1. Record Nr.	UNISA996418212203316
Titolo	Advances in cryptology - ASIACRYPT 2020 : 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020 : proceedings, Part I / / Shiho Moriai, Huaxiong Wang (editors)
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2020] ©2020
ISBN	3-030-64837-0
Edizione	[1st ed. 2020.]
Descrizione fisica	1 online resource (XXVII, 914 p. 123 illus.)
Collana	Lecture notes in computer science ; ; 12491
Disciplina	005.82
Soggetti	Data encryption (Computer science) Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Best Paper Awards -- Finding Collisions in a Quantum World: Quantum Black-Box Separation of Collision-Resistance and One-Wayness -- New results on Gimli: full-permutation distinguishers and improved collisions -- SQISign: Compact Post-Quantum signatures from Quaternions and Isogenies -- Encryption Schemes -- Public-Key Generation with Verifiable Randomness -- Simulation-Sound Arguments for LWE and Applications to KDM-CCA2 Security -- CCA-Secure (Puncturable) KEMs from Encryption With Non-Negligible Decryption Errors -- Possibility and Impossibility Results for Receiver Selective Opening Secure PKE in the Multi-Challenge Setting -- Security Reductions for White-Box Key-Storage in Mobile Payments -- Circular Security Is Complete for KDM Security -- Post-Quantum Cryptography -- Scalable Ciphertext Compression Techniques for Post-Quantum KEMs and their Applications -- Post-Quantum Verification of Fujisaki-Okamoto -- A New Decryption Failure Attack against HQC -- Cryptanalysis -- A Bit-Vector Differential Model for the Modular Addition by a Constant -- Mind the Propagation of States New Automatic Search Tool for Impossible Differentials and Impossible Polytopic Transitions -- An Algebraic Formulation of the Division Property: Revisiting Degree Evaluations, Cube Attacks, and Key-

Sommario/riassunto

The three-volume proceedings LNCS 12491, 12492, and 12493 constitutes the proceedings of the 26th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2020, which was held during December 7-11, 2020. The conference was planned to take place in Daejeon, South Korea, but changed to an online format due to the COVID-19 pandemic. The total of 85 full papers presented in these proceedings was carefully reviewed and selected from 316 submissions. The papers were organized in topical sections as follows: Part I: Best paper awards; encryption schemes.- post-quantum cryptography; cryptanalysis; symmetric key cryptography; message authentication codes; side-channel analysis. Part II: public key cryptography; lattice-based cryptography; isogeny-based cryptography; quantum algorithms; authenticated key exchange. Part III: multi-party computation; secret sharing; attribute-based encryption; updatable encryption; zero knowledge; blockchains and contact tracing. .