Identity-Based Matchmaking Encryption from Standard Assumptions

Jie Chen

East China Normal University

Yu Li

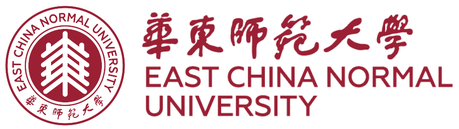
East China Normal University

Jinming Wen

Jinan University

Jian Weng

Jinan University



Asiacrypt 2022

IB-ME from SXDH

Identity-Based Matchmaking Encryption
[AFNV19]

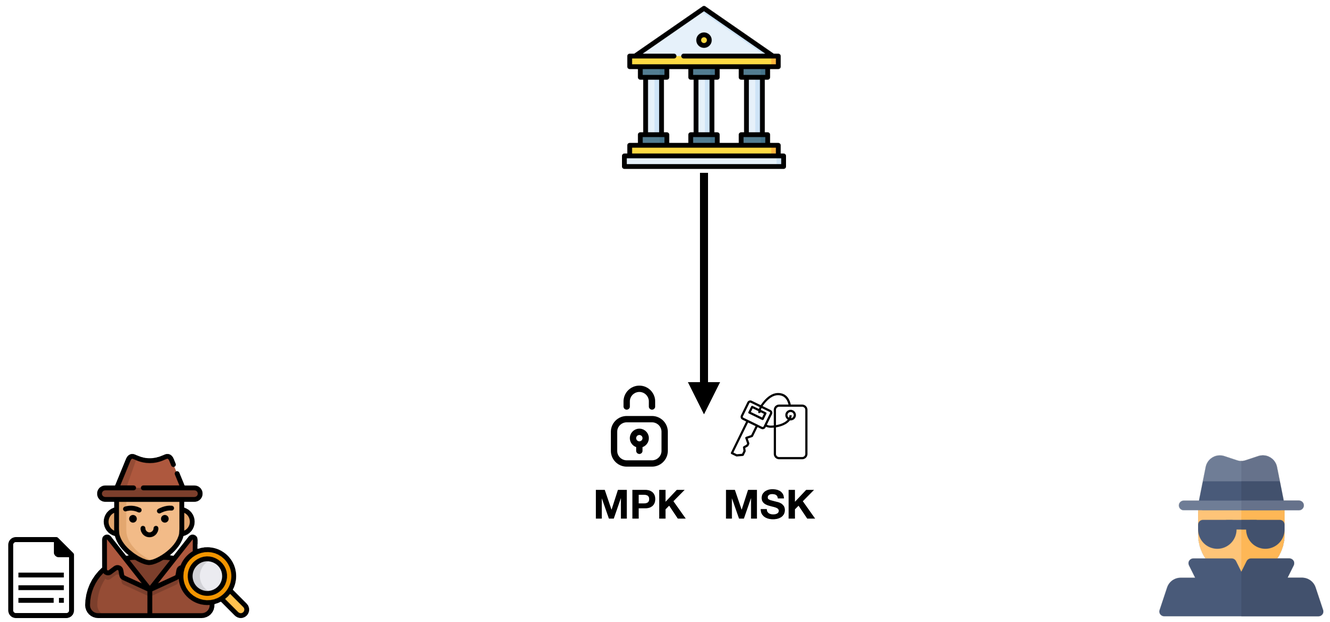
[AFNV19]: Ateniese, G., Francati, D., Nuñez, D., Venturi, D.: Match me if you can: Match- making encryption and its applications. CRYPTO 2019

IB-ME from SXDH

Identity-Based Matchmaking Encryption
[AFNV19]

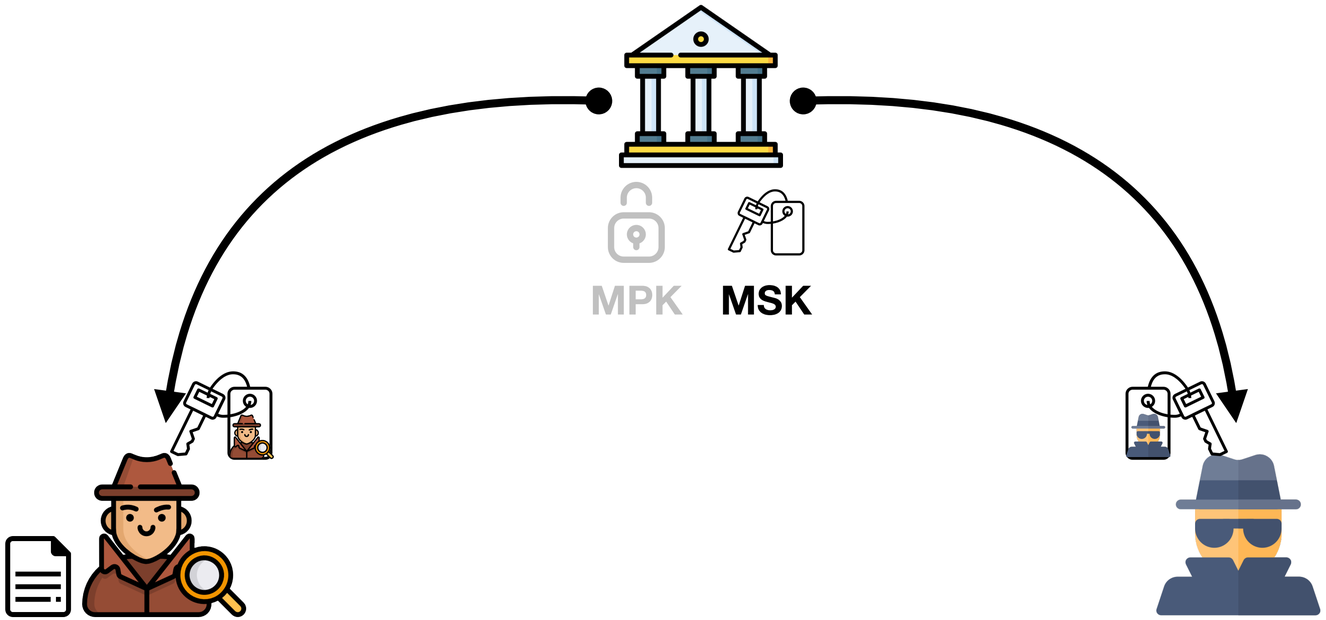
IB-ME from SXDH

Identity-Based Matchmaking Encryption
[AFNV19]



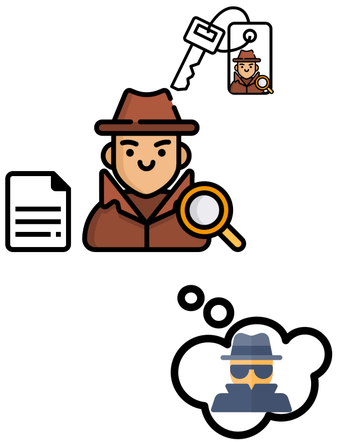
IB-ME from SXDH

Identity-Based Matchmaking Encryption
[AFNV19]



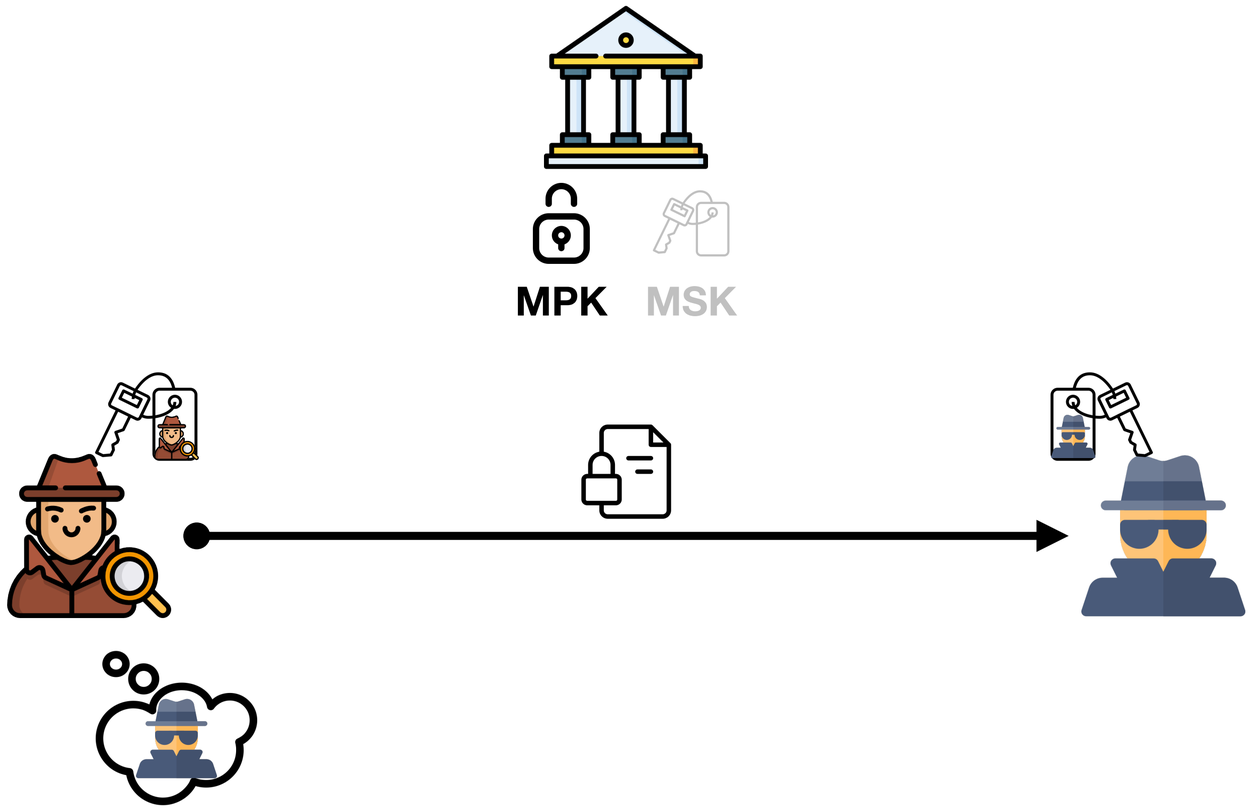
IB-ME from SXDH

Identity-Based Matchmaking Encryption
[AFNV19]



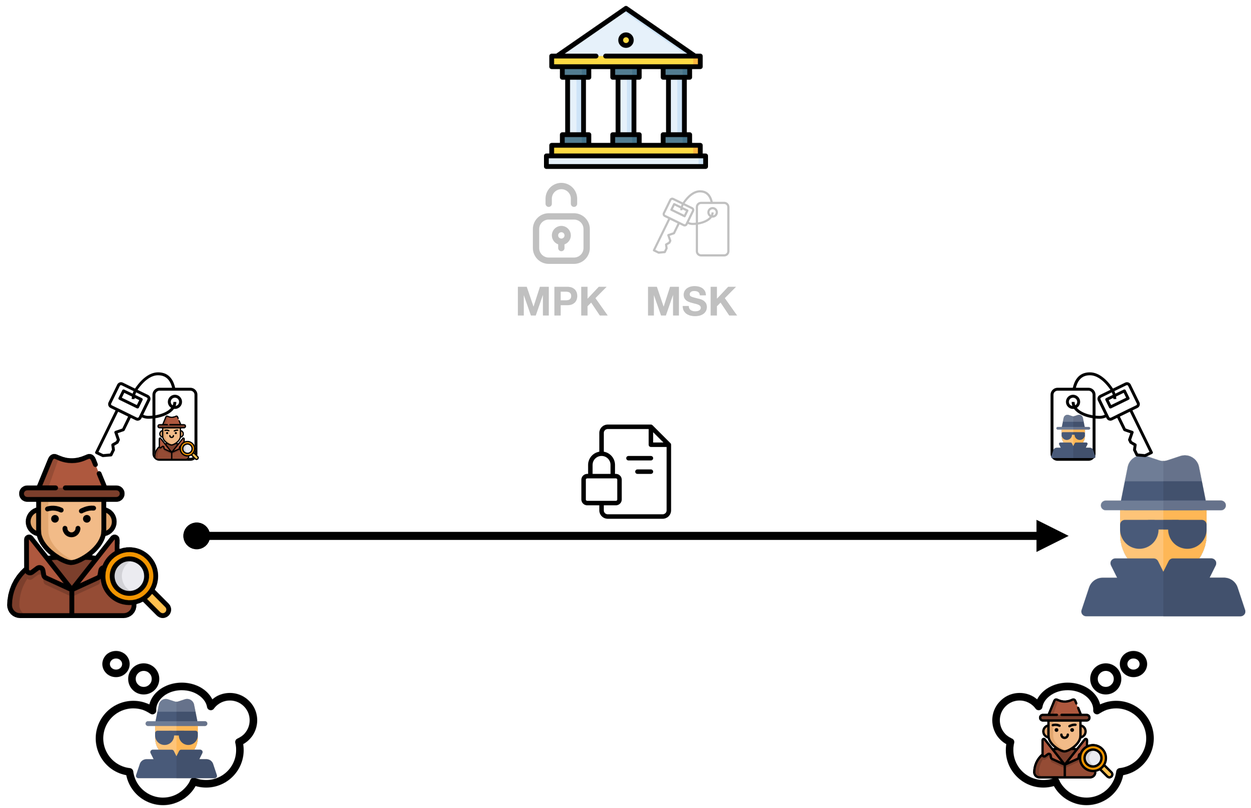
IB-ME from SXDH

Identity-Based Matchmaking Encryption
[AFNV19]



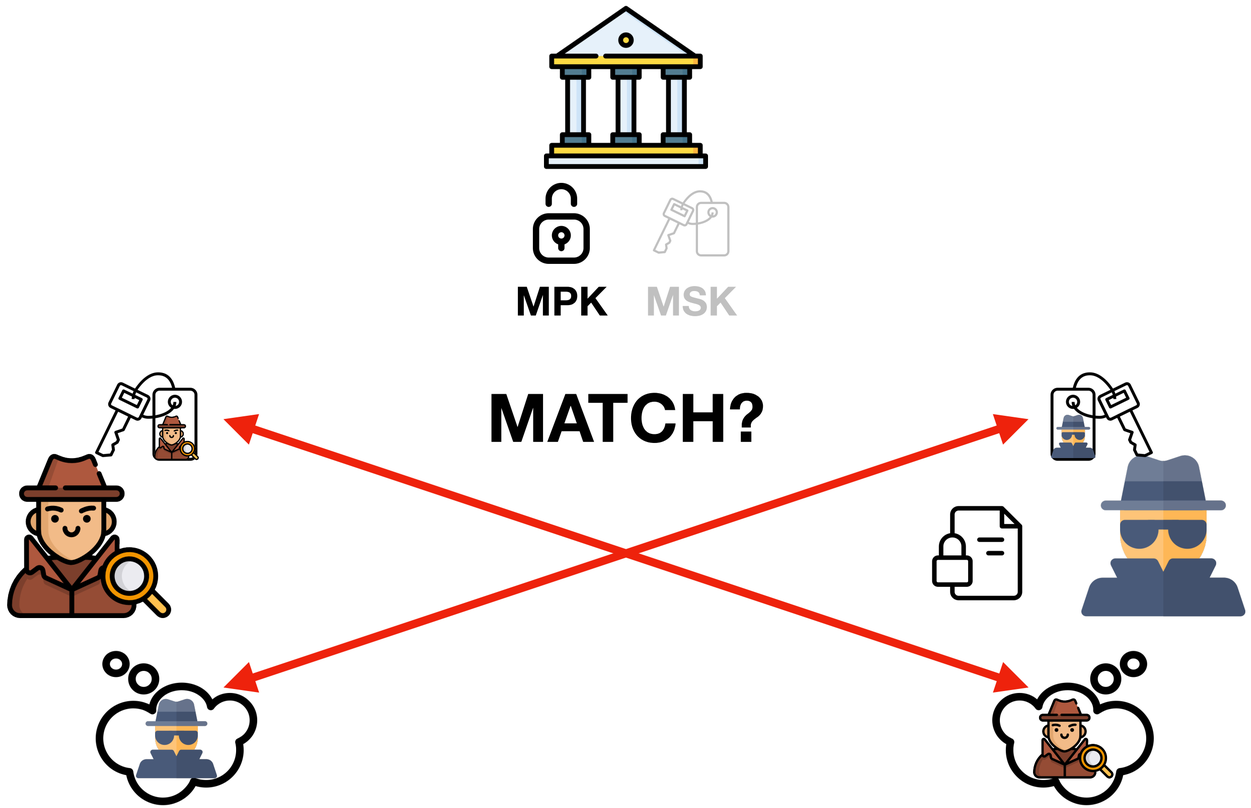
IB-ME from SXDH

Identity-Based Matchmaking Encryption
[AFNV19]



