riscv64, riscvunleashed000, crypto_sign, key size, signature size, excerpt for NIST Post-Quantum Cryptography Standardization Project

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.

- rainbow1c
- rainbow1b
- dilithium5(aes)
- dilithium3(aes)
- mqdss64
- mqdss48
- sphincsf256(haraka, sha256, shake256)(robust, simple)
- falcon1024tree
- falcon1024dyn
- sphincsf128(haraka, sha256, shake256)(robust, simple)
- sphincsf192(haraka, sha256, shake256)(robust, simple)
- sphincsf128(haraka, sha256, shake256)(robust, simple)
- sphincss128(haraka,sha256,sha256,sha256)(robust, simple)