md64, ruaba7, crypto_kem, enc time, ciphertext size, excerpt for NIST Post-Quantum Cryptography Standardization Project

Horizontal axis: Time (cycles) to generate a ciphertext given a public key (crypto_kem, enc).

Vertical axis: Space (bytes) for a ciphertext (crypto_kem_CIPHERTEXTBYTES).

❑ means that the SUPERCOP database does not list IND-CCA2 security as a goal for this primitive.

❑ means that the SUPERCOP database does not list constant time as a goal for this implementation.

https://bench.cr.yp.to

20240108