

1. Record Nr.	UNINA9910349399903321
Titolo	Provable Security : 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	005.8 005.82
Soggetti	Cryptography Data encryption (Computer science) Software engineering Computer engineering Computer networks Data structures (Computer science) Information theory Computers Cryptology Software Engineering Computer Engineering and 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: Further Applications of DejaQ and Dual-Form Signature -- Digital Signatures from the Middle-Product LWE -- Generic Double-Authentication Preventing Signatures and a Post-Quantum Instantiation -- A Simpler Construction of Identity-Based Ring Signatures from Lattices -- A Generic Construction of Sequential Aggregate MACs from Any MACs -- Length-Preserving Encryption Based on Single-key Tweakable Block Cipher -- Modeling Privacy in WiFi Fingerprinting Indoor Localization -- Security Notions for Cloud Storage and Deduplication -- Forward Secrecy for SPAKE2 -- User-Mediated Authentication Protocols and Unforgeability for Key Collision -- BAdASS: Preserving Privacy in Behavioural Advertising with Applied Secret Sharing -- Signcryption with Quantum Random Oracles -- Formal Treatment of Verifiable Privacy-Preserving Data-Aggregation Protocols. .

---

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.

---