Supercop: Space-Time Trade-offs for Key Size and Ciphertext Size of Crypto-KEM Primitives

**Horizontal axis:** Space (bytes) for a public key (crypto.kem_PUBLICKEYBYTES).

**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.