1. Record Nr. UNISA996650068703316

Titolo	Post-Quantum Cryptography : 16th International Workshop, PQCrypto 2025, Taipei, Taiwan, April 8–10, 2025, Proceedings, Part I / / edited by Ruben Niederhagen, Markku-Juhani O. Saarinen
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2025
ISBN	3-031-86599-5
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (XIV, 386 p. 44 illus., 15 illus. in color.)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 15577
Disciplina	005.824
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	-- Code-Based Cryptography. -- On the Structure of the Schur Squares of Twisted Generalized Reed-Solomon Codes and Application to Cryptanalysis. -- Quadratic Modelings of Syndrome Decoding. -- An Improved Algorithm for Code Equivalence. -- An Improved Both-May Information Set Decoding Algorithm: Towards More Efficient Time-Memory Trade-Offs. -- Enhancing Threshold Group Action Signature Schemes: Adaptive Security and Scalability Improvements. -- Multivariate Cryptography. -- Share the MAYO: Thresholdizing MAYO. -- SoK: On the Physical Security of UOV-based Signature Schemes. -- Shifting our Knowledge of MQ-Sign Security. -- Lattice-Based Cryptography. -- Module Learning With Errors With Truncated Matrices. -- Lattice-Based Sanitizable Signature Schemes: Chameleon Hash Functions and More. -- Giant Does NOT Mean Strong: Cryptanalysis of BQTRU. -- Batch Anonymous MAC Tokens from Lattices.
Sommario/riassunto	The two-volume set LNCS 15577 + 15578 constitutes the proceedings

of the 16th International Workshop on Post-Quantum Cryptography, PQCrypto 2025, held in Taipei, Taiwan, during April 8–10, 2025. The 25 full papers presented in the proceedings were carefully selected and reviewed from 59 submissions. The papers have been organized in the following topical sections: Part I: Code-Based Cryptography; Multivariate Cryptography; Lattice-Based Cryptography. Part II: Isogeny-Based Cryptography; Cryptanalysis; Quantum Security; Side-Channel Attacks; Security Notions.