Horizontal axis: Time (cycles) to generate a ciphertext given a public key (crypto_kem_enc).
Vertical axis: Space (bytes) for a ciphertext (crypto_kem_CIPHERTEXTBYTES).

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

Diagram includes various primitives such as frodokem1344shake, frodokem640shake, ledakem52sl, limasp2062cca, ledakem5264, ntrulpr4591761, sikep751comp, sikep751, titaniumccasuper, ledakem53sl, limasp1822cca, ledakem5364, ledakem54sl, limasp1306cca, ledakem5464, titaniumccamed, ledakem32sl, ledakem3264, ledakem34sl, ledakem3464, ledakem33sl, lima2p2048cca, lima2p1024cca, kindi512321, ntrulpr1277, ntruhps4096821, kyber90s1024, ntrulpr1013, ntruhrss701, ntrulpr953, ntruhps2048677, kyber1024, ntrulpr857, sntrup1277, ntruhps2048509, kyber90s768, ntrulpr761, sntrup1013, sntrup953, kindi512222, kindi512241, newhope1024cca, newhope512cca, saber2, kindi256342, kindi256522, kindi512124, kindi512241, newhope1024cca, newhope512cca, saber2, kindi256342, kindi256522, kindi512124, kindi512241, newhope1024cca, newhope512cca, saber2, kindi256342, kindi256522, kindi512124, kindi512241, newhope1024cca, newhope512cca, saber2, kindi256342, kindi256522, kindi512124, kindi512241.