Identity based encryption (IBE)

Jiageng Chen

Boneh, D., & Franklin, M. (2001, August). Identity-based encryption from the Weil pairing. In *Annual international cryptology conference* (pp. 213-229). Springer, Berlin, Heidelberg.

Recall: Pub-Key Encryption (PKE)

<u>PKE Three algorithms</u> : (G, E, D)

$G(\lambda) \to (pk, sk)$ outputs pub-key and secret-key

$E(pk, m) \to c$ encrypt m using pub-key pk

$D(sk, c) \to m$ decrypt c using sk

obtain pk_{alice}

$E(\ pk_{alice}\ ,\ \ msg\ )$

Example: ElGamal encryption

- $G(\lambda)$: $(G, g, q) \leftarrow \text{GenGroup}(\lambda)$

  $sk := (\alpha \leftarrow F_p)$; $pk := (h \leftarrow g^\alpha)$

- $E(pk,\ m \in G)$: $s \leftarrow Z_q$ and do $c \leftarrow (g^s,\ m \cdot h^{\mathbf{s}})$

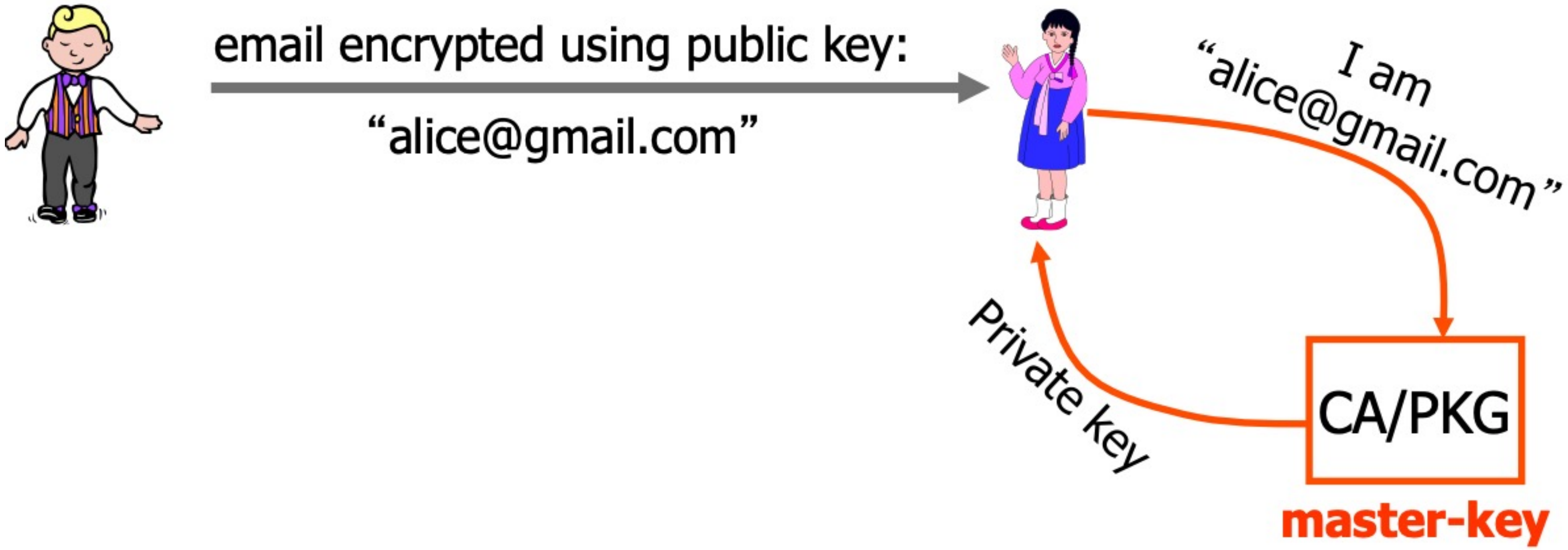
- $D(sk=\alpha,\ c=(c_1,c_2))$: observe $c_1^\alpha = (g^s)^\alpha = h^s$

- Security (IND-CPA) based on the DDH assumption:

  (g, h, g^s, h^s) indist. from (g, h, g^s, g^{rand})

Identity based encryption

- IBE: PKE system where PK is an arbitrary string
  - e.g. e-mail address, phone number, ip address



IBE in practice

Bob encrypts message with pub-key:

$\underbrace{\text{“alice@hotmail} \;||\; \text{role=accounting}}_{\text{policy-based encryption}} \;||\; \underbrace{\text{time=week-num”}}_{\text{short-lived keys}}$

Voltage
security

Aug. 2011: “… Voltage SecureMail … with over one billion secure business emails sent annually and over 50 million worldwide users.”

