Horizontal axis: Space (bytes) for a public key (crypto_sign_PUBLICKEYBYTES).
Vertical axis: Space overhead (bytes) for signing a long message (at most crypto_sign_BYTES).

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

- ssh2
- ssh3
- m64
- b3neo
- crypto_sign
- key size
- signature size
-excerpt for NIST Post-Quantum Cryptography Standardization Project

https://bench.cr.yp.to

20231202

T:qtesla3p
T:qtesla1p
dilithium5(,aes)
T:qtesla3f
T:qtesla3s
dilithium3(,aes)
T:mqdss64
dilithium2(,aes)
T:sphincsf256(haraka,shake256)(robust,simple)
T:falcon1024(dyn,tree)
T:sphincsf128(haraka,shake256)(robust,simple)
T:sphincss128(haraka,shake256)(robust,simple)
T:sphincsf192(haraka,shake256)(robust,simple)
T:sphincss192(haraka,shake256)(robust,simple)
T:sphincsf256(haraka,shake256)(robust,simple)
T:sphincsf256(haraka,shake256)(robust,simple)