

amd64, freshwrap, little, crypto_sign, open time, key size, excerpt for NIST Post-Quantum Cryptography Standardization Project

Horizontal axis: Time (cycles) to generate a message given a signed message (crypto_sign_open).

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

“T” means that the SUPERCOP database does not list constant time as a goal for this implementation.

