1. Record Nr. UNINA9910895192003321

Titolo	Global trends in renewable energy investment .. / Frankfurt School FS-UNEP Collaborating Centre for Climate & Sustainable Energy Finance; UN Environment, United Nations Environment Programme; Bloomberg New Energy Finance
Pubbl/distr/stampa	Frankfurt, : Frankfurt School of Finance & Management Nairobi, 2011-
Descrizione fisica	Online-Ressource
Disciplina	333.7 320
Soggetti	Zeitschrift
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Periodico
Note generali	Gesehen am 19.06.2019

2. Record Nr. UNINA9910595028503321

Titolo	Post-Quantum Cryptography : 13th International Workshop, PQCrypto 2022, Virtual Event, September 28–30, 2022, Proceedings / / edited by Jung Hee Cheon, Thomas Johansson
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2022
ISBN	9783031172342 3031172345
Edizione	[1st ed. 2022.]
Descrizione fisica	1 online resource (523 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 13512
Disciplina	005.8 005.82
Soggetti	Cryptography Data encryption (Computer science) Application software Computer networks Cryptology Computer and Information Systems Applications Computer Communication Networks
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Code-Based Cryptography -- Hybrid Decoding - Classical-Quantum Trade-O s for Information Set Decoding -- How to Backdoor (Classic) McEliece and How to Guard Against Backdoors -- LRPC codes with multiple syndromes: near ideal-size KEMs without ideals -- Interleaved Prange: A New Generic Decoder for Interleaved Codes -- A Study of Error Floor Behavior in QC-MDPC Codes -- Multivariate Cryptography and the MinRank Problem -- Improvement of algebraic attacks for superdetermined MinRank -- A New Fault Attack on UOV Multivariate Signature Scheme -- MR-DSS - Smaller MinRank-based (Ring-) Signatures -- IPRainbow -- 2F - A New Method for Constructing E cient Multivariate Encryption Schemes -- Quantum Algorithms, Attacks and Models -- Quantum Attacks on Lai-Massey Structure -- Sponge-based Authenticated Encryption: Security against Quantum Attackers -- Post-

quantum Plaintext-awareness -- On Quantum Ciphertext Indistinguishability, Recoverability, and OAEP -- Implementation and Side channel attacks -- Effciently Masking Polynomial Inversion at Arbitrary Order -- A Power Side-Channel Attack on the Reed-Muller Reed-Solomon Version of the HQC Cryptosystem -- A New Key Recovery Side-Channel Attack on HQC with Chosen Ciphertext -- Isogeny -- On Actively Secure Fine-Grained Access Structures from Isogeny Assumptions -- Attack on SHealS and HealS: the Second Wave of GPST -- Post-Quantum Signal Key Agreement from SIDH -- Lattice-Based Cryptography -- Forward-Secure Revocable Secret Handshakes from Lattices -- Estimating the Hidden Overheads in the BDGL Lattice Sieving Algorithm -- Cryptanalysis -- Breaking Category Five SPHINCS+ with SHA-256.

Sommario/riassunto

This volume constitutes the proceedings of the 13th International Conference on post-quantum cryptography, PQCrypto 2022, held in as a Virtual Event in September 2022. The 23 full papers presented in this volume were carefully reviewed and selected from 66 submissions. They cover a broad spectrum of research within the conference's scope, including code-, hash-, isogeny-, and lattice-based cryptography, multivariate cryptography, and quantum cryptanalysis. The papers are categorized in the following topical sub-headings: Code-Based Cryptography; Multivariate Cryptography and the MinRank Problem; Quantum Algorithims, Attacks and Models; Implementation and Side Channel Attacks; Isogeny; Lattice-based Cryptography; Cryptanalysis.