1. Record Nr. UNINA9910865255803321

Autore	Saarinen Markku-Juhani
Titolo	Post-Quantum Cryptography : 15th International Workshop, PQCrypto 2024, Oxford, UK, June 12–14, 2024, Proceedings, Part I / / edited by Markku-Juhani Saarinen, Daniel Smith-Tone
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
ISBN	9783031627439 9783031627422
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (440 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14771
Altri autori (Persone)	Smith-ToneDaniel
Disciplina	5,824
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	Applications and Protocols -- Post Quantum Secure ZRTP -- A New Hash-based Enhanced Privacy ID Signature Scheme -- Code Based Cryptography -- The Blockwise Rank Syndrome Learning problem and its applications to cryptography -- Reducing Signature Size of Matrix code based Signature Schemes -- Group-Action-Based Cryptography -- CCA Secure Updatable Encryption from Non Mappable Group Actions -- Properties of Lattice Isomorphism as a Cryptographic Group Action -- A Subexponential Quantum Algorithm for the Semidirect Discrete Logarithm Problem -- On digital signatures based on group actions QROM security and ring signatures -- Lattice-Based Cryptography -- Phoenix Hash and Sign with Aborts from Lattice Gagdets -- Efficient Identity Based Encryption with Tight Adaptive Anonymity from RLWE -- An Improved Practical Key Mismatch Attack Against NTRU -- Improved Provable Reduction of NTRU and Hypercubic Lattices -- Compact Encryption based on Module NTRU problems -- Analyzing Pump and

jump BKZ algorithm using dynamical systems.

Sommario/riassunto

The two-volume set LNCS 14771 and 14772 constitutes the refereed proceedings of the 15th International Workshop, PQCrypto 2024, held in Oxford, UK, during June 12–14, 2024. The 28 full papers included in these proceedings were carefully reviewed and selected from 76 submissions. They were organized in topical sections as follows: Part I: Applications and protocols; code-based cryptography; group-action-based cryptography; lattice-based cryptography; Part II: Isogeny-Based cryptgraphy; multivariate cryptography; quantum algorithms; transforms and proofs. .