

amd64, rome0, crypto\_sign, keypair time, excerpt for NIST Post-Quantum Cryptography Standardization Project

Horizontal axis: Time (cycles) to generate a public key (crypto\_sign\_keypair).

Vertical axis: Space (bytes) for a public key (crypto\_sign\_PUBLICKEYBYTES).

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