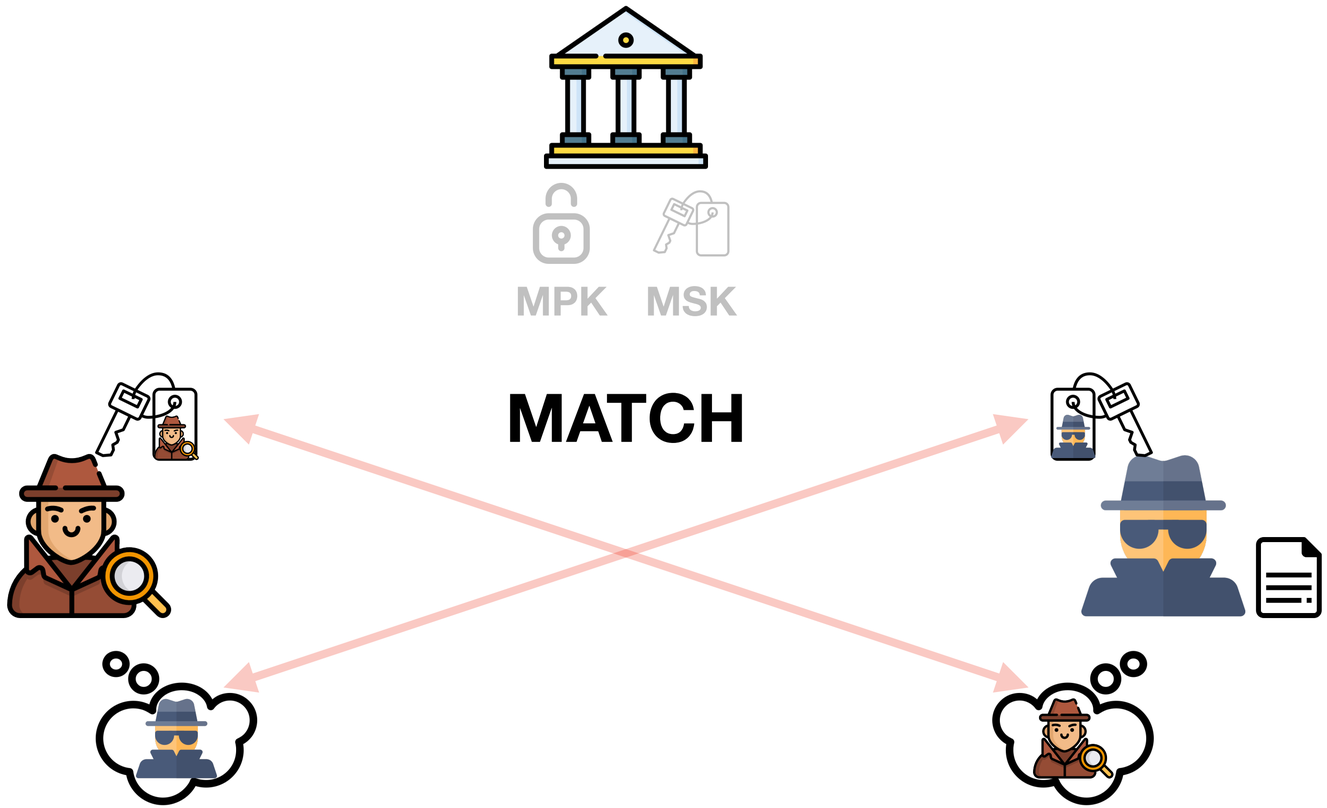
IB-ME from SXDH

Identity-Based Matchmaking Encryption
[AFNV19]



IB-ME from SXDH

Identity-Based Matchmaking Encryption
[AFNV19]



IB-ME from SXDH

Syntax

IB-ME from SXDH

Syntax

Setup ⟶

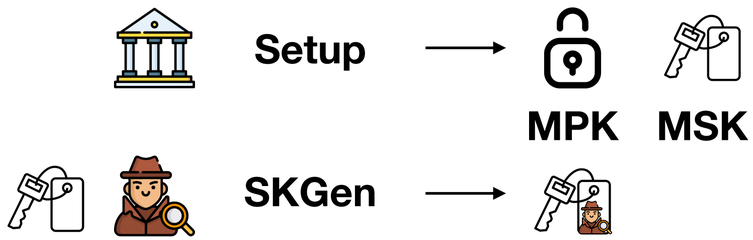
MPK

MSK

$\text{Setup}(1^\lambda) \rightarrow (mpk, msk)$

IB-ME from SXDH

Syntax

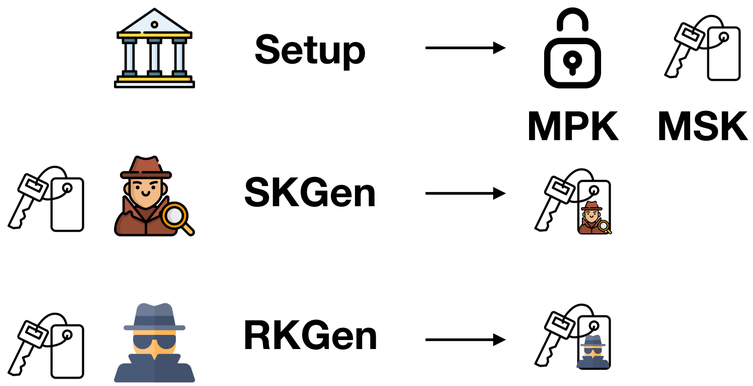


$\mathsf{Setup}(1^\lambda) \rightarrow (mpk, msk)$

$\mathsf{SKGen}(mpk, msk, \sigma) \rightarrow ek_\sigma$

IB-ME from SXDH

Syntax



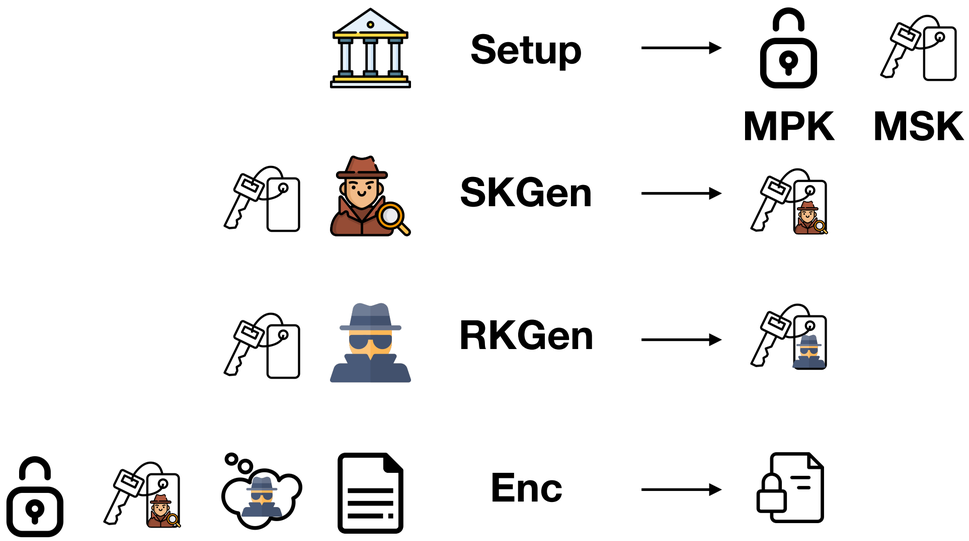
$\mathsf{Setup}(1^\lambda) \rightarrow (mpk, msk)$

$\mathsf{SKGen}(mpk, msk, \sigma) \rightarrow ek_\sigma$

$\mathsf{RKGen}(mpk, msk, \rho) \rightarrow dk_\rho$

IB-ME from SXDH

Syntax



$\mathsf{Setup}(1^\lambda) \rightarrow (mpk, msk)$

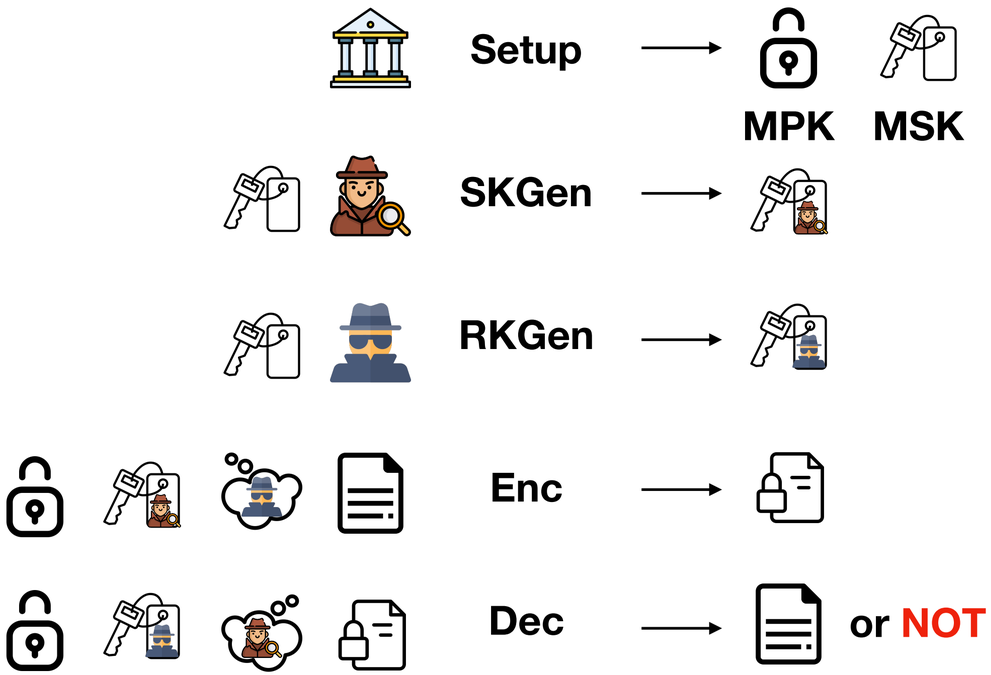
$\mathsf{SKGen}(mpk, msk, \sigma) \rightarrow ek_\sigma$

$\mathsf{RKGen}(mpk, msk, \rho) \rightarrow dk_\rho$

$\mathsf{Enc}(mpk, ek_\sigma, \mathsf{rcv}, m) \rightarrow ct$

IB-ME from SXDH

Syntax



$\mathsf{Setup}(1^\lambda) \rightarrow (mpk, msk)$

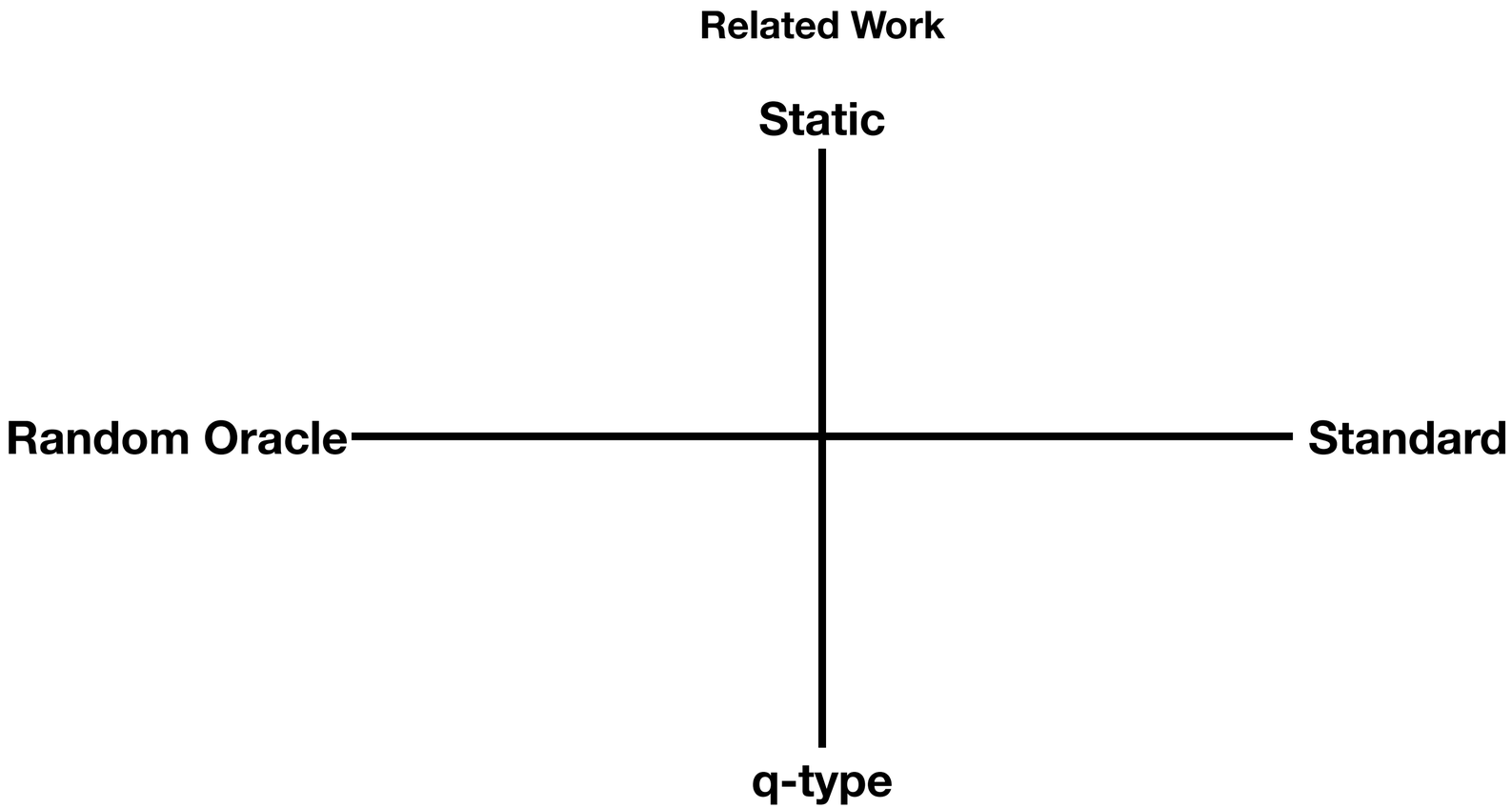
$\mathsf{SKGen}(mpk, msk, \sigma) \rightarrow ek_\sigma$

$\mathsf{RKGen}(mpk, msk, \rho) \rightarrow dk_\rho$

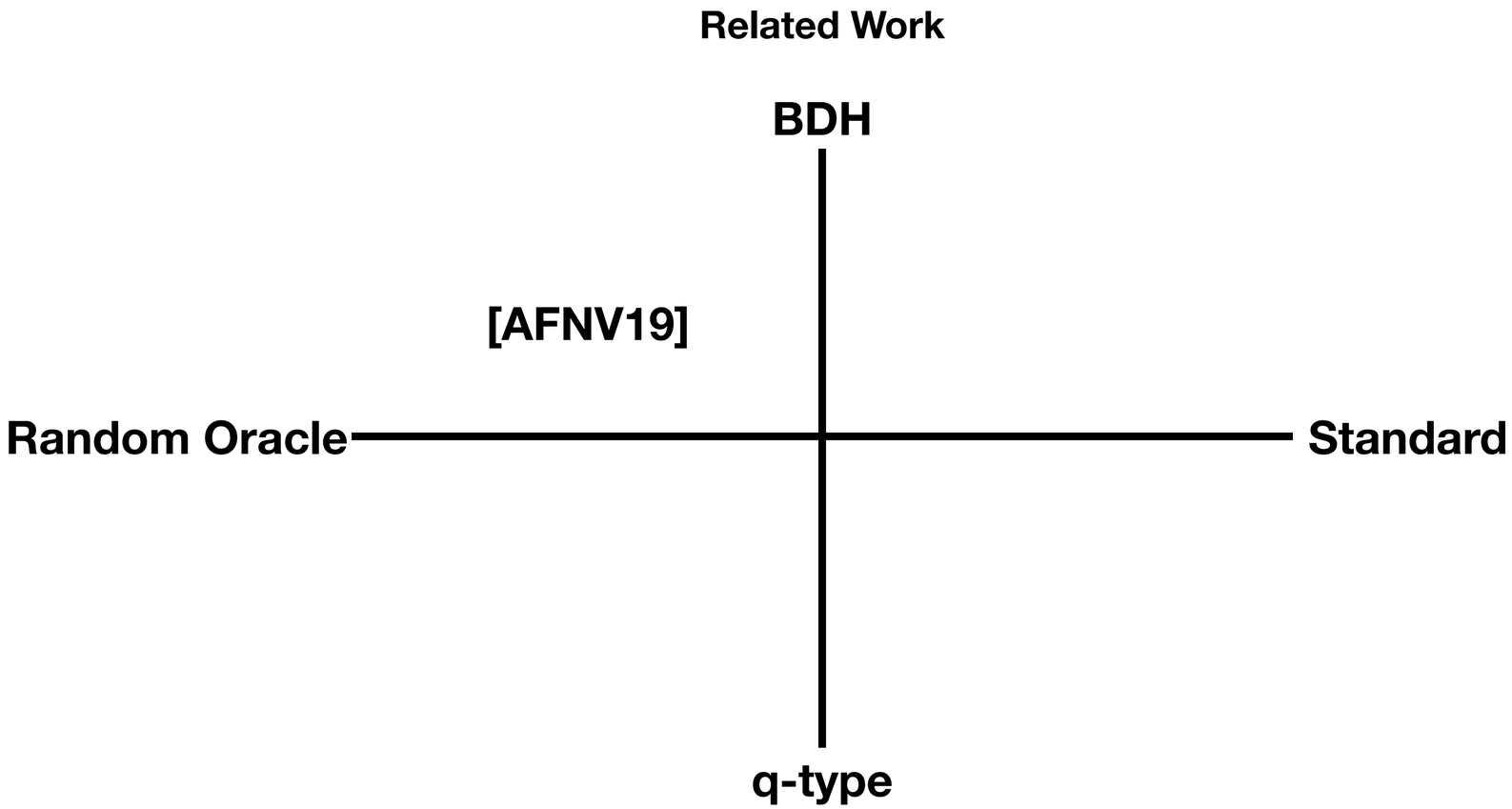
$\mathsf{Enc}(mpk, ek_\sigma, \mathsf{rcv}, m) \rightarrow ct$