Four Algorithms

- S *is a probabilistic algorithm invoked as* $(mpk, msk) \xleftarrow{R} S()$, *where* mpk *is called the* ***master public key*** *and* msk *is called the* ***master secret key*** *for the IBE scheme.*

- G *is a probabilistic algorithm invoked as* $sk_{id} \xleftarrow{R} G(msk, id)$, *where* msk *is the master secret key (as output by* S*),* $id \in \mathcal{ID}$ *is an identity, and* sk_{id} *is a secret key for* id.

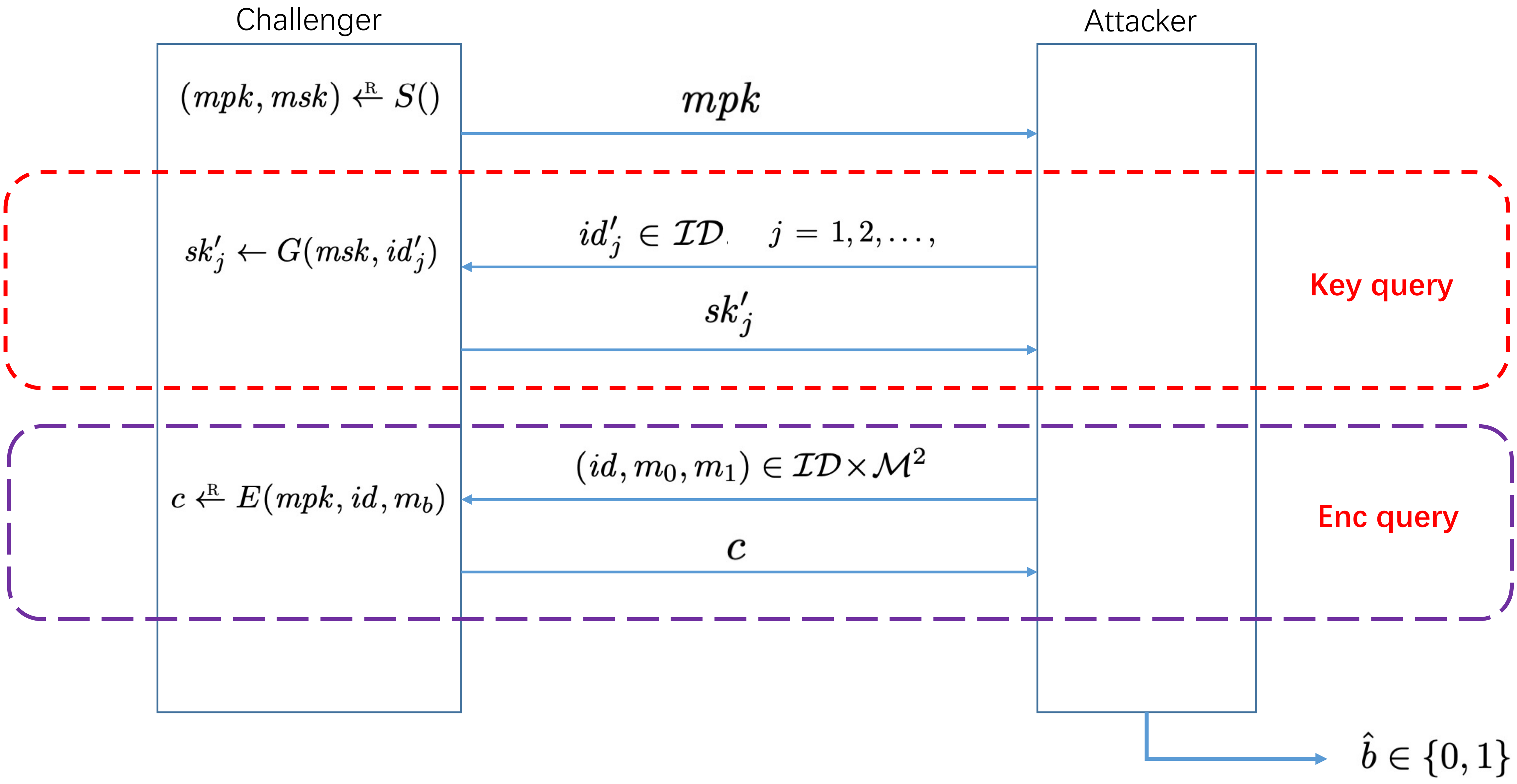
- E *is a probabilistic algorithm invoked as* $c \xleftarrow{R} E(mpk, id, m)$.

