Horizontal axis: Time (cycles) to generate a session key given a ciphertext (crypto_kem_dec).
Vertical axis: Space (bytes) for a ciphertext (crypto_kem_CIPHERTEXTBYTES).

X 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.

crypto_kem, crypto_kem_dec, time, ciphertext size
https://bench.cr.yp.to
20210605
md64, rumba5, crypto_kem, dec time, ciphertext size