$\mathsf{Dec}(mpk, dk_\rho, \mathsf{snd}, ct) \rightarrow m / \perp$

IB-ME from SXDH

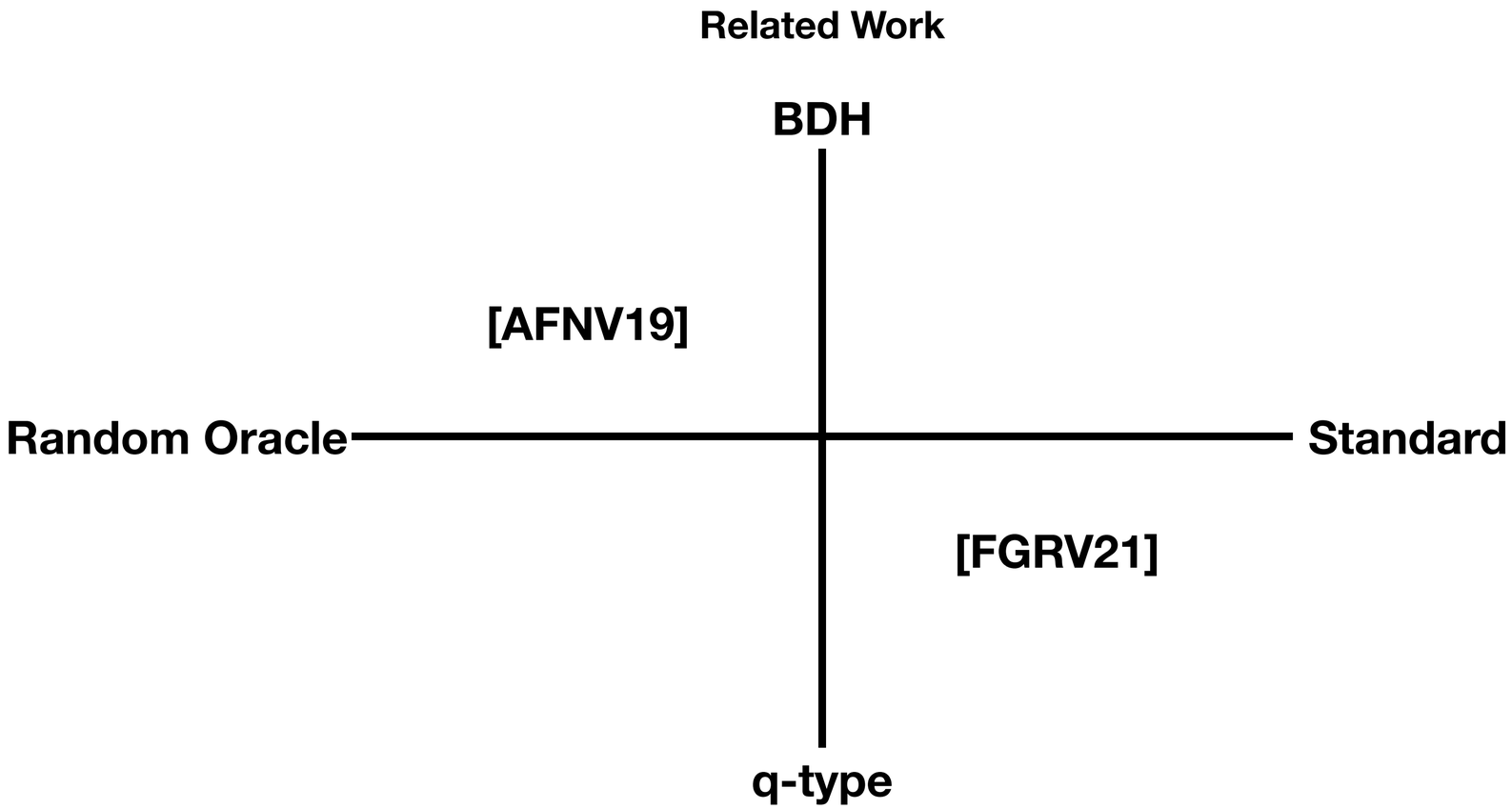


IB-ME from SXDH



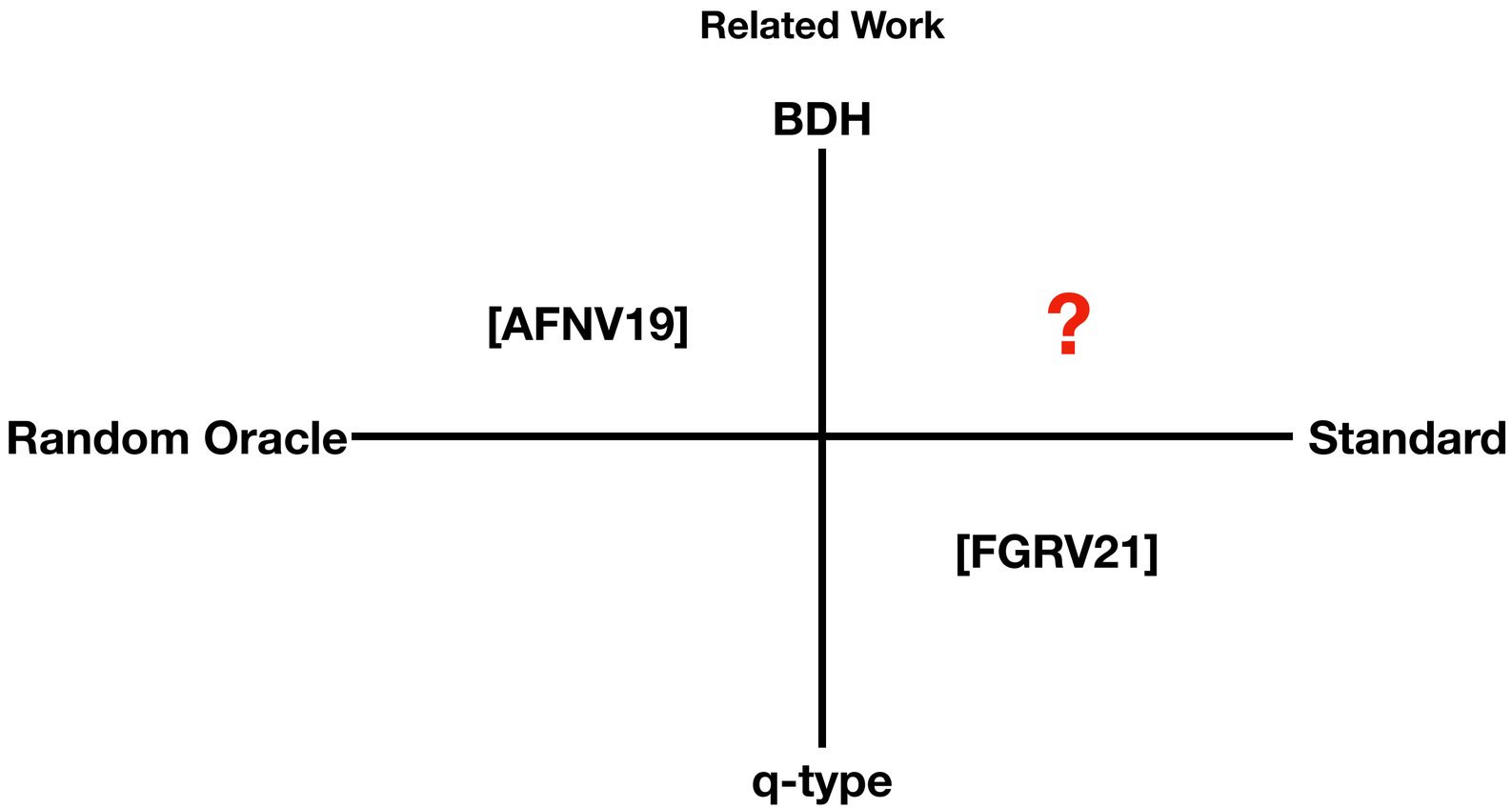
[AFNV19]: Ateniese, G., Francati, D., Nuñez, D., Venturi, D.: Match me if you can: Match- making encryption and its applications. CRYPTO 2019

IB-ME from SXDH



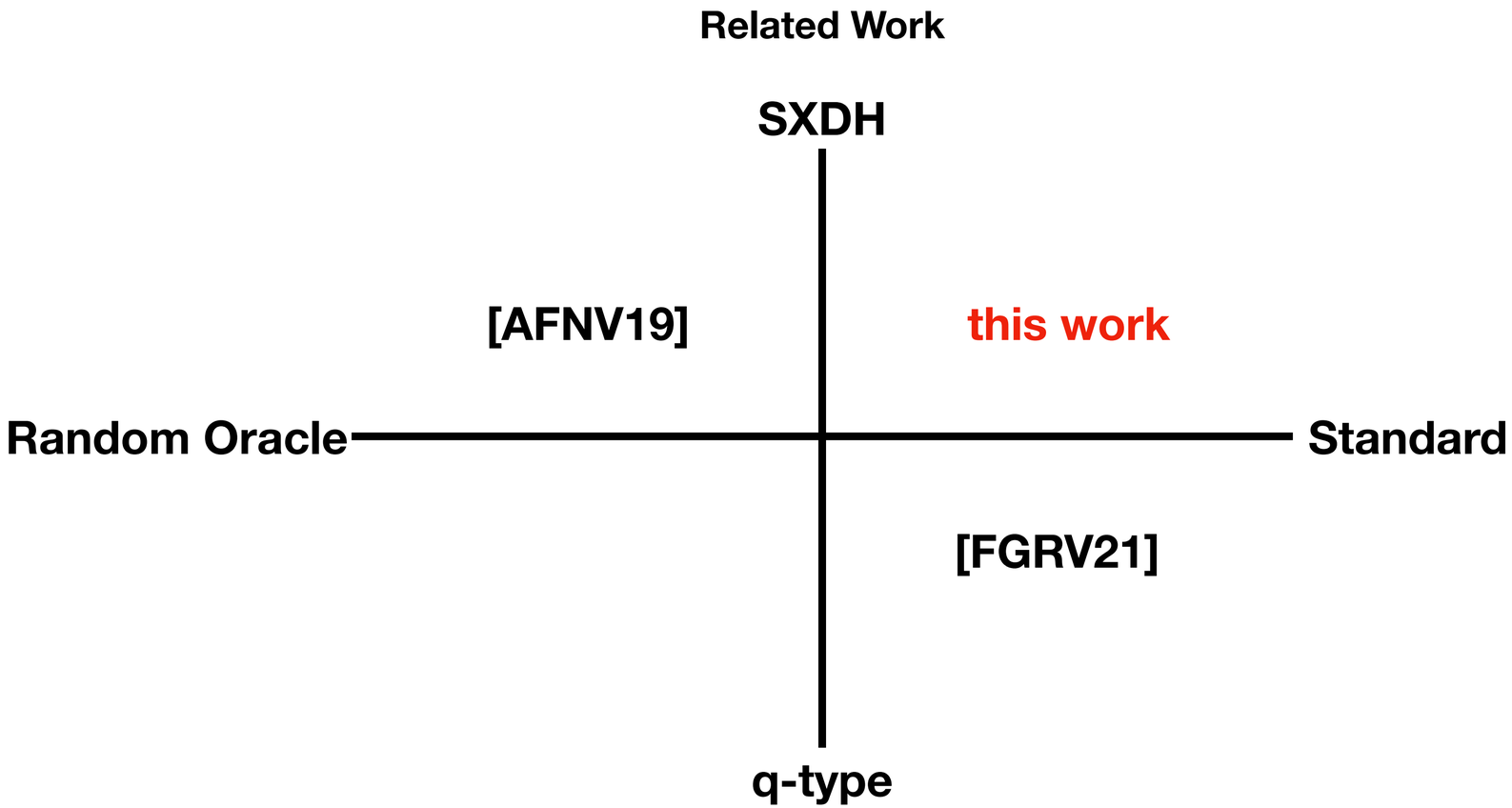
[AFNV19]: Ateniese, G., Francati, D., Nuñez, D., Venturi, D.: Match me if you can: Match- making encryption and its applications. CRYPTO 2019
[FGRV21]: Francati, D., Guidi, A., Russo, L., Venturi, D.: Identity-based matchmaking en- cryption without random oracles. INDOCRYPT 2021

IB-ME from SXDH



[AFNV19]: Ateniese, G., Francati, D., Nuñez, D., Venturi, D.: Match me if you can: Match- making encryption and its applications. CRYPTO 2019
[FGRV21]: Francati, D., Guidi, A., Russo, L., Venturi, D.: Identity-based matchmaking en- cryption without random oracles. INDOCRYPT 2021

IB-ME from SXDH



[AFNV19]: Ateniese, G., Francati, D., Nuñez, D., Venturi, D.: Match me if you can: Match- making encryption and its applications. CRYPTO 2019
[FGRV21]: Francati, D., Guidi, A., Russo, L., Venturi, D.: Identity-based matchmaking en- cryption without random oracles. INDOCRYPT 2021

Security

$\mathbf{G}^{\text{ib-priv}}_{\Pi,\mathsf{A}}(\lambda)$ **Privacy**

$(\mathsf{mpk}, \mathsf{msk}) \leftarrow\!\!\$\ \mathsf{Setup}(1^\lambda)$

$(m_0, m_1, \mathsf{rcv}_0, \mathsf{rcv}_1, \sigma_0, \sigma_1, \alpha) \leftarrow\!\!\$\ \mathsf{A}_1^{\mathsf{O}_1,\mathsf{O}_2}(1^\lambda, \mathsf{mpk})$

$b \leftarrow\!\!\$\ \{0,1\}$

$\mathsf{ek}_{\sigma_b} \leftarrow\!\!\$\ \mathsf{SKGen}(\mathsf{msk}, \sigma_b)$

$c \leftarrow\!\!\$\ \mathsf{Enc}(\mathsf{ek}_{\sigma_b}, \mathsf{rcv}_b, m_b)$

$b' \leftarrow\!\!\$\ \mathsf{A}_2^{\mathsf{O}_1,\mathsf{O}_2}(1^\lambda, c, \alpha)$

If $(b' = b)$ **return** 1

Else **return** 0

$\mathbf{G}^{\text{ib-auth}}_{\Pi,\mathsf{A}}(\lambda)$ **Authenticity**

$(\mathsf{mpk}, \mathsf{msk}) \leftarrow\!\!\$\ \mathsf{Setup}(1^\lambda)$

$(c, \rho, \mathsf{snd}) \leftarrow\!\!\$\ \mathsf{A}^{\mathsf{O}_1,\mathsf{O}_2}(1^\lambda, \mathsf{mpk})$

