

amd64, nucnu, crypto\_kem, keypair time, key size, excerpt for NIST Post-Quantum Cryptography Standardization Project

Horizontal axis: Time (cycles) to generate a public key (crypto\_kem\_keypair).

Vertical axis: Space (bytes) for a public key (crypto\_kem\_PUBLICKEYBYTES).

“C:” means that the SUPERCOP database does not list IND-CCA2 security as a goal for this primitive. “T:” means that the SUPERCOP database does not list constant time as a goal for this implementation.

