

Horizontal axis: Time (cycles) to generate a session key given a ciphertext (crypto_kem_dec).

20191027

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.

