

amd64, alder, 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.

