amd64, rumba5, crypto_kem, key size, ciphertext size, excerpt for NIST Post-Quantum Cryptography Standardization Project

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

"C:" means that the SUPERCOP database does not list IND-CCA2 security as a goal for this primitive. "T:" means that the SUPERCOP database does not list constant time as a goal for this implementation.

Benchmarks for various crypto_kem primitives are plotted on a graph with space (bytes) for a public key on the horizontal axis and space (bytes) for a ciphertext on the vertical axis. The graph includes points for different algorithms, such as FrodoKem1344(aes, shake), NTSKem13136, McEliece8192128(), McEliece6688128(), FrodoKem976, FrodoKem976(aes, shake), and others.

For a complete list of benchmarks and their details, please refer to the comprehensive database at https://bench.cr.yp.to.