1. Record Nr. UNINA9910865238503321

Autore	Saarinen Markku-Juhani
Titolo	Post-Quantum Cryptography : 15th International Workshop, PQCrypto 2024, Oxford, UK, June 12–14, 2024, Proceedings, Part II / / edited by Markku-Juhani Saarinen, Daniel Smith-Tone
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
ISBN	9783031627460 9783031627453
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (380 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14772
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	Isogeny-Based Cryptography -- Adaptive attacks against FESTA without input validation or constant time implementation -- Updatable Encryption from Group Actions -- Fault Attack on SQIsign -- Multivariate Cryptography -- Cryptanalysis of the SNOVA Signature Scheme -- One vector to rule them all Key recovery from one vector in UOV schemes -- Polynomial XL A Variant of the XL Algorithm Using Macaulay Matrices over Polynomial Rings -- State of the art of HFE variants Is it possible to repair HFE with appropriate modifiers -- Practical key recovery attack on MQ Sign and more -- Practical and Theoretical Cryptanalysis of VOX.-Quantum Algorithms -- Extending Regevs Factoring Algorithm to Compute Discrete Logarithms -- Transforms and Proofs -- A note on Failing gracefully Completing the picture for explicitly rejecting Fujisaki Okamoto transforms using worst case correctness -- Two Round Threshold Lattice Based Signatures from Threshold Homomorphic Encryption -- Hash your Keys before

	Signing BUFF Security of the Additional NIST PQC Signatures -- Revisiting Anonymity in Post Quantum Public Key Encryption.
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.