

amd64, gcc67, crypto_dh, dh time, key size
Horizontal axis: Time (cycles) to generate a shared secret given a public key (crypto_dh).
Vertical axis: Space (bytes) for a public key (crypto_dh_PUBLICKEYBYTES).

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

