

HYBRID-PRE CONSTRUCTION

function PRE.Setup(1^λ) ▷ Setup
  Choose $\mathbb{G}$ of prime order q with generator g
  return $pp = (g, q)$

function PRE.KG(pp) ▷ Key Generation
  $sk \xleftarrow{\$} \mathbb{Z}_q^*$; $pk \leftarrow g^{sk}$
  return (pk, sk)

function PRE.RKG($(pk_i, sk_i), (pk_j, sk_j)$)
▷ ReKey Generation
  $rk_{i \to j} \leftarrow sk_i / sk_j$
  return $rk_{i \to j}$

function PRE.E(pk, a, m) ▷ Encryption
  $r \xleftarrow{\$} \mathbb{Z}_q^*$; $c_1 \leftarrow g^r$
  $K = F(pk^r)$; $c_2 \leftarrow \mathsf{SE.E}(K, a, m)$
  return (c_1, c_2)

function PRE.D(sk, a, c) ▷ Decryption
  Parse c as (c_1, c_2)
  $K = F(c_1^{sk})$; $m \leftarrow \mathsf{SE.D}(K, a, c)$
  return m

function PRE.RE($rk_{i \to j}, a, c$) ▷ ReEncryption
  Parse c as (c_1, c_2)
  $c_1' \leftarrow c_1^{rk_{i \to j}}$
  return (c_1', c_2)

FIG. 9