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

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.

crypto_kem time, ciphertext size

amd64, saber214, crypto_kem, dec time, ciphertext size

https://bench.cr.yp.to
20240511