Strongly Existentially Unforgettable Signature Schemes with Leakage Resiliency -- Bounded Pre-Image Awareness and the Security of Hash-Tree Keyless Signatures -- Protocol -- Verifiable Computation in Multiparty Protocols with Honest Majority -- Public Key Encryption -- Lossy Trapdoor Relation and Its Application to Lossy Encryption and Adaptive Trapdoor Relation. -Compact Public Key Encryption with Minimum Ideal Property of Hash Functions -- Proxy Re-Encryption -- RCCA-Secure Multi-use Bidirectional Proxy Re-Encryption with Master Secret Security -- Fine-grained Conditional Proxy Re-encryption and Application -- Predicate Encryption -- Constructing Subspace Membership Encryption through Inner Product Encryption -- Efficient (Anonymous) Compact HIBE From Standard Assumptions -- Attribute-based Cryptosystem -- Computationally Efficient Ciphertext-Policy Attribute-Based Encryption with Constant-Size Ciphertexts -- Attribute-Based Signcryption : Signer Privacy, Strong Unforgetability and IND-CCA2 Security in Adaptive-Predicates Attack -- Short Papers -- How to Use Pseudorandom Generators in Unconditional Security Settings -- Equivalence between MAC and PRF for Blockcipher based Constructions -- A Short Fail-Stop Signature Scheme from Factoring -- Computational Soundness of Asymmetric Bilinear Pairing-based Protocols -- Timed-Release Computational Secret Sharing Scheme and Its Applications -- Deniable Version of SIGMA Key Exchange Protocol Resilient to Ephemeral Key Leakage -- Complete Robustness in Identity-Based Encryption.

Sommario/riassunto

This book constitutes the refereed proceedings of the 8th International Conference on Provable Security, ProvSec 2012, held in Chengdu, China, in September 2012. The 20 full papers and 7 short papers presented together with 2 invited talks were carefully reviewed and selected from 68 submissions. The papers are grouped in topical sections on fundamental, symmetric key encryption, authentication, signatures, protocol, public key encryption, proxy re-encryption, predicate encryption, and attribute-based cryptosystem.