Horizontal axis: Time (cycles) to generate a session key given a ciphertext (crypto.kem.keygen).
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.

md64, ruba5, crypto_kem, dec time, ciphertext size
https://bench.cr.yp.to
20240108