1. Record Nr. UNINA9910349282803321

Titolo	Progress in Cryptology – LATINCRYPT 2019 : 6th International Conference on Cryptology and Information Security in Latin America, Santiago de Chile, Chile, October 2–4, 2019, Proceedings / / edited by Peter Schwabe, Nicolas Thériault
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2019
ISBN	3-030-30530-9
Edizione	[1st ed. 2019.]
Descrizione fisica	1 online resource (X, 385 p. 133 illus., 19 illus. in color.)
Collana	Security and Cryptology ; ; 11774
Disciplina	005.82
Soggetti	Data encryption (Computer science) Computer organization Coding theory Information theory Cryptology Computer Systems Organization and Communication Networks Coding and Information Theory
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Quantum LLL with an Application to Mersenne Number Cryptosystems -- Cryptanalysis -- Breaking randomized mixed-radix scalar multiplication algorithms -- Symmetric Cryptography -- Optimally Indi erentiable Double-Block-Length Hashing without Post-processing and with Support for Longer Key than Single Block -- Side-Channel Analysis -- More Practical Single-Trace Attacks on the Number Theoretic Transform -- Authenticated Encryption with Nonce Misuse and Physical Leakage: Definitions, Separation Results & First Construction -- Stronger and Faster Side-Channel Protections for CSIDH -- Post-Quantum Cryptography -- A Reaction Attack against Cryptosystems based on LRPC Codes -- Lattice-based Zero-knowledge SNARGs for Arithmetic Circuits -- Compact and simple RLWE based key encapsulation mechanism -- Signatures and Protocols -- Compact and simple RLWE based key encapsulation mechanism -- Implementation

-- Compact and simple RLWE based key encapsulation mechanism.

Sommario/riassunto

This book constitutes the proceedings of the 6th International Conference on Cryptology and Security in Latin America, LATINCRYPT 2019, held in Santiago di Chile, Chile, in October 2019. The 18 revised full papers presented were carefully reviewed and selected from 40 submissions. The papers are organized in topical sections on cryptoanalysis, symmetric cryptography, ide-channel cryptography, post-quantum cryptography, signatures and protocols, and implementation.