

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.

