amd64, gcc67, 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).

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

https://bench.cr.yp.to

20200110