1.

Record Nr.	UNINA9910508454703321
Titolo	Provable and Practical Security : 15th International Conference, ProvSec 2021, Guangzhou, China, November 5–8, 2021, Proceedings / / edited by Qiong Huang, Yu Yu
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2021
ISBN	3-030-90402-4
Edizione	[1st ed. 2021.]
Descrizione fisica	1 online resource (397 pages)
Collana	Security and Cryptology, , 2946-1863 ; ; 13059
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Computer engineering Computer networks Data protection Cryptology Computer Engineering and Networks Data and Information Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Searchable Encryption -- Public Key Based Searchable Encryption with Fine-Grained Sender Permission Control -- Improved Security Model for Public-key Authenticated Encryption with Keyword Search -- Public Key Encryption with Fuzzy Matching -- Partitioned Searchable Encryption -- Key Exchange & Zero Knowledge Proof -- Key Exposure Resistant Group Key Agreement Protocol -- NIKE from Affine Determinant Programs -- OrBit: OR-Proof Identity-Based Identification with Tight Security for (as low as) 1-bit Loss -- Card-based Zero-knowledge Proof Protocols for Graph Problems and Their Computational Model -- Post Quantum Cryptography -- Recovery Attack on Bob's Reused Randomness in CRYSTALS-KYBER and SABERA Lattice Reduction Algorithm Based on Sublattice BKZ -- On the (M) iNTRU assumption in the integer case -- Functional Encryption -- Verifiable Functional Encryption using Intel SGX -- Fully Secure

Sommario/riassunto

This book constitutes the refereed proceedings of the 15th International Conference on Provable Security, ProvSec 2021, held in Guangzhou, China, in November 2021. The 21 full papers presented were carefully reviewed and selected from 67 submissions. The papers focus on provable security as an essential tool for analyzing security of modern cryptographic primitives. They are divided in the following topical sections: Searchable Encryption, Key Exchange & Zero Knowledge Proof, Post Quantum Cryptography, Functional Encryption, Digital Signature, and Practical Security Protocols.