$\mathsf{dk}_\rho \leftarrow\!\!\$\ \mathsf{RKGen}(\mathsf{msk}, \rho)$

$m = \mathsf{Dec}(\mathsf{dk}_\rho, \mathsf{snd}, c)$

If $\forall \sigma \in \mathcal{Q}_{\mathsf{O}_1} : (\sigma \neq \mathsf{snd}) \wedge (m \neq \perp)$

  return 1

Else **return** 0

Security

Privacy

Privacy: $\mathbf{G}^{\text{ib-priv}}_{\Pi,\mathsf{A}}(\lambda)$

$(\mathsf{mpk}, \mathsf{msk}) \leftarrow_{\mathsf{R}} \mathsf{Setup}(1^\lambda)$

$(m_0, m_1, \mathsf{rcv}_0, \mathsf{rcv}_1, \sigma_0, \sigma_1, st) \leftarrow_{\mathsf{R}} \mathsf{A}_1^{\mathsf{O}_1,\mathsf{O}_2}(1^\lambda, \mathsf{mpk})$

$b \leftarrow_{\mathsf{R}} \{0,1\}$

$ek_{\sigma_b} \leftarrow_{\mathsf{R}} \mathsf{SKGen}(\mathsf{msk}, \sigma_b)$

$ct \leftarrow_{\mathsf{R}} \mathsf{Enc}(ek_{\sigma_b}, \mathsf{rcv}_b, m_b)$

$b' \leftarrow_{\mathsf{R}} \mathsf{A}_2^{\mathsf{O}_1,\mathsf{O}_2}(1^\lambda, ct, st)$

`If` $(b' = b)$ **return** 1

`Else` **return** 0

Security

Privacy

Privacy: $\mathbf{G}^{\text{ib-priv}}_{\Pi,\mathsf{A}}(\lambda)$

$(\mathsf{mpk}, \mathsf{msk}) \leftarrow_{\mathsf{R}} \mathsf{Setup}(1^{\lambda})$

$(m_0, m_1, \mathsf{rcv}_0, \mathsf{rcv}_1, \sigma_0, \sigma_1, st) \leftarrow_{\mathsf{R}} \mathsf{A}_1^{\mathsf{O}_1,\mathsf{O}_2}(1^{\lambda}, \mathsf{mpk})$

$b \leftarrow_{\mathsf{R}} \{0,1\}$

$ek_{\sigma_b} \leftarrow_{\mathsf{R}} \mathsf{SKGen}(\mathsf{msk}, \sigma_b)$

$ct \leftarrow_{\mathsf{R}} \mathsf{Enc}(ek_{\sigma_b}, \mathsf{rcv}_b, m_b)$

$b' \leftarrow_{\mathsf{R}} \mathsf{A}_2^{\mathsf{O}_1,\mathsf{O}_2}(1^{\lambda}, ct, st)$

`If` $(b' = b)$ **return** 1

`Else` **return** 0

Security

Privacy

Privacy: $\mathbf{G}^{\text{ib-priv}}_{\Pi,A}(\lambda)$

$(\mathsf{mpk}, \mathsf{msk}) \leftarrow_R \mathsf{Setup}(1^\lambda)$

$(m_0, m_1, \mathsf{rcv}_0, \mathsf{rcv}_1, \sigma_0, \sigma_1, st) \leftarrow_R \mathsf{A}_1^{\mathsf{O}_1,\mathsf{O}_2}(1^\lambda, \mathsf{mpk})$

$b \leftarrow_R \{0,1\}$

~~$ek_{\sigma_b} \leftarrow_R \mathsf{SKGen}(\mathsf{msk}, \sigma_b)$~~

$ct \leftarrow_R \mathsf{Enc}(\text{~~}ek_{\sigma_b}\text{~~}, \mathsf{rcv}_b, m_b)$

$b' \leftarrow_R \mathsf{A}_2^{\mathsf{O}_1,\mathsf{O}_2}(1^\lambda, ct, st)$

`If` $(b' = b)$ **return** 1

`Else` **return** 0

Anonymous Identity-Based Encryption (AIBE)

Security

Privacy

Privacy: $\mathbf{G}^{\text{ib-priv}}_{\Pi,\mathsf{A}}(\lambda)$

$(\mathsf{mpk}, \mathsf{msk}) \leftarrow_{\mathsf{R}} \mathsf{Setup}(1^\lambda)$

$(m_0, m_1, \mathsf{rcv}_0, \mathsf{rcv}_1, \sigma_0, \sigma_1, st) \leftarrow_{\mathsf{R}} \mathsf{A}_1^{\mathsf{O}_1,\mathsf{O}_2}(1^\lambda, \mathsf{mpk})$

$b \leftarrow_{\mathsf{R}} \{0,1\}$

$ek_{\sigma_b} \leftarrow_{\mathsf{R}} \mathsf{SKGen}(\mathsf{msk}, \sigma_b)$

$ct \leftarrow_{\mathsf{R}} \mathsf{Enc}(ek_{\sigma_b}, \mathsf{rcv}_\mathsf{b}, m_b)$

$b' \leftarrow_{\mathsf{R}} \mathsf{A}_2^{\mathsf{O}_1,\mathsf{O}_2}(1^\lambda, ct, st)$

$\mathtt{If}(b' = b)$ **return** 1

$\mathtt{Else}$ **return** 0

Anonymity: $\mathbf{G}^{\mathsf{AIBE}}_{\Pi,\mathsf{A}}(\lambda)$

$(\mathsf{mpk}, \mathsf{msk}) \leftarrow_{\mathsf{R}} \mathsf{Setup}(1^\lambda)$

$(m_0, m_1, \mathsf{id}_0, \mathsf{id}_1, st) \leftarrow_{\mathsf{R}} \mathsf{A}_1^{\mathsf{O}}(1^\lambda, \mathsf{mpk})$

$b \leftarrow_{\mathsf{R}} \{0,1\}$

$ct \leftarrow_{\mathsf{R}} \mathsf{Enc}(\mathsf{id}_\mathsf{b}, m_b)$

$b' \leftarrow_{\mathsf{R}} \mathsf{A}_2^{\mathsf{O}}(1^\lambda, ct, st)$

$\mathtt{If}(b' = b)$ **return** 1

$\mathtt{Else}$ **return** 0

Security

Privacy

Privacy: $\mathbf{G}^{\text{ib-priv}}_{\Pi,\mathsf{A}}(\lambda)$

$(\mathsf{mpk}, \mathsf{msk}) \leftarrow_{\mathsf{R}} \mathsf{Setup}(1^\lambda)$

$(m_0, m_1, \mathsf{rcv}_0, \mathsf{rcv}_1, \sigma_0, \sigma_1, st) \leftarrow_{\mathsf{R}} \mathsf{A}_1^{\mathsf{O}_1,\mathsf{O}_2}(1^\lambda, \mathsf{mpk})$

$b \leftarrow_{\mathsf{R}} \{0,1\}$

$ek_{\sigma_b} \leftarrow_{\mathsf{R}} \mathsf{SKGen}(\mathsf{msk}, \sigma_b)$

$ct \leftarrow_{\mathsf{R}} \mathsf{Enc}(ek_{\sigma_b}, \mathsf{rcv}_b, m_b)$

$b' \leftarrow_{\mathsf{R}} \mathsf{A}_2^{\mathsf{O}_1,\mathsf{O}_2}(1^\lambda, ct, st)$

$\mathtt{If}(b' = b)$ **return** 1

$\mathtt{Else}$ **return** 0

Anonymity: $\mathbf{G}^{\mathsf{AIBE}}_{\Pi,\mathsf{A}}(\lambda)$

$(\mathsf{mpk}, \mathsf{msk}) \leftarrow_{\mathsf{R}} \mathsf{Setup}(1^\lambda)$

$(m_0, m_1, \mathsf{id}_0, \mathsf{id}_1, st) \leftarrow_{\mathsf{R}} \mathsf{A}_1^{\mathsf{O}}(1^\lambda, \mathsf{mpk})$

$b \leftarrow_{\mathsf{R}} \{0,1\}$

$ct \leftarrow_{\mathsf{R}} \mathsf{Enc}(\mathsf{id}_b, m_b)$

$b' \leftarrow_{\mathsf{R}} \mathsf{A}_2^{\mathsf{O}}(1^\lambda, ct, st)$

$\mathtt{If}(b' = b)$ **return** 1

$\mathtt{Else}$ **return** 0

Security

Privacy

Privacy: $\mathbf{G}^{\text{ib-priv}}_{\Pi,\mathsf{A}}(\lambda)$

$(\mathsf{mpk}, \mathsf{msk}) \leftarrow_{\mathsf{R}} \mathsf{Setup}(1^\lambda)$

$(m_0, m_1, \mathsf{rcv}_0, \mathsf{rcv}_1, \sigma_0, \sigma_1, st) \leftarrow_{\mathsf{R}} \mathsf{A}_1^{\mathsf{O}_1,\mathsf{O}_2}(1^\lambda, \mathsf{mpk})$

$b \leftarrow_{\mathsf{R}} \{0,1\}$

$ek_{\sigma_b} \leftarrow_{\mathsf{R}} \mathsf{SKGen}(\mathsf{msk}, \sigma_b)$

$ct \leftarrow_{\mathsf{R}} \mathsf{Enc}(ek_{\sigma_b}, \mathsf{rcv}_b, m_b)$

$b' \leftarrow_{\mathsf{R}} \mathsf{A}_2^{\mathsf{O}_1,\mathsf{O}_2}(1^\lambda, ct, st)$

$\mathtt{If}(b' = b)$ **return** 1

$\mathtt{Else}$ **return** 0

Anonymity: $\mathbf{G}^{\mathsf{AIBE}}_{\Pi,\mathsf{A}}(\lambda)$

$(\mathsf{mpk}, \mathsf{msk}) \leftarrow_{\mathsf{R}} \mathsf{Setup}(1^\lambda)$

$(m_0, m_1, \mathsf{id}_0, \mathsf{id}_1, st) \leftarrow_{\mathsf{R}} \mathsf{A}_1^{\mathsf{O}}(1^\lambda, \mathsf{mpk})$

$b \leftarrow_{\mathsf{R}} \{0,1\}$

$ct \leftarrow_{\mathsf{R}} \mathsf{Enc}(\mathsf{id}_b, m_b)$

$b' \leftarrow_{\mathsf{R}} \mathsf{A}_2^{\mathsf{O}}(1^\lambda, ct, st)$

$\mathtt{If}(b' = b)$ **return** 1

$\mathtt{Else}$ **return** 0

Security

Authenticity

Authenticity: $\mathbf{G}^{\text{ib-auth}}_{\Pi,\mathsf{A}}(\lambda)$

$(\mathsf{mpk}, \mathsf{msk}) \leftarrow_{\mathsf{R}} \mathsf{Setup}(1^{\lambda})$

$(ct, \rho, \mathsf{snd}) \leftarrow_{\mathsf{R}} \mathsf{A}^{\mathsf{O}_1,\mathsf{O}_2}(1^{\lambda}, \mathsf{mpk})$

$dk_{\rho} \leftarrow_{\mathsf{R}} \mathsf{RKGen}(\mathsf{msk}, \rho)$

$m = \mathsf{Dec}(dk_{\rho}, \mathsf{snd}, ct)$

If $\forall \sigma \in \mathcal{Q}_{\mathsf{O}_1} : (\sigma \neq \mathsf{snd}) \wedge (m \neq \perp)$

    return 1

Else **return** 0

Security

Authenticity

Authenticity: $\mathbf{G}^{\text{ib-auth}}_{\Pi,A}(\lambda)$

$(\text{mpk}, \text{msk}) \leftarrow_R \text{Setup}(1^\lambda)$

$(ct, \rho, \text{snd}) \leftarrow_R A^{O_1, O_2}(1^\lambda, \text{mpk})$

$dk_\rho \leftarrow_R \text{RKGen}(\text{msk}, \rho)$

$m = \text{Dec}(dk_\rho, \text{snd}, ct)$

If $\forall \sigma \in \mathcal{Q}_{O_1} : (\sigma \neq \text{snd}) \wedge (m \neq \perp)$

    return 1

Else **return** 0

Unforgeability: $\mathbf{G}^{\text{Signature}}_{\Pi,A}(\lambda)$

$(\text{mpk}, \text{msk}) \leftarrow_R \text{Setup}(1^\lambda)$

$(m, \sigma) \leftarrow_R A^{\text{Sign}(\text{msk}, \cdot)}(1^\lambda, \text{mpk})$

$v = \text{Verify}(\text{mpk}, m, \sigma)$

If $\forall m \notin \mathcal{Q}_{\text{Sign}} \wedge (v = 1)$

    return 1

Else **return** 0

Security

Authenticity

Authenticity: $\mathbf{G}^{\text{ib-auth}}_{\Pi,A}(\lambda)$

$(\text{mpk}, \text{msk}) \leftarrow_R \text{Setup}(1^\lambda)$

$(ct, \rho, \text{snd}) \leftarrow_R A^{O_1, O_2}(1^\lambda, \text{mpk})$

$dk_\rho \leftarrow_R \text{RKGen}(\text{msk}, \rho)$

$m = \text{Dec}(dk_\rho, \text{snd}, ct)$

If $\forall \sigma \in \mathcal{Q}_{O_1} : (\sigma \neq \text{snd}) \wedge (m \neq \perp)$

    return 1

Else **return** 0

Unforgeability: $\mathbf{G}^{\text{Signature}}_{\Pi,A}(\lambda)$

$(\text{mpk}, \text{msk}) \leftarrow_R \text{Setup}(1^\lambda)$

$(m, \sigma) \leftarrow_R A^{\text{Sign}(\text{msk}, \cdot)}(1^\lambda, \text{mpk})$

$v = \text{Verify}(\text{mpk}, m, \sigma)$

If $\forall m \notin \mathcal{Q}_{\text{Sign}} \wedge (v = 1)$

    return 1

Else **return** 0

Security

Authenticity

Authenticity: $\mathbf{G}^{\text{ib-auth}}_{\Pi,A}(\lambda)$

$(\mathsf{mpk}, \mathsf{msk}) \leftarrow_R \mathsf{Setup}(1^\lambda)$

$(ct, \rho, \mathsf{snd}) \leftarrow_R A^{O_1, O_2}(1^\lambda, \mathsf{mpk})$

$dk_\rho \leftarrow_R \mathsf{RKGen}(\mathsf{msk}, \rho)$

$m = \mathsf{Dec}(dk_\rho, \mathsf{snd}, ct)$

If $\forall \sigma \in \mathcal{Q}_{O_1} : (\sigma \neq \mathsf{snd}) \wedge (m \neq \perp)$

return 1

Else **return** 0

Unforgeability: $\mathbf{G}^{\text{Signature}}_{\Pi,A}(\lambda)$

$(\mathsf{mpk}, \mathsf{msk}) \leftarrow_R \mathsf{Setup}(1^\lambda)$

$(m, \sigma) \leftarrow_R A^{\mathsf{Sign}(\mathsf{msk}, \cdot)}(1^\lambda, \mathsf{mpk})$

$v = \mathsf{Verify}(\mathsf{mpk}, m, \sigma)$

If $\forall m \notin \mathcal{Q}_{\mathsf{Sign}} \wedge (v = 1)$

return 1

Else **return** 0

Security

Authenticity

Authenticity: $\mathbf{G}^{\text{ib-auth}}_{\Pi,\mathsf{A}}(\lambda)$

$(\mathsf{mpk}, \mathsf{msk}) \leftarrow_{\mathsf{R}} \mathsf{Setup}(1^\lambda)$

$(ct, \rho, \mathsf{snd}) \leftarrow_{\mathsf{R}} \mathsf{A}^{\mathsf{O}_1,\mathsf{O}_2}(1^\lambda, \mathsf{mpk})$

$dk_\rho \leftarrow_{\mathsf{R}} \mathsf{RKGen}(\mathsf{msk}, \rho)$

$m = \mathsf{Dec}(dk_\rho, \mathsf{snd}, ct)$

If $\forall \sigma \in \mathcal{Q}_{\mathsf{O}_1} : (\sigma \neq \mathsf{snd}) \wedge (m \neq \perp)$

return 1

Else **return** 0

Unforgeability: $\mathbf{G}^{\text{Signature}}_{\Pi,\mathsf{A}}(\lambda)$

$(\mathsf{mpk}, \mathsf{msk}) \leftarrow_{\mathsf{R}} \mathsf{Setup}(1^\lambda)$

$(m, \sigma) \leftarrow_{\mathsf{R}} \mathsf{A}^{\mathsf{Sign}(\mathsf{msk},\cdot)}(1^\lambda, \mathsf{mpk})$

