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

• means that the SUPERCOP database does not list constant time as a goal for this implementation.

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

https://bench.cr.yp.to
20200907
amd64, saaba, crypto_kem, keypair time, key size
Horizontal axis: Time (cycles) to generate a public key (crypto_kem_keypair).