

Horizontal axis: Time (cycles) to generate a ciphertext given a public key (crypto_kem_enc).

20190905

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.

