

amd64, pmod076, crypto\_kem, key size, ciphertext size  
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.

