Horizontal axis: Time (cycles) to generate a ciphertext given a public key (crypto_kem.pub).
Vertical axis: Space (bytes) for a ciphertext (crypto_kem.CIPHERTEXTBYTES).

■ 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
20240430