$v = \mathsf{Verify}(\mathsf{mpk}, m, \sigma)$

If $\forall m \notin \mathcal{Q}_{\mathsf{Sign}} \wedge (v = 1)$

return 1

Else **return** 0

Security

$\mathbf{G}^{\text{ib-priv}}_{\Pi,\mathsf{A}}(\lambda)$ **Privacy**

$(\mathsf{mpk}, \mathsf{msk}) \leftarrow\!\!\$\ \mathsf{Setup}(1^\lambda)$
$(m_0, m_1, \mathsf{rcv}_0, \mathsf{rcv}_1, \sigma_0, \sigma_1, \alpha) \leftarrow\!\!\$\ \mathsf{A}_1^{\mathsf{O}_1,\mathsf{O}_2}(1^\lambda, \mathsf{mpk})$
$b \leftarrow\!\!\$\ \{0,1\}$
$\mathsf{ek}_{\sigma_b} \leftarrow\!\!\$\ \mathsf{SKGen}(\mathsf{msk}, \sigma_b)$
$c \leftarrow\!\!\$\ \mathsf{Enc}(\mathsf{ek}_{\sigma_b}, \mathsf{rcv}_b, m_b)$
$b' \leftarrow\!\!\$\ \mathsf{A}_2^{\mathsf{O}_1,\mathsf{O}_2}(1^\lambda, c, \alpha)$
If $(b' = b)$ **return** 1
Else **return** 0

$\mathbf{G}^{\text{ib-auth}}_{\Pi,\mathsf{A}}(\lambda)$ **Authenticity**

$(\mathsf{mpk}, \mathsf{msk}) \leftarrow\!\!\$\ \mathsf{Setup}(1^\lambda)$
$(c, \rho, \mathsf{snd}) \leftarrow\!\!\$\ \mathsf{A}^{\mathsf{O}_1,\mathsf{O}_2}(1^\lambda, \mathsf{mpk})$
$\mathsf{dk}_\rho \leftarrow\!\!\$\ \mathsf{RKGen}(\mathsf{msk}, \rho)$
$m = \mathsf{Dec}(\mathsf{dk}_\rho, \mathsf{snd}, c)$
If $\forall \sigma \in \mathcal{Q}_{\mathsf{O}_1} : (\sigma \neq \mathsf{snd}) \wedge (m \neq \perp)$
  return 1
Else **return** 0

Security

$\mathbf{G}^{\text{ib-priv}}_{\Pi,\mathsf{A}}(\lambda)$ **Privacy**

$(\mathsf{mpk}, \mathsf{msk}) \leftarrow\!\!\$\ \mathsf{Setup}(1^\lambda)$
$(m_0, m_1, \mathsf{rcv}_0, \mathsf{rcv}_1, \sigma_0, \sigma_1, \alpha) \leftarrow\!\!\$\ \mathsf{A}_1^{\mathsf{O}_1,\mathsf{O}_2}(1^\lambda, \mathsf{mpk})$
$b \leftarrow\!\!\$\ \{0,1\}$
$\mathsf{ek}_{\sigma_b} \leftarrow\!\!\$\ \mathsf{SKGen}(\mathsf{msk}, \sigma_b)$
$c \leftarrow\!\!\$\ \mathsf{Enc}(\mathsf{ek}_{\sigma_b}, \mathsf{rcv}_b, m_b)$
$b' \leftarrow\!\!\$\ \mathsf{A}_2^{\mathsf{O}_1,\mathsf{O}_2}(1^\lambda, c, \alpha)$
If $(b' = b)$ **return** 1
Else **return** 0

$\mathbf{G}^{\text{ib-auth}}_{\Pi,\mathsf{A}}(\lambda)$ **Authenticity**

$(\mathsf{mpk}, \mathsf{msk}) \leftarrow\!\!\$\ \mathsf{Setup}(1^\lambda)$
$(c, \rho, \mathsf{snd}) \leftarrow\!\!\$\ \mathsf{A}^{\mathsf{O}_1,\mathsf{O}_2}(1^\lambda, \mathsf{mpk})$
$\mathsf{dk}_\rho \leftarrow\!\!\$\ \mathsf{RKGen}(\mathsf{msk}, \rho)$
$m = \mathsf{Dec}(\mathsf{dk}_\rho, \mathsf{snd}, c)$
If $\forall \sigma \in \mathcal{Q}_{\mathsf{O}_1} : (\sigma \neq \mathsf{snd}) \wedge (m \neq \perp)$
  return 1
Else **return** 0

Anonymous IBE

Signature

Security

$\mathbf{G}^{\text{ib-priv}}_{\Pi,\mathsf{A}}(\lambda)$ **Privacy**

$(\mathsf{mpk}, \mathsf{msk}) \leftarrow\!\!\$\ \mathsf{Setup}(1^\lambda)$
$(m_0, m_1, \mathsf{rcv}_0, \mathsf{rcv}_1, \sigma_0, \sigma_1, \alpha) \leftarrow\!\!\$\ \mathsf{A}_1^{\mathsf{O}_1,\mathsf{O}_2}(1^\lambda, \mathsf{mpk})$
$b \leftarrow\!\!\$\ \{0,1\}$
$\mathsf{ek}_{\sigma_b} \leftarrow\!\!\$\ \mathsf{SKGen}(\mathsf{msk}, \sigma_b)$
$c \leftarrow\!\!\$\ \mathsf{Enc}(\mathsf{ek}_{\sigma_b}, \mathsf{rcv}_b, m_b)$
$b' \leftarrow\!\!\$\ \mathsf{A}_2^{\mathsf{O}_1,\mathsf{O}_2}(1^\lambda, c, \alpha)$
If $(b' = b)$ **return** 1
Else **return** 0

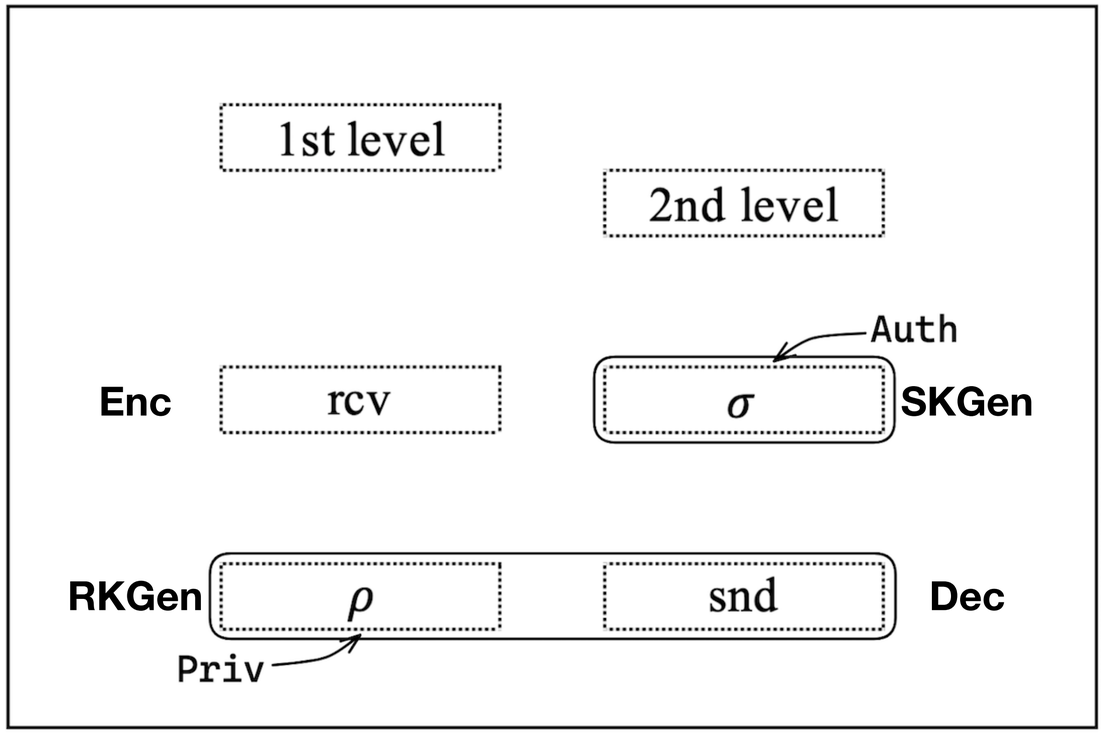
$\mathbf{G}^{\text{ib-auth}}_{\Pi,\mathsf{A}}(\lambda)$ **Authenticity**

$(\mathsf{mpk}, \mathsf{msk}) \leftarrow\!\!\$\ \mathsf{Setup}(1^\lambda)$
$(c, \rho, \mathsf{snd}) \leftarrow\!\!\$\ \mathsf{A}^{\mathsf{O}_1,\mathsf{O}_2}(1^\lambda, \mathsf{mpk})$
$\mathsf{dk}_\rho \leftarrow\!\!\$\ \mathsf{RKGen}(\mathsf{msk}, \rho)$
$m = \mathsf{Dec}(\mathsf{dk}_\rho, \mathsf{snd}, c)$
If $\forall \sigma \in \mathcal{Q}_{\mathsf{O}_1} : (\sigma \neq \mathsf{snd}) \wedge (m \neq \perp)$
  return 1
Else **return** 0

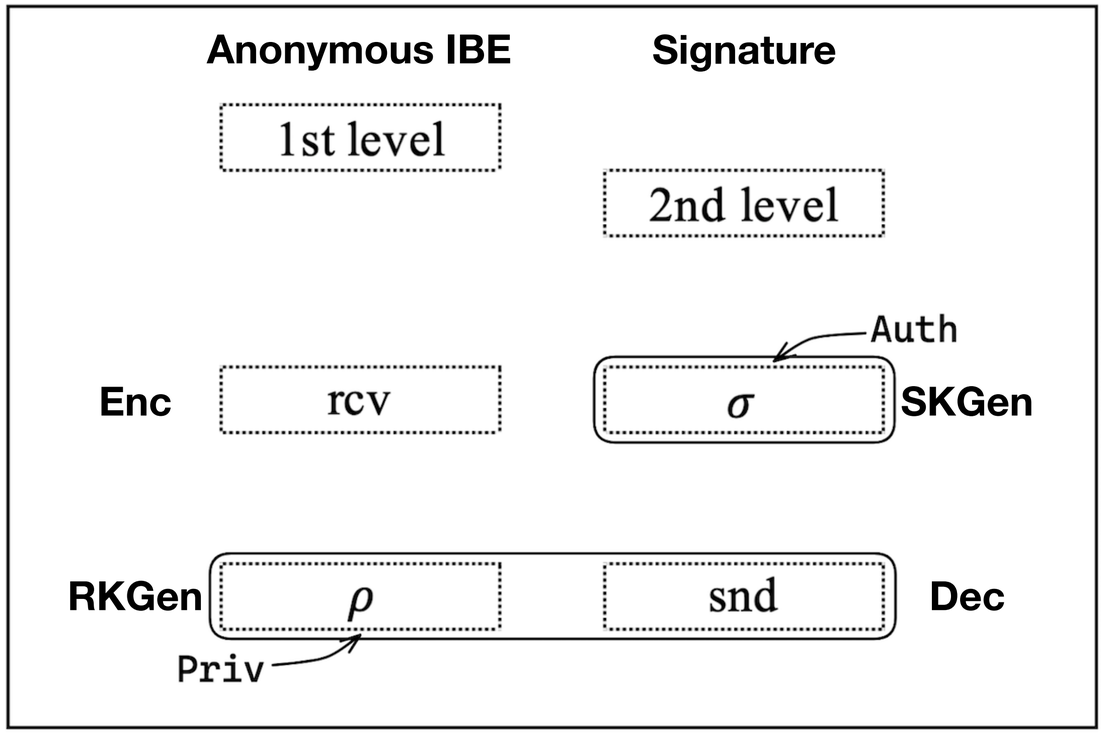
Anonymous IBE —[BF01]→ **Signature**

[BF01]: Boneh, D., Franklin, M.K.: Identity-based encryption from the weil pairing. CRYPTO 2001.

Idea

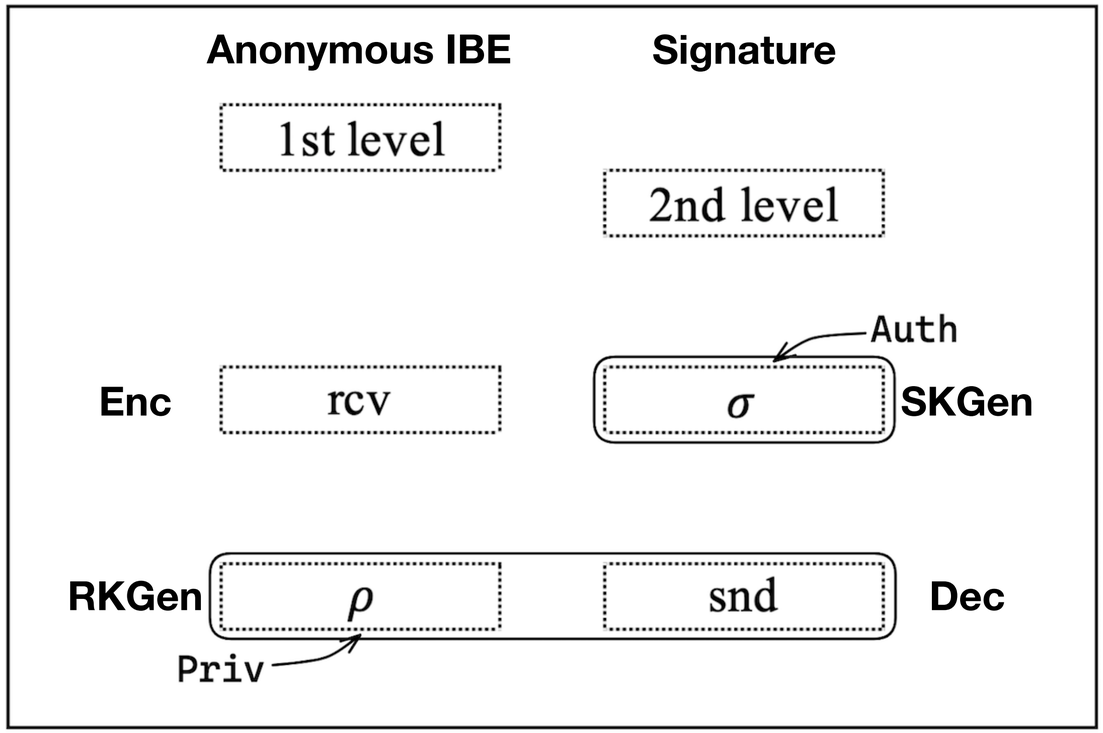


Idea


Anonymous IBE
Signature
1st level
2nd level
Auth
Enc
rcv
σ
SKGen
RKGen
ρ
snd
Dec
Priv

Idea

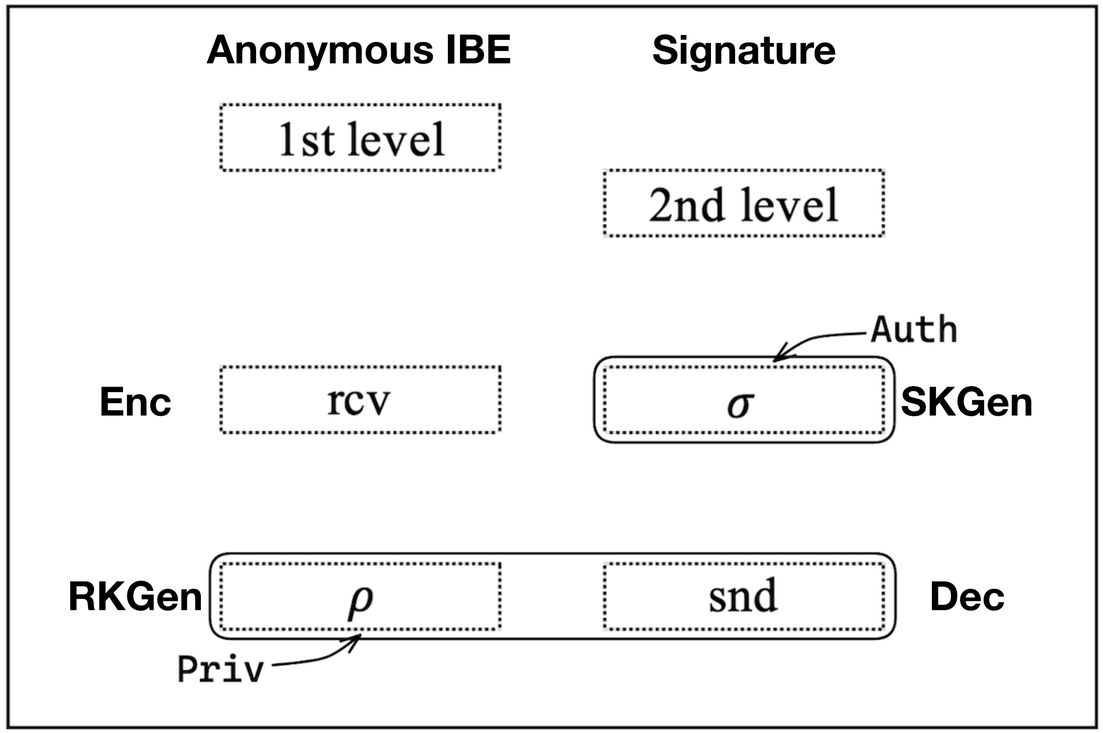
[CLLWW14]



