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

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

Horizontal axis: Time (cycles) to generate a public key (crypto_kem_KEYPAIRTIME).

"C" 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.

https://bench.cr.yp.to
20230604