amd64, dali, crypto_kem, key size, ciphertext size, excerpt for NIST Post-Quantum Cryptography Standardization Project

Horizontal axis: Space (bytes) for a public key (crypto_kem_PUBLICKEYBYTES).

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

"C:" means that the SUPERCOP database does not list IND-CCA2 security as a goal for this primitive. "T:" means that the SUPERCOP database does not list constant time as a goal for this implementation.

https://bench.cr.yp.to

20240912