[CLLWW14]: Chen, J., Lim, H.W., Ling, S., Wang, H., Wee, H.: Shorter identity-based encryption via asymmetric pairings. Des. Codes Cryptogr. 2014

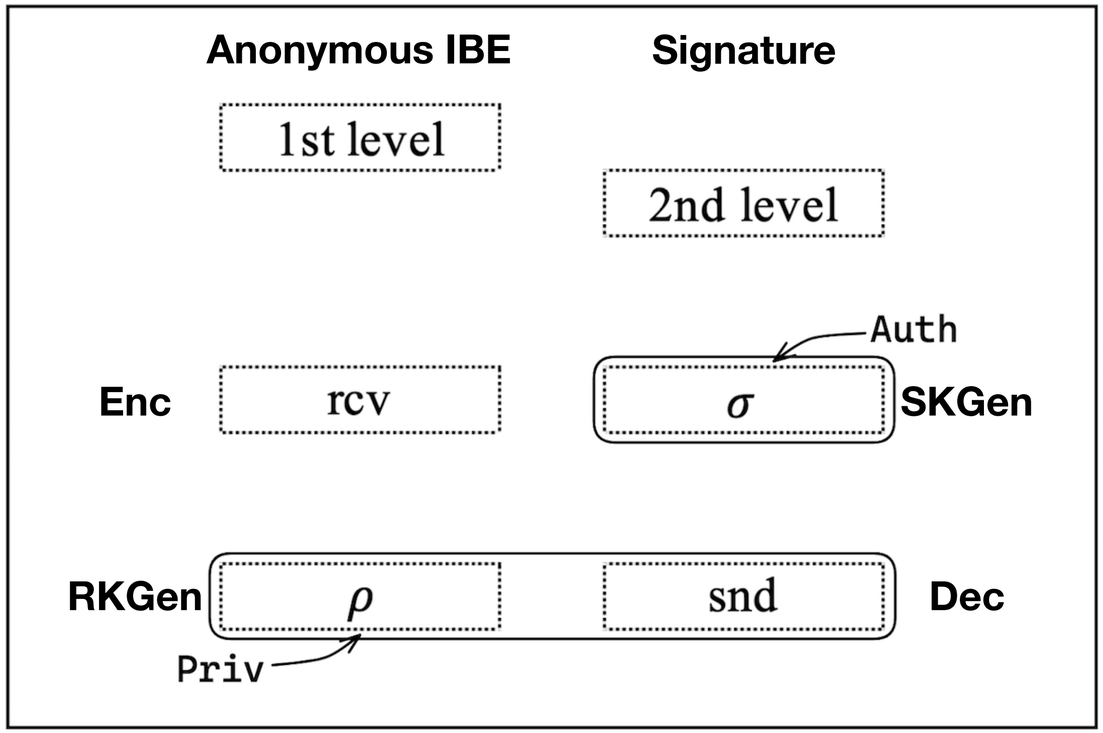
Idea

[CLLWW14]
[Waters09]
[OT09]



[CLLWW14]: Chen, J., Lim, H.W., Ling, S., Wang, H., Wee, H.: Shorter identity-based encryption via asymmetric pairings. Des. Codes Cryptogr. 2014
[Waters09]: Waters, B.: Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. CRYPTO 2009
[OT09]: Okamoto, T., Takashima, K.: Hierarchical predicate encryption for inner-products. ASIACRYPT 2009

Construction



[CLLWW14]: AIBE

$AIBE\_mpk,\ AIBE\_msk$

$SK_{\mathsf{id}} = g_2^{\alpha \mathbf{d_1^*} + s(\mathsf{id}\mathbf{d_1^*} - \mathbf{d_2^*})}$

$CT = \{\mathsf{C} = m \cdot (g_T^{\alpha})^s, \mathsf{C}_0 = g_1^{s(\mathbf{d_1} + \mathsf{id}\mathbf{d_2})}\}$

[CLLWW14]: Signature

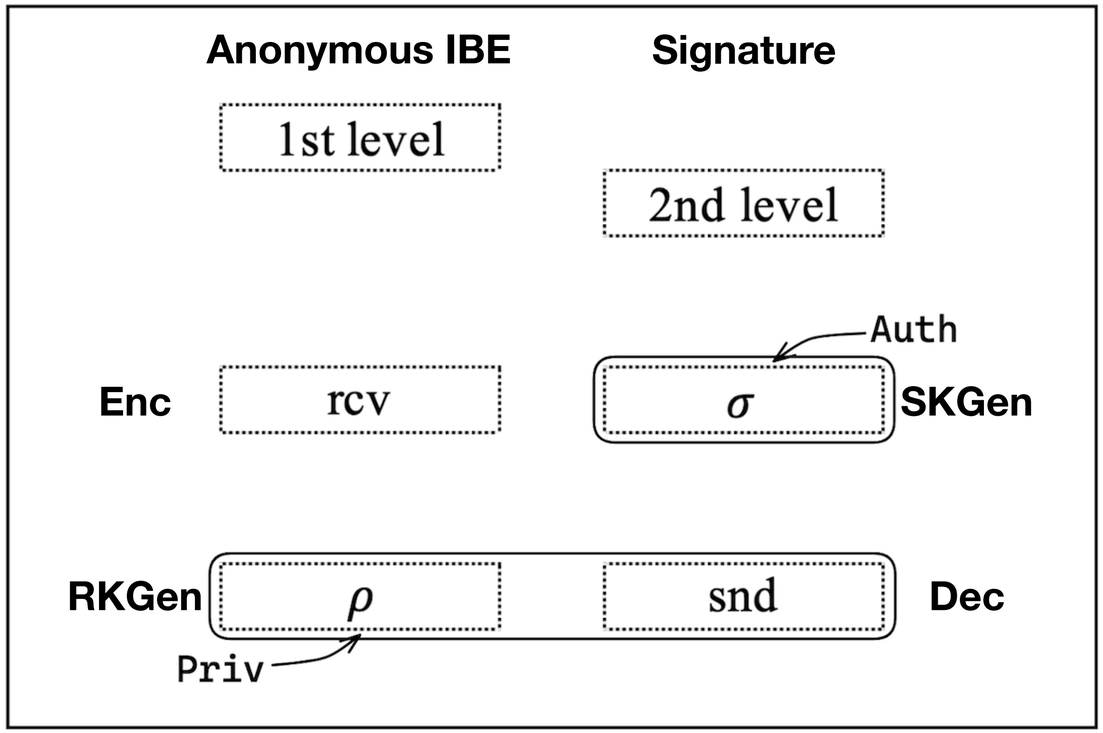
$Sig\_mpk,\ Sig\_msk$

$Sign : \sigma = g_2^{\alpha \mathbf{d_1^*} + s(m\mathbf{d_1^*} - \mathbf{d_2^*})}$

$Verify : e(g_1^{\mathbf{d_1} + m\mathbf{d_2}}, \sigma) = g_T^{\alpha}$

[CLLWW14]: Chen, J., Lim, H.W., Ling, S., Wang, H., Wee, H.: Shorter identity-based encryption via asymmetric pairings. Des. Codes Cryptogr. 2014

Construction



Anonymous IBE

$$SK_{\mathsf{id}} = g_2^{\alpha \mathbf{d}_1^* + s(\mathsf{id}\mathbf{d}_1^* - \mathbf{d}_2^*)}$$

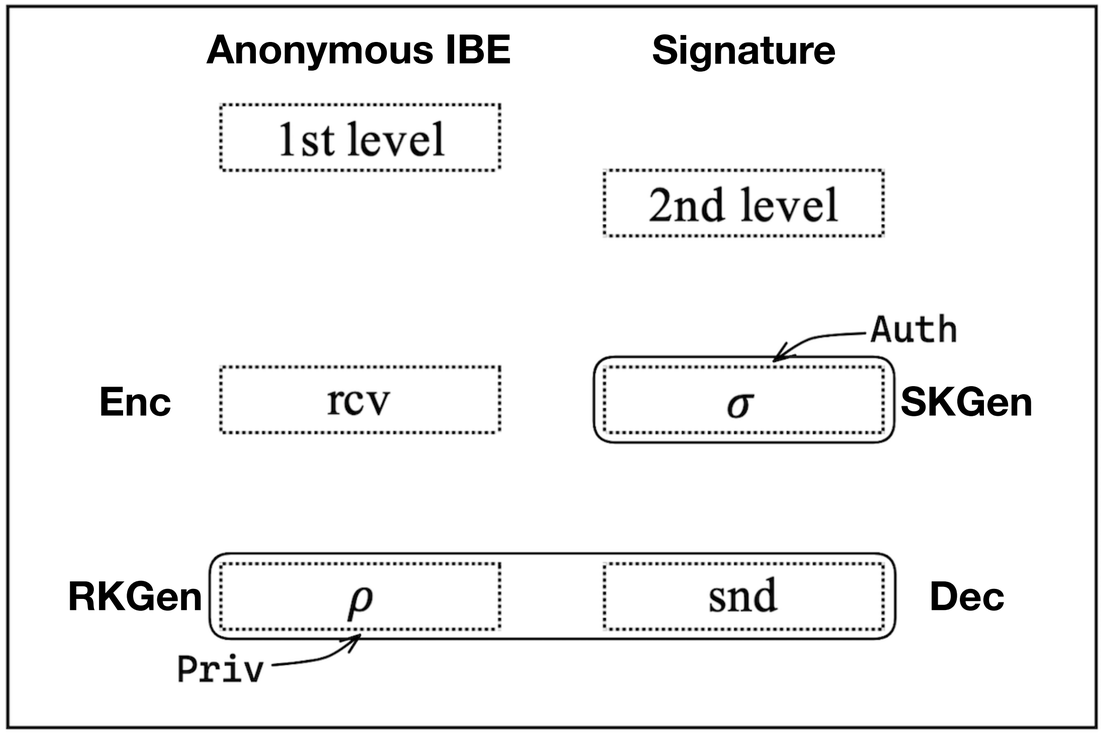
$$CT = \{\mathsf{C} = m \cdot (g_T^{\alpha})^s, \mathsf{C}_0 = g_1^{s(\mathbf{d}_1 + \mathsf{id}\mathbf{d}_2)}\}$$

Signature

$$Sign : \sigma = g_2^{\alpha \mathbf{d}_1^* + s(m\mathbf{d}_1^* - \mathbf{d}_2^*)}$$

$$Verify : e(g_1^{\mathbf{d}_1 + m\mathbf{d}_2}, \sigma) = g_T^{\alpha}$$

Construction



Anonymous IBE

$$SK_{\mathsf{id}} = g_2^{\alpha \mathbf{d}_1^* + s(\mathsf{id}\mathbf{d}_1^* - \mathbf{d}_2^*)}$$

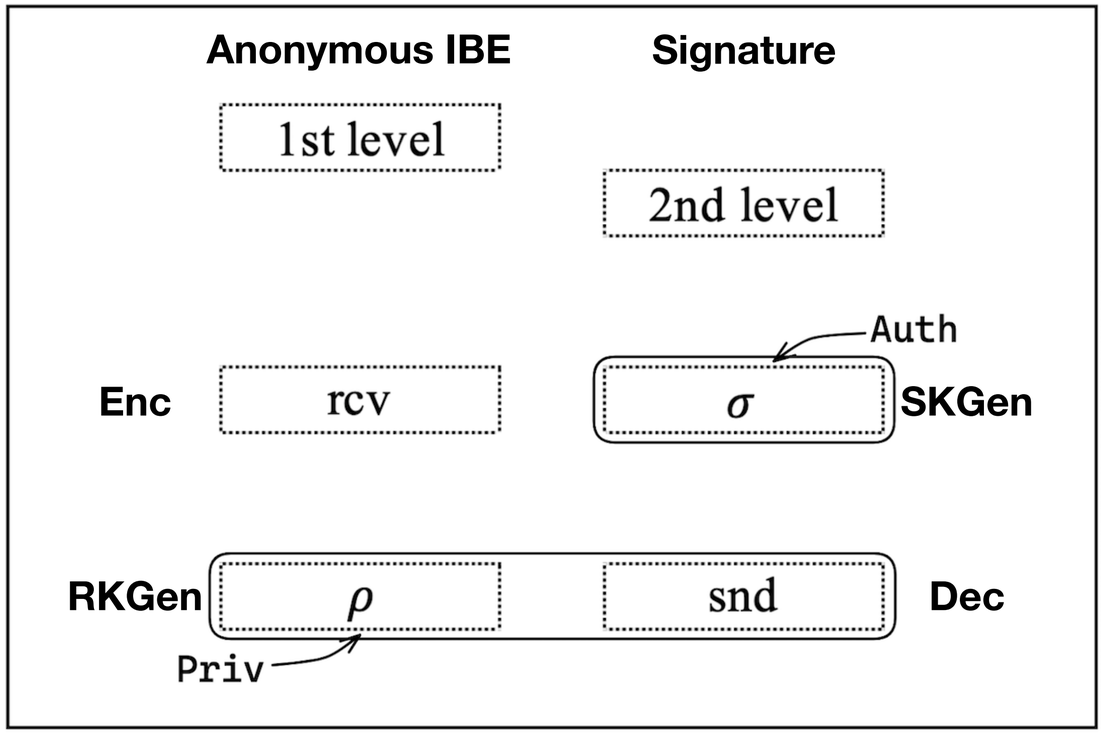
$$CT = \{\mathsf{C} = m \cdot (g_T^{\alpha})^s, \mathsf{C}_0 = g_1^{s(\mathbf{d}_1 + \mathsf{id}\mathbf{d}_2)}\}$$

Signature

$$Sign : \sigma = g_2^{\alpha \mathbf{d}_1^* + s(m\mathbf{d}_1^* - \mathbf{d}_2^*)}$$

$$Verify : e(g_1^{\mathbf{d}_1 - m\mathbf{d}_2}, \sigma) = g_T^{\alpha}$$

Construction



Anonymous IBE

$$SK_{\mathsf{id}} = g_2^{\alpha \mathbf{d}_1^* + s(\mathsf{id}\mathbf{d}_1^* - \mathbf{d}_2^*)}$$

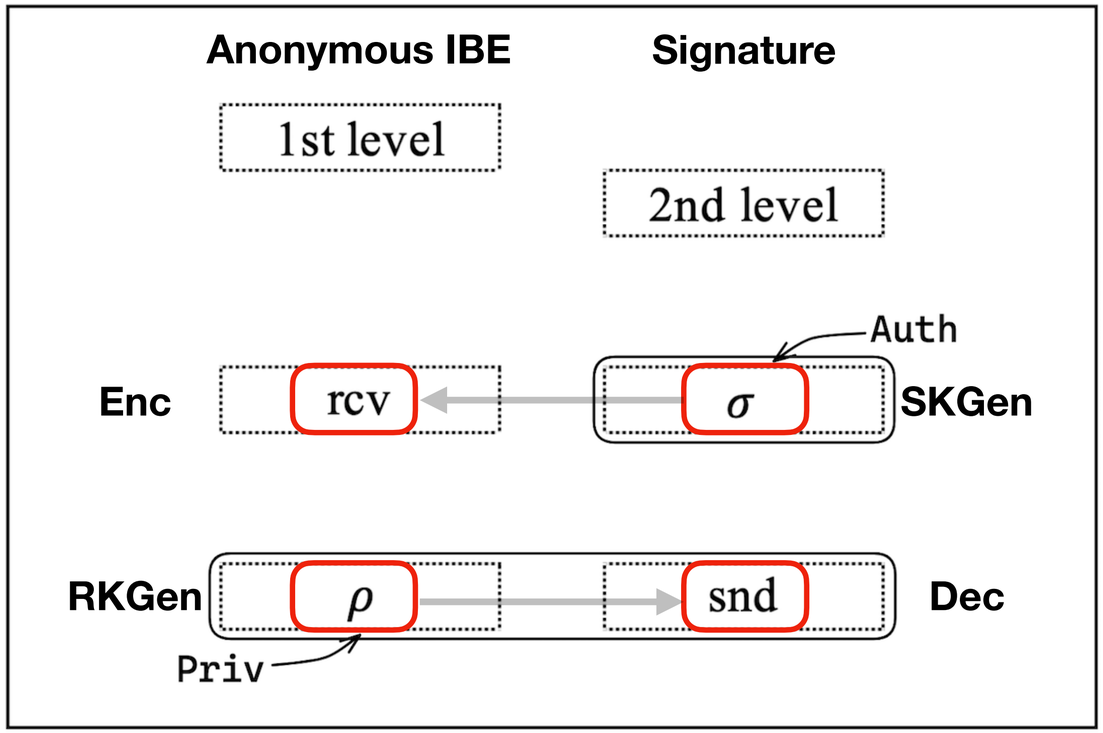
$$CT = \{\mathsf{C} = m \cdot (g_T^{\alpha})^s, \mathsf{C}_0 = g_1^{s(\mathbf{d}_1 + \mathsf{id}\mathbf{d}_2)}\}$$