- D *is a deterministic algorithm invoked as* $m \leftarrow D(sk_{id}, c)$. *Here* m *is either a message, or a special* reject *value (distinct from all messages).*

- *As usual, we require that decryption undoes encryption; specifically, for all possible outputs* (mpk, msk) *of* S*, all identities* $id \in \mathcal{ID}$*, and all messages* m*, we have*

$$\Pr\Big[D\big(G(msk, id),\ E(mpk, id, m)\big) = m\Big] = 1.$$

Semantic security for IBE



Construction

- $S()$: the setup algorithm runs as follows:

$$\alpha \xleftarrow{\text{R}} \mathbb{Z}_q, \quad u_1 \leftarrow g_1^{\alpha}, \quad mpk \leftarrow u_1, \quad msk \leftarrow \alpha, \quad \text{output } (mpk, msk).$$

- $G(msk, id)$: key generation using $msk = \alpha$ runs as:

$$sk_{id} \leftarrow H_0(id)^{\alpha} \in \mathbb{G}_0, \quad \text{output } sk_{id}.$$

- $E(mpk, id, m)$: encryption using the public parameters $mpk = u_1$ runs as:

$$\beta \xleftarrow{\text{R}} \mathbb{Z}_q, \quad w_1 \leftarrow g_1^{\beta}, \quad z \leftarrow e\big(H_0(id),\ u_1^{\beta}\big) \in \mathbb{G}_{\text{T}},$$
$$k \leftarrow H_1(w_1, z), \quad c \xleftarrow{\text{R}} E_{\text{s}}(k, m), \quad \text{output } (w_1, c).$$

- $D\big(sk_{id},\ (w_1, c)\big)$: decryption using secret key sk_{id} of ciphertext (w_1, c) run as follows:

$$z \leftarrow e(sk_{id}, w_1), \quad k \leftarrow H_1(w_1, z), \quad m \leftarrow D_{\text{s}}(k, c), \quad \text{output } m.$$

$$\boxed{e\big(sk_{id}, w_1\big) = e\big(H_0(id)^{\alpha},\ g_1^{\beta}\big) = e\big(H_0(id),\ g_1^{\alpha\beta}\big) = e\big(H_0(id),\ u_1^{\beta}\big).}$$

Decision-BDH assumption

Pairing: $e : \mathbb{G}_0 \times \mathbb{G}_1 \to \mathbb{G}_T$

Generators: $g_0 \in \mathbb{G}_0$ and $g_1 \in \mathbb{G}_1$

Experiment b $\quad$ **(**$b = 0, 1$**):**

- The challenger computes

$$\alpha, \beta, \gamma, \delta \xleftarrow{\text{R}} \mathbb{Z}_q, \quad u_0 \leftarrow g_0^{\alpha}, \quad u_1 \leftarrow g_1^{\alpha}, \quad v_0 \leftarrow g_0^{\beta}, \quad w_1 \leftarrow g_1^{\gamma},$$
$$z^{(0)} \leftarrow e(g_0, g_1)^{\alpha\beta\gamma} \in \mathbb{G}_T, \quad z^{(1)} \xleftarrow{\text{R}} e(g_0, g_1)^{\delta} \in \mathbb{G}_T$$

  and gives $(u_0, u_1, v_0, w_1, z^{(b)})$ to the adversary.

