Horizontal axis: Space (bytes) for a public key (crypto_kem_PUBLICKEYBYTES).

Vertical axis: Space (bytes) for a ciphertext (crypto_kem_CIPHERTEXTBYTES).

A "•" means that the SUPERCOP database does not list IND-CCA2 security as a goal for this primitive. A "■" means that the SUPERCOP database does not list constant time as a goal for this implementation.