1. Record Nr. UNISA996678672203316

Autore	Gee James C
Titolo	Medical Image Computing and Computer Assisted Intervention - MICCAI 2025 : 28th International Conference, Daejeon, South Korea, September 23-27, 2025, Proceedings, Part XIII
Pubbl/distr/stampa	Cham : , : Springer, , 2025 ©2026
ISBN	9783032051691
Edizione	[1st ed.]
Descrizione fisica	1 online resource (1305 pages)
Collana	Lecture Notes in Computer Science Series ; ; v.15972
Altri autori (Persone)	AlexanderDaniel C HongJaesung IglesiasJuan Eugenio SudreCarole H VenkataramanArchana GollandPolina KimChong-hyo ParkJinah
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Sommario/riassunto	The 16-volume set LNCS 15960 - 15975 constitutes the refereed proceedings of the 28th International Conference on Medical Image Computing and Computer Assisted Intervention, MICCAI 2025, which took place in Daejeon, South Korea, during September 23-27, 2025.

2. Record Nr. UNISA996650069403316

Titolo	Post-Quantum Cryptography : 16th International Workshop, PQCrypto 2025, Taipei, Taiwan, April 8–10, 2025, Proceedings, Part II / / edited by Ruben Niederhagen, Markku-Juhani O. Saarinen
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2025
ISBN	3-031-86602-9
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (XIV, 386 p. 64 illus., 32 illus. in color.)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 15578
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	-- Isogeny-Based Cryptography. -- Efficient Theta-Based Algorithms for Computing (,)-Isogenies on Kummer Surfaces for Arbitrary Odd . -- Commuting Ramanujan Graphs and the Random Self-Reducibility of Isogeny Problems. -- Cryptanalysis. -- Discrete Gaussian Sampling for BKZ-Reduced Basis. -- An Efficient Collision Attack on Castryck-Decru-Smith's Hash Function. -- Heuristic Algorithm for Solving Restricted SVP and its Applications. -- Cryptanalysis of an Efficient Signature Based on Isotropic Quadratic Forms. -- Analysis of REDOG: the Pad Thai Attack. -- Quantum Security. -- Quantum IND-CPA Security Notions for AEAD. -- Reducing the Number of Qubits in Solving LWE. -- Side-Channel Attacks. -- Single Trace Side-Channel Attack on the MPC-in-the-Head Framework. -- Et tu, Brute? Side-Channel Assisted Chosen Ciphertext Attacks using Valid Ciphertexts on HQC KEM. -- Security Notions. -- Treating Dishonest Ciphertexts in Post-Quantum KEMs – Explicit vs Implicit Rejection in the FO Transform. -- IND-CPAC: A New Security Notion for Conditional

Decryption in Fully Homomorphic Encryption.

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.