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

- $\times$ means that the SUPERCOP database does not list IND-CCA2 security as a goal for this primitive.
- $\square$ means that the SUPERCOP database does not list constant time as a goal for this implementation.