



Notation:  $(d, Q) \leftarrow \text{Curve25519}()$  is the key generation function that generates  $d$  as private key and  $Q$  as public key.