ARCH64, pi4b, crypto_kem, keypair, time, key size, excerpt for NIST Post-Quantum Cryptography Standardization Project.

Horizontal axis: Time (cycles) to generate a public key (crypto_kem_keypair).

Vertical axis: Space (bytes) for a public key (crypto_kem_PUBLICKEYBYTES).

* means 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.