Vertical axis: Space (bytes) for a public key (\texttt{crypto\_kem\_PUBLICKEYBYTES}).

Horizontal axis: Time (cycles) to generate a public key (\texttt{crypto\_kem\_keypair}).

\textbullet\ means that the SUPERCOP database does not list IND-CCA2 security as a goal for this primitive. \rotatebox{90}{\textbullet\ }\ means that the SUPERCOP database does not list constant time as a goal for this implementation.

\texttt{crypto\_kem}\, \texttt{crypto\_kem\_PUBLICKEYBYTES}, arch64, pi3aplus, crypto\_ken, keypair time, key size, excerpt for NIST Post-Quantum Cryptography Standardization Project

https://bench.cr.yp.to
20211124