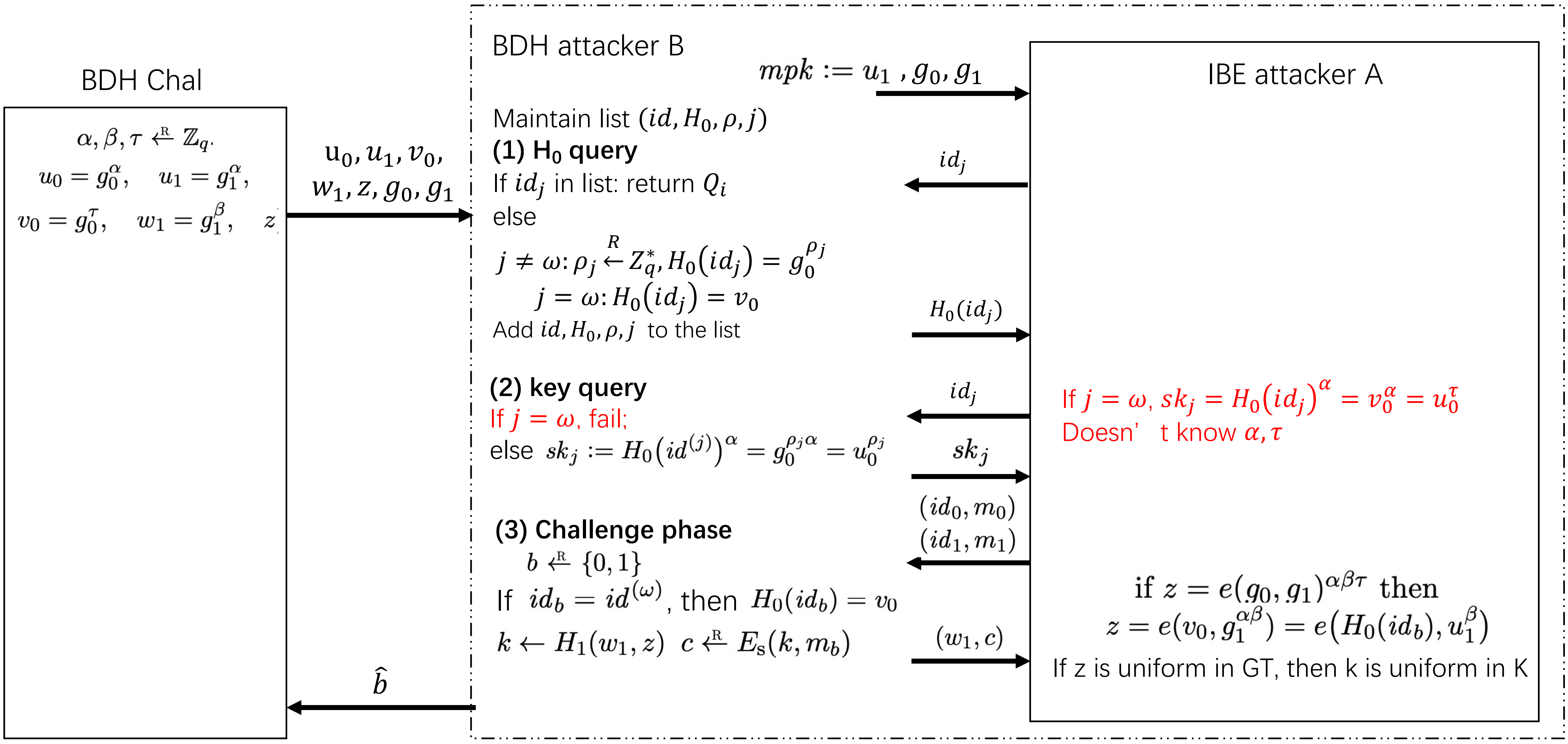
- The adversary outputs a bit $\hat{b} \in \{0, 1\}$.

$$\text{DBDH}\mathsf{adv}[\mathcal{A}, e] := \Big|\Pr[W_0] - \Pr[W_1]\Big|.$$

Security of IBE

Theorem. If decision BDH holds for e, H_0 is modeled as random oracle, H_1 is a secure KDF, and Es is semantically secure, then the IBE scheme is semantically secure.

$$\mathrm{SS}^{\mathrm{ro}}\mathsf{adv}[\mathcal{A}, \mathcal{E}_{\mathrm{BF}}] \leq 2 \cdot 2.72 \cdot (Q_{\mathrm{s}} + 1) \cdot \mathrm{DBDH}\mathsf{adv}[\mathcal{B}_{\mathrm{e}}, e] + 2 \cdot \mathrm{KDF}\mathsf{adv}[\mathcal{B}_{\mathrm{kdf}}, H_1] + \mathrm{SS}\mathsf{adv}[\mathcal{B}_{\mathrm{s}}, \mathcal{E}_{\mathrm{s}}].$$


BDH Chal
$\alpha, \beta, \tau \xleftarrow{R} \mathbb{Z}_q.$
$u_0 = g_0^{\alpha}, \quad u_1 = g_1^{\alpha},$
$v_0 = g_0^{\tau}, \quad w_1 = g_1^{\beta}, \quad z$
$u_0, u_1, v_0,$
w_1, z, g_0, g_1
$\hat{b}$
BDH attacker B
$mpk := u_1, g_0, g_1$
Maintain list (id, H_0, ρ, j)
(1) H_0 query
If id_j in list: return Q_i
else
$j \neq \omega$: $\rho_j \xleftarrow{R} Z_q^*, H_0(id_j) = g_0^{\rho_j}$
$j = \omega$: $H_0(id_j) = v_0$
Add id, H_0, ρ, j to the list
id_j
$H_0(id_j)$
(2) key query
If $j = \omega$, fail;
else $sk_j := H_0(id^{(j)})^{\alpha} = g_0^{\rho_j \alpha} = u_0^{\rho_j}$
id_j
sk_j
(3) Challenge phase
$b \xleftarrow{R} \{0,1\}$
If $id_b = id^{(\omega)}$, then $H_0(id_b) = v_0$
$k \leftarrow H_1(w_1, z) \quad c \xleftarrow{R} E_s(k, m_b)$
(id_0, m_0)
(id_1, m_1)
(w_1, c)
IBE attacker A
If $j = \omega$, $sk_j = H_0(id_j)^{\alpha} = v_0^{\alpha} = u_0^{\tau}$
Doesn' t know α, τ
if $z = e(g_0, g_1)^{\alpha\beta\tau}$ then
$z = e(v_0, g_1^{\alpha\beta}) = e(H_0(id_b), u_1^{\beta})$
If z is uniform in GT, then k is uniform in K