https://bench.cr.yp.to

The graph visualizes the relationship between the size of a public key and the size of a ciphertext for various cryptographic primitives. The axes represent the space (bytes) for a public key and the space (bytes) for a ciphertext, respectively. The color and symbol of each point correspond to specific cryptographic primitives, such as crypto_kem, mceliece, newhope, kindi, locker, kindi256, and others. The SUPERCOP database does not list IND-CCA2 security as a goal for some of these primitives, indicated by "\(\square\)".

The notation "\(\star\)" means that the SUPERCOP database does not list constant time as a goal for this implementation.

For more details, refer to the webpage at https://bench.cr.yp.to.