1.

Record Nr.	UNISA996466325403316
Titolo	Provable Security [[electronic resource]] : 12th International Conference, ProvSec 2018, Jeju, South Korea, October 25-28, 2018, Proceedings / / edited by Joonsang Baek, Willy Susilo, Jongkil Kim
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2018
ISBN	3-030-01446-0
Edizione	[1st ed. 2018.]
Descrizione fisica	1 online resource (XI, 424 p. 42 illus.)
Collana	Security and Cryptology ; ; 11192
Disciplina	005.8
Soggetti	Data encryption (Computer science) Software engineering Computer organization Data structures (Computer science) Computers Cryptology Software Engineering/Programming and Operating Systems Computer Systems Organization and Communication Networks Data Structures and Information Theory Computing Milieux
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	On the Leakage of Corrupted Garbled Circuits -- Location-Proof System Based on Secure Multi-Party Computations -- Verifiable Homomorphic Secret Sharing -- Single Private-Key Generator Security Implies Multiple Private-Key Generators Security -- Secure Outsourcing of Cryptographic Circuits Manufacturing -- On the Hardness of Learning Parity with Noise over Rings -- A CCA-Secure Collusion-Resistant Identity-Based Proxy Re-Encryption Scheme -- Multivariate Encryption Schemes Based on the Constrained MQ Problem -- Token-Based Multi-Input Functional Encryption -- On the CCA2 Security of McEliece in the Standard Model -- Efficient Attribute-Based Encryption with BlackBox Traceability -- A Code-Based Linkable Ring Signature Scheme -- Towards Static Assumption Based Cryptosystem in Pairing Setting:

Sommario/riassunto

This book constitutes the refereed proceedings of the 12th International Conference on Provable Security, ProvSec 2018, held in Jeju, South Korea, in October 2018. The 21 full and 4 short papers presented were carefully reviewed and selected from 48 submissions. The papers are grouped in topical sections on foundation. Public key encryption, digital signature, symmetric key cryptography, and applications.