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

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

- means that IND-CCA2 security is not a goal for this primitive.  means that the SUPERCOP database does not list constant time as a goal for this implementation.