Hashing and random numbers are provided by crypto_hash and crypto_pseudo_random_bytes, respectively. crypto_kem_PUBLICKEYBYTES represents the size of public keys in bytes. The vertical axis measures the space (bytes) for a public key (crypto_kem_PUBLICKEYBYTES). The horizontal axis measures the time (cycles) to generate a public key (crypto_kem_keypair). 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.