Horizontal axis: Time (cycles) to generate a session key given a ciphertext (\texttt{crypto\_kem\_dec}).

Vertical axis: Space (bytes) for a ciphertext (\texttt{crypto\_kem\_CIPHERTEXTBYTES}).

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

https://bench.cr.yp.to
20240108