Validated and open-source crypto_kem implementations that were benchmarked in 2024.

Horizontal axis: Time (cycles) to generate a public key (crypto_kem_keypair).
Vertical axis: Space (bytes) for a public key (crypto_kem_PUBLICKEYBYTES).

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

Download the benchmark results at https://bench.cr.yp.to

These results are sorted by ascent order on the vertical axis (space) in their respective category. The sizes of the circles are representative of the area of the points in the graph.

Legend:
- Green circles: IND-CCA2 security
- Orange circles: IND-CPA security
- Blue circles: IND-CPA and IND-dec
- Black circles: IND-CPA, IND-dec and IND-CCA2 security
- Red circles: IND-CPA, IND-dec, IND-CCA2 security, IND-CPA and IND-dec security

The implementations with "•" symbol are not included in the legend to avoid cluttering the chart. The SUPERCOP database does not list IND-CCA2 security as a goal for these primitives.