

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

20201206

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.