Signature

$$Sign : \sigma = g_2^{\eta \mathbf{d}_3^* + r(\mathsf{id}\mathbf{d}_3^* - \mathbf{d}_4^*)}$$

$$Verify : e(g_1^{\mathbf{d}_3 + \mathsf{id}\mathbf{d}_4}, \sigma) = g_T^{\eta}$$

Construction



Anonymous IBE

$$SK_{\mathsf{id}} = g_2^{\alpha \mathbf{d}_1^* + s(\mathsf{id}\mathbf{d}_1^* - \mathbf{d}_2^*)}$$

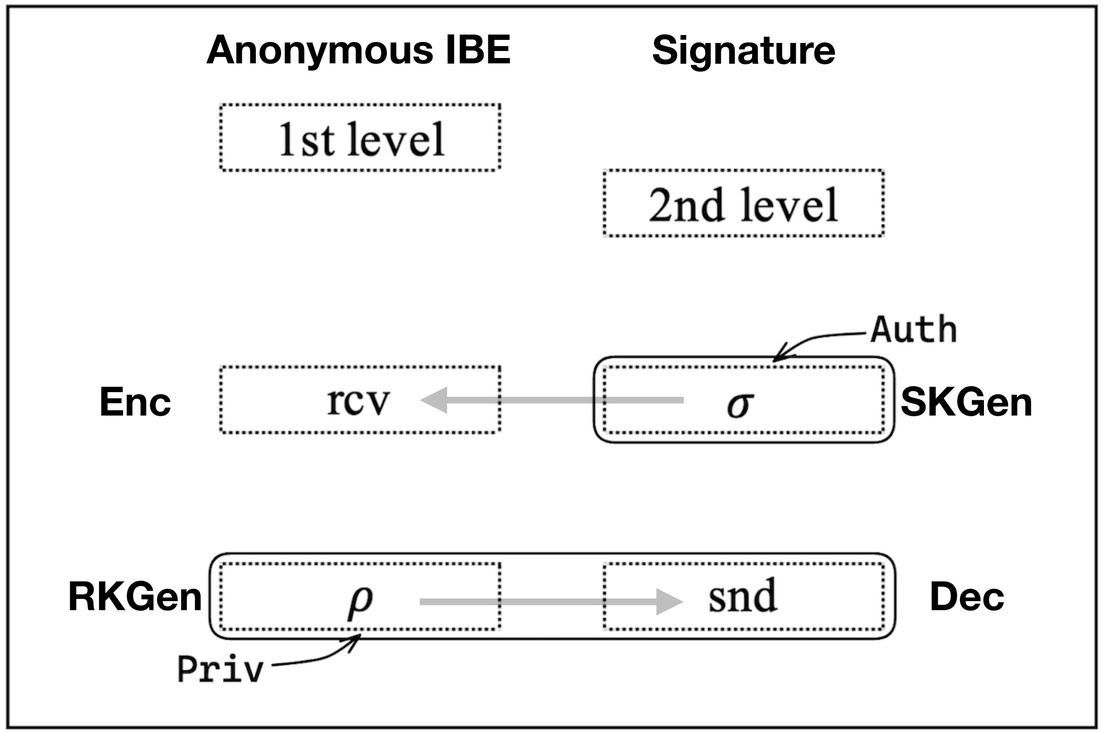
$$CT = \{\mathsf{C} = m \cdot (g_T^{\alpha})^s, \mathsf{C}_0 = g_1^{s(\mathbf{d}_1 - \mathsf{id}\mathbf{d}_2)}\}$$

Signature

$$Sign : \sigma = g_2^{\eta \mathbf{d}_3^* + r(\mathsf{id}\mathbf{d}_3^* - \mathbf{d}_4^*)}$$

$$Verify : e(g_1^{\mathbf{d}_3 - \mathsf{id}\mathbf{d}_4}, \sigma) = g_T^{\eta}$$

Construction



Anonymous IBE

$$SK_{\mathsf{id}} = g_2^{\alpha \mathbf{d}_1^* + s(\rho \mathbf{d}_1^* - \mathbf{d}_2^*)}$$

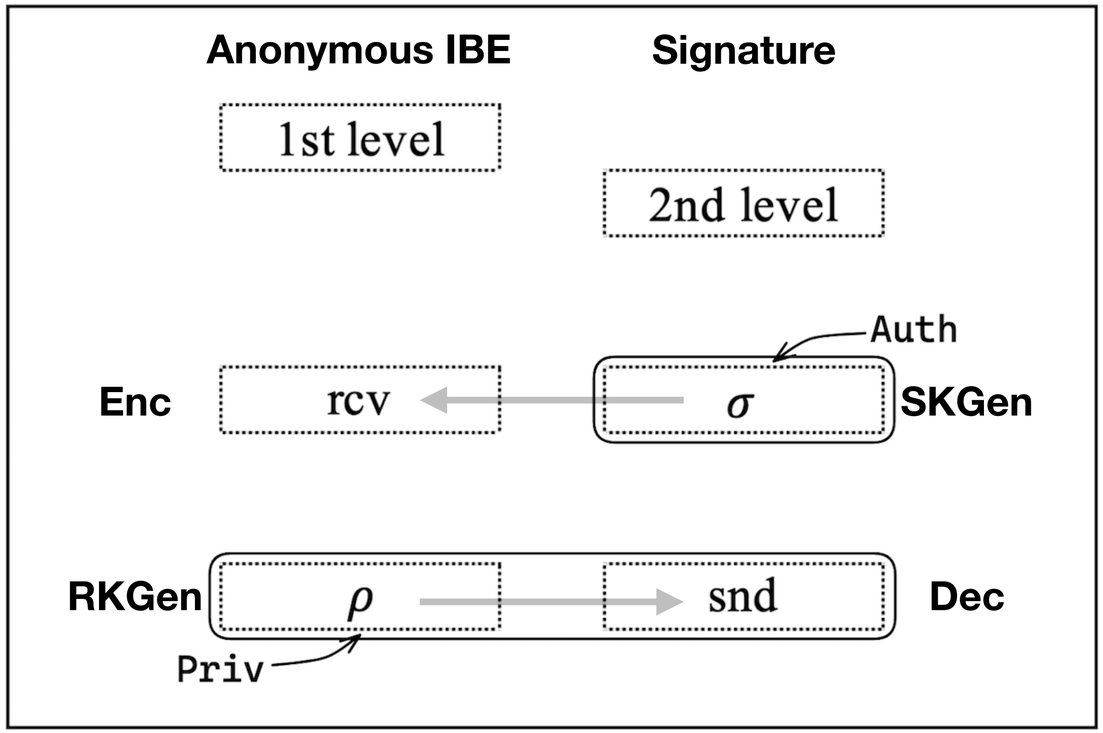
$$CT = \{\mathsf{C} = m \cdot (g_T^{\alpha})^s, \mathsf{C}_0 = g_1^{s(\mathbf{d}_1 - \mathsf{rcv}\mathbf{d}_2)}\}$$

Signature

$$Sign : \sigma_1 = g_2^{\eta \mathbf{d}_3^* + r(\sigma \mathbf{d}_3^* - \mathbf{d}_4^*)}$$

$$Verify : e(g_1^{\mathbf{d}_3 - \mathsf{snd}\mathbf{d}_4}, \sigma_1) = g_T^{\eta}$$

Construction



Anonymous IBE

$$SK_{\mathsf{id}} = g_2^{\alpha \mathbf{d}_1^* + s(\rho \mathbf{d}_1^* - \mathbf{d}_2^*)}$$ **RKGen**

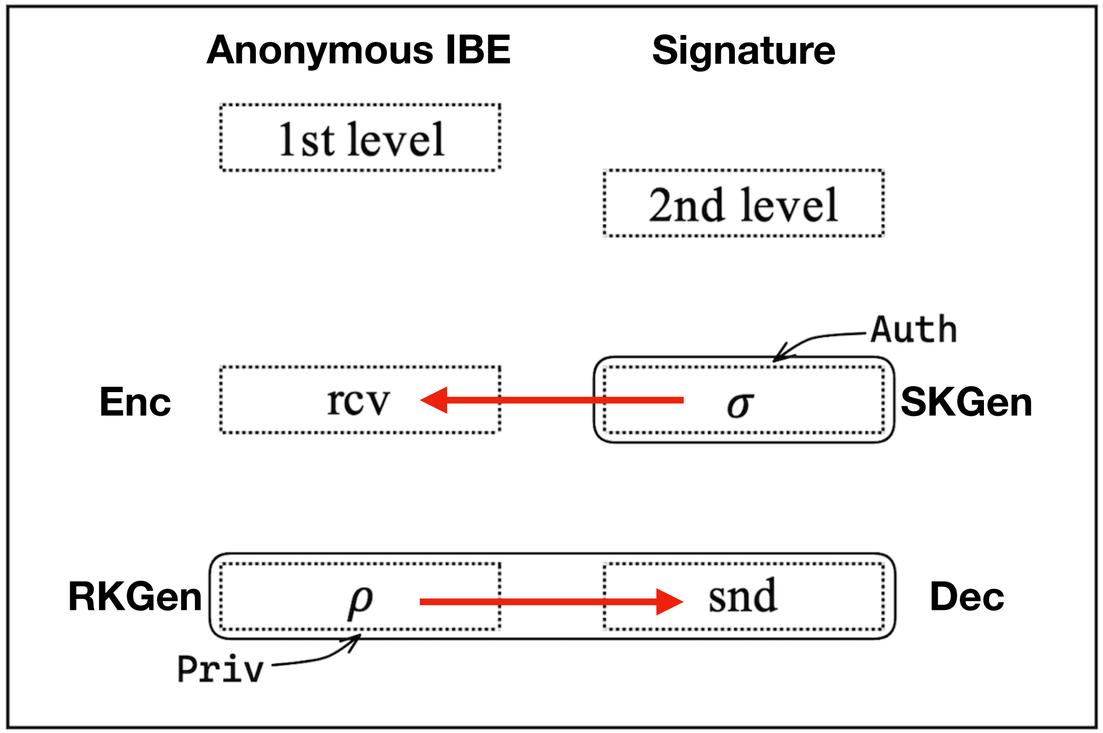
$$CT = \{\mathsf{C} = m \cdot (g_T^{\alpha})^s, \mathsf{C}_0 = g_1^{s(\mathbf{d}_1 - \mathsf{rcv}\mathbf{d}_2)}\}$$ **Enc**

Signature

$$Sign : \sigma_1 = g_2^{\eta \mathbf{d}_3^* + r(\sigma \mathbf{d}_3^* - \mathbf{d}_4^*)}$$ **SKGen**

$$Verify : e(g_1^{\mathbf{d}_3 - \mathsf{snd}\mathbf{d}_4}, \sigma_1) = g_T^{\eta}$$ **Dec**

Construction



$\mathsf{Enc}(mpk, ek_\sigma, \mathsf{rcv}, m) \rightarrow ct$

$\mathsf{Dec}(mpk, dk_\rho, \mathsf{snd}, ct) \rightarrow m$

Anonymous IBE

$SK_{\mathsf{id}} = g_2^{\alpha \mathbf{d}_1^* + s(\rho \mathbf{d}_1^* - \mathbf{d}_2^*)}$

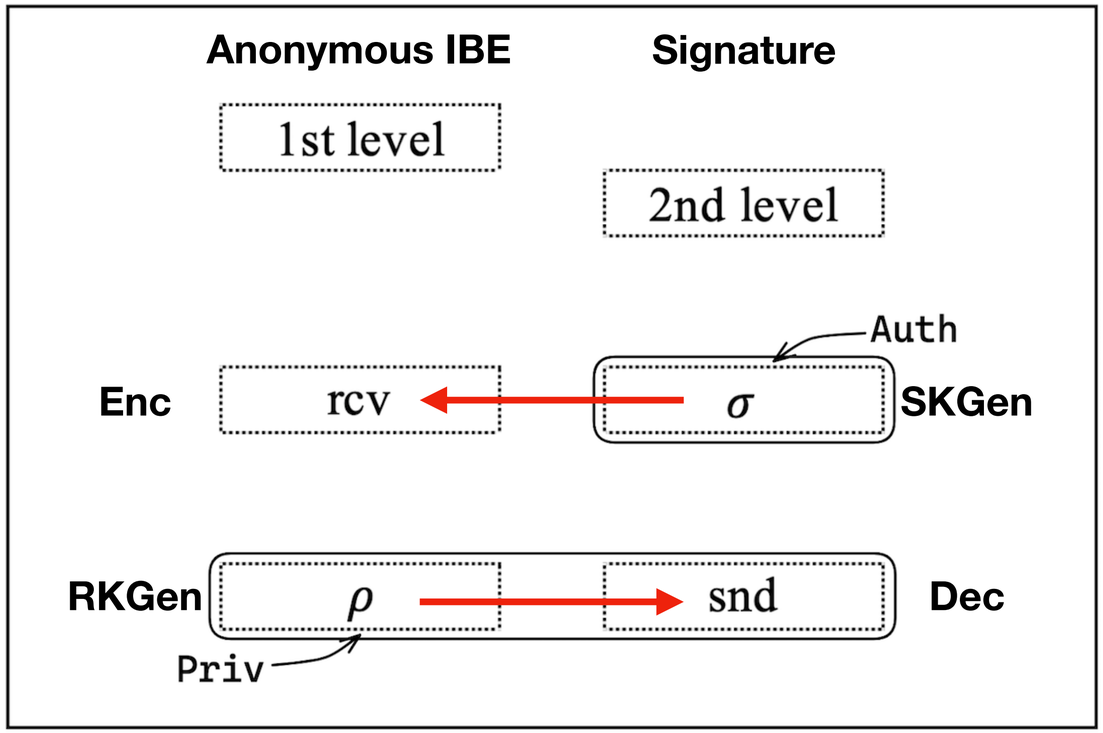
$CT = \{\mathsf{C} = m \cdot (g_T^\alpha)^s, \mathsf{C}_0 = g_1^{s(\mathbf{d}_1 + \mathsf{rcv}\mathbf{d}_2)}\}$

Signature

$Sign : \sigma_1 = g_2^{\eta \mathbf{d}_3^* + r(\sigma \mathbf{d}_3^* - \mathbf{d}_4^*)}$

$Verify : e(g_1^{\mathbf{d}_3 + \mathsf{snd}\mathbf{d}_4}, \sigma_1) = g_T^\eta$

Construction



$\mathsf{Enc}(mpk, ek_\sigma, \mathsf{rcv}, m) \rightarrow ct$

$\mathsf{Dec}(mpk, dk_\rho, \mathsf{snd}, ct) \rightarrow m$

Anonymous IBE

$SK_{\mathsf{id}} = g_2^{\alpha \mathbf{d}_1^* + s(\rho \mathbf{d}_1^* - \mathbf{d}_2^*)}$

