1.

Record Nr.	UNINA9910427669803321
Titolo	Provable and Practical Security : 14th International Conference, ProvSec 2020, Singapore, November 29 – December 1, 2020, Proceedings / / edited by Khoa Nguyen, Wenling Wu, Kwok Yan Lam, Huaxiong Wang
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2020
ISBN	3-030-62576-1
Edizione	[1st ed. 2020.]
Descrizione fisica	1 online resource (XIII, 423 p. 123 illus., 14 illus. in color.)
Collana	Security and Cryptology, , 2946-1863 ; ; 12505
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Computer engineering Computer networks Data structures (Computer science) Information theory Software engineering Computers Cryptology Computer Engineering and Networks Data Structures and Information Theory Software Engineering Computing Milieux
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Signature Schemes -- Group Signature without Random Oracles from Randomizable Signatures -- Constant-size Lattice-Based Group Signature with Forward Security in the Standard Model -- A Lattice-based Provably Secure Multisignature Scheme in Quantum Random Oracle Model -- Achieving Pairing-Free Aggregate Signatures using Pre-Communication between Signers -- Short Lattice Signatures in the Standard Model with Efficient Tag Generation -- One-Time Delegation of Unlinkable Signing Rights and Its Application -- Watermarkable

Sommario/riassunto

This book constitutes the refereed proceedings of the 14th International Conference on Provable Security, ProvSec 2020, held in Singapore, in November 2020. The 20 full papers presented were carefully reviewed and selected from 59 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: signature schemes, encryption schemes and NIZKS, secure machine learning and multiparty computation, secret sharing schemes, and security analyses. * The conference was held virtually due to the COVID-19 pandemic.