| Horizontal axis: Space (bytes) for a public key (crypto_kem_PUBLICKEYBYTES). |
| Vertical axis: Space (bytes) for a ciphertext (crypto_kem_CIPHERTEXTBYTES). |

- ❄️ means that the SUPERCOP database does not list constant time as a goal for this implementation.
- 🔴 means that the SUPERCOP database does not list IND-CCA2 security as a goal for this implementation.

```
C: r5n15kem0d
C: r5n13kem0d
C: hila5
C: lake2
C: rolloi128
C: ledakemc33
C: ledakemc52
C: 3bears936r2cpa,
C: r5nd3kem0d
C: r5nd1kem4longkey
C: r5nd3kem5d
C: r5nd5kem0d
T: ledakemc33
T: ledakemc54
C: r5nd1kem0d
C: r5nd1kem5d
C: bikel3
C: 3bears1248r2cpa,
C: lake3
•
C: ledakemc13
C: 3bears624r2cpa,
C: r5nd5kem5d
C: lake1
C: r5nd0kem2iot
C: ledakemc32
C: ledakemc53
C: ledakemc12
```

```
amd64, colossus6, crypto_kem, key size, ciphertext size
```

```
20201018
```

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

```
mrd64, colossus6, crypto_kem, key size, ciphertext size
```

```
Horizontal axis: Space (bytes) for a public key (crypto_kem_PUBLICKEYBYTES).
Vertical axis: Space (bytes) for a ciphertext (crypto_kem_CIPHERTEXTBYTES).
```

- ❄️ means that the SUPERCOP database does not list constant time as a goal for this implementation.
- 🔴 means that the SUPERCOP database does not list IND-CCA2 security as a goal for this implementation.