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

Horizontal axis: Space (bytest) for a public key (crypto_kem_PUBLICKEYBYTES).
Vertical axis: Space (bytest) for a ciphertext (crypto_kem_CIPHERTEXTBYTES).

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

https://bench.cr.yp.to

20190819