

Horizontal axis: Time (cycles) to generate a ciphertext given a public key (crypto\_kem\_enc).

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.

