Horizontal axis: Time (cycles) to generate a public key (crypto_kem.keypair).
Vertical axis: Space (bytes) for a public key (crypto_kem_PUBLICKEYBYTES).

means that the SUPERCOP database does not list IND-CCA2 security as a goal for this primitive.
means that the SUPERCOP database does not list constant time as a goal for this implementation.

The graph shows a comparison of various cryptographic primitives based on their performance in terms of time and space requirements. The x-axis represents the time (cycles) to generate a public key, while the y-axis represents the space (bytes) required for a public key.

Primitives are color-coded to indicate different groups and are labeled with their names and parameters. The graph includes a variety of primitives such as FrodoKem, NewHope, Kyber, NewHope-Lac, etc., each with different time and space requirements.

For example, FrodoKem (frodo128) requires less time and space compared to NewHope (newhope1024cca), which in turn requires less time and space than Kyber (kyber1024).

TheSUPERCOP database does not list IND-CCA2 security as a goal for FrodoKem and NewHope but does for Kyber.