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

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

- "C:意味する " 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.

The SUPERCOP database does not list IND-CCA2 security as a goal for this primitive.

md64, jasper2, crypto_kem, key size, ciphertext size, excerpt for NIST Post-Quantum Cryptography Standardization Project

[https://bench.cr.yp.to](https://bench.cr.yp.to)

20231109