horizontal axis: Time (cycles) to generate a session key given a ciphertext (crypto_kem_dec). 20240108
vertical axis: Space (bytes) for a ciphertext (crypto_kem_CIPHERTEXTBYTES).

“C” means that the SUPERCOP database does not list IND-CCA2 security as a goal for this primitive. “T” means that the SUPERCOP database does not list constant time as a goal for this implementation.