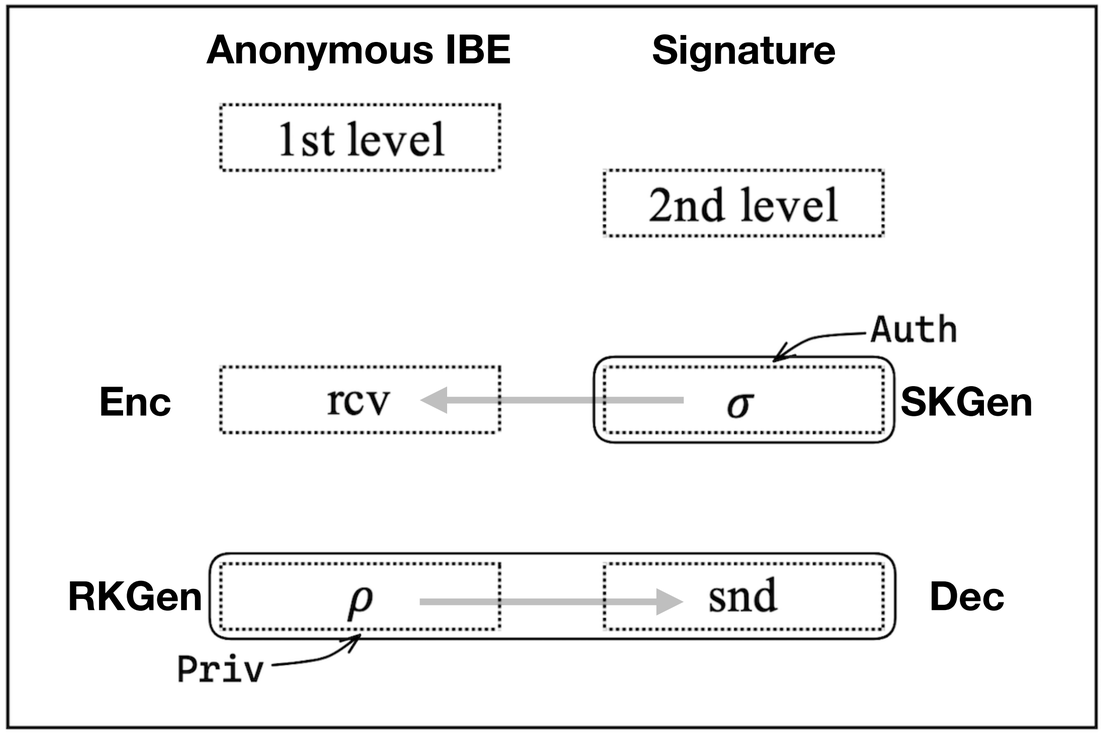
$CT = \{\mathsf{C} = m \cdot (g_T^\alpha)^s, \mathsf{C}_0 = g_1^{s(\mathbf{d}_1 + \mathsf{rcv}\mathbf{d}_2)}\}$

Signature

$Sign : \sigma_1 = g_2^{\eta \mathbf{d}_3^* + r(\sigma \mathbf{d}_3^* - \mathbf{d}_4^*)}$

$Verify : e(g_1^{\mathbf{d}_3 + \mathsf{snd}\mathbf{d}_4}, \sigma_1) = g_T^\eta$

Construction



$\mathsf{Enc}(mpk, ek_\sigma, \mathsf{rcv}, m) \rightarrow ct$

$\mathsf{Dec}(mpk, dk_\rho, \mathsf{snd}, ct) \rightarrow m$

Anonymous IBE

$$SK_{\mathsf{id}} = g_2^{\alpha \mathbf{d}_1^* + s(\rho \mathbf{d}_1^* - \mathbf{d}_2^*)}$$

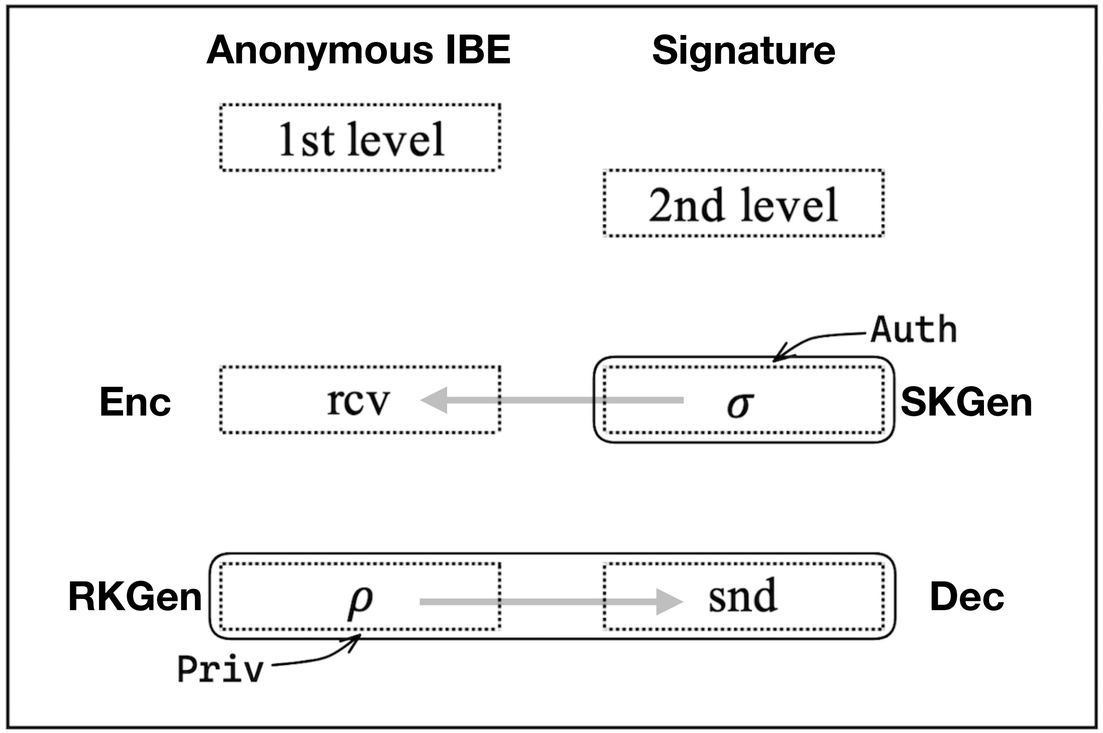
$$CT = \{\mathsf{C} = m \cdot (g_T^\alpha)^s, \mathsf{C}_0 = g_1^{s(\mathbf{d}_1 + \mathsf{rcv}\mathbf{d}_2)}\}$$

Signature

$$Sign: \sigma_1 = g_1^{\eta \mathbf{d}_3 + r(\sigma \mathbf{d}_3 - \mathbf{d}_4)}$$

$$Verify: e(g_2^{\mathbf{d}_3^* + \mathsf{snd}\mathbf{d}_4^*}, \sigma_1) \stackrel{?}{=} g_T^\eta$$

Construction



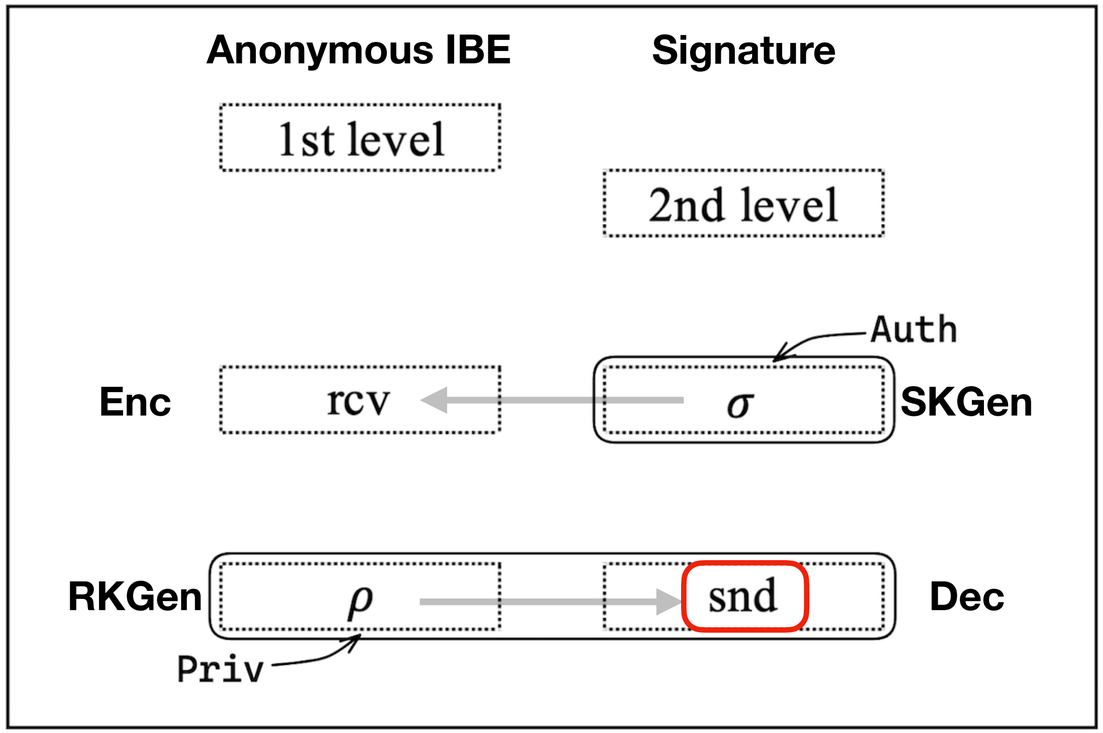
$$SKGen : ek_\sigma = g_1^{\eta \mathbf{d_3} + r(\sigma \mathbf{d_3} - \mathbf{d_4})}$$

$$RKGen : dk_\rho = g_2^{\alpha \mathbf{d_1^*} + s(\rho \mathbf{d_1^*} - \mathbf{d_2^*})}$$

$$CT = \{\mathsf{C} = m \cdot (g_T^\alpha)^z, \mathsf{C}_1 = ek_\sigma \cdot \mathsf{C}_0 = ek_\sigma \cdot g_1^{z(\mathbf{d_1} + \mathrm{rcv}\mathbf{d_2})}\}$$

$$m = \frac{\mathsf{C}}{e(\mathsf{C}_1, ?)}$$

Construction



$$SKGen : ek_\sigma = g_1^{\eta \mathbf{d_3} + r(\sigma \mathbf{d_3} - \mathbf{d_4})}$$

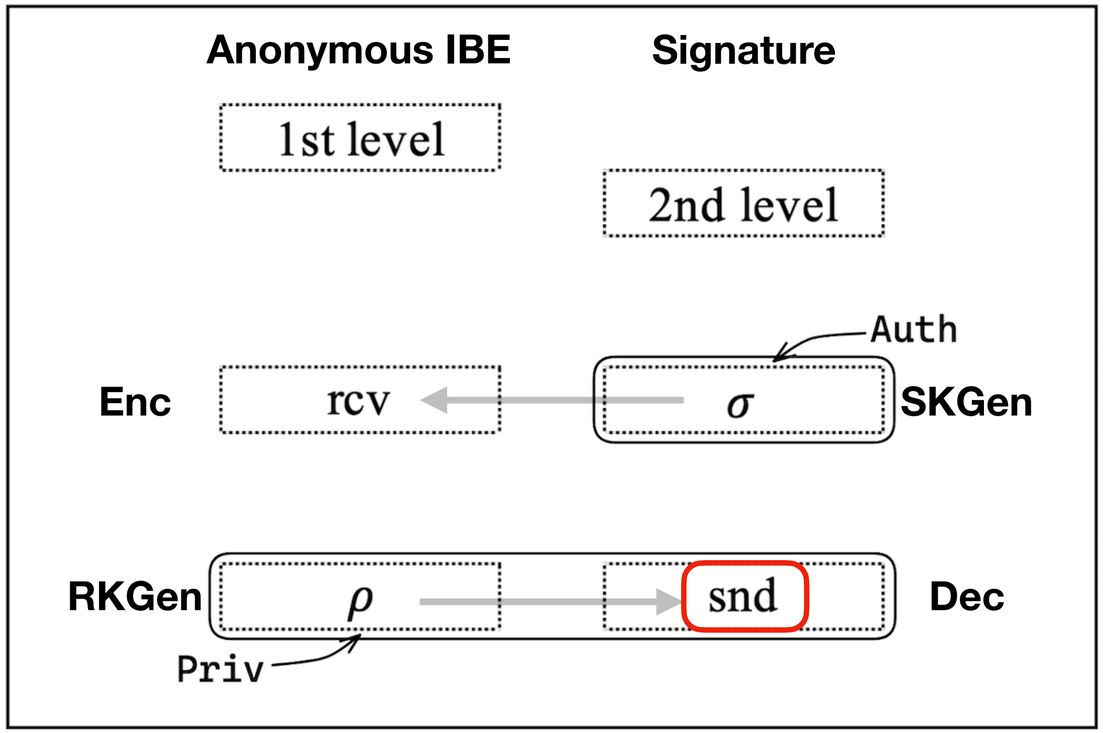
$$RKGen : dk_\rho = g_2^{\alpha \mathbf{d_1^*} + s(\rho \mathbf{d_1^*} - \mathbf{d_2^*})}$$

$$CT = \{\mathsf{C} = m \cdot (g_T^\alpha)^z, \mathsf{C}_1 = ek_\sigma \cdot \mathsf{C}_0 = ek_\sigma \cdot g_1^{z(\mathbf{d_1} + \mathrm{rcv}\mathbf{d_2})}\}$$

$$m = \frac{\mathsf{C}}{e(\mathsf{C}_1, ?)}$$

Sign: Verify ?

Construction



$$SKGen : ek_\sigma = g_1^{\eta \mathbf{d_3} + r(\sigma \mathbf{d_3} - \mathbf{d_4})}$$

$$RKGen : dk_\rho = g_2^{\alpha \mathbf{d_1^*} + s(\rho \mathbf{d_1^*} - \mathbf{d_2^*})}$$

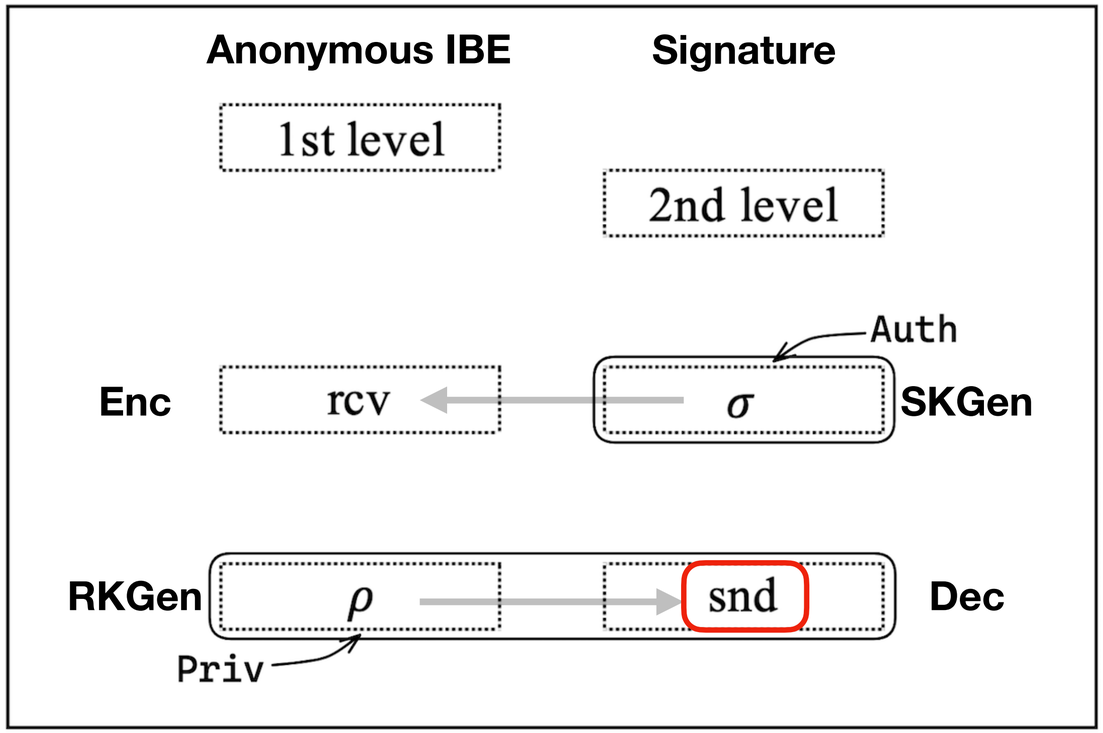
$$CT = \{\mathsf{C} = m \cdot (g_T^\alpha)^z, \mathsf{C}_1 = ek_\sigma \cdot \mathsf{C}_0 = ek_\sigma \cdot g_1^{z(\mathbf{d_1} + \mathrm{rcv}\mathbf{d_2})}\}$$

$$m = \frac{\mathsf{C}}{e(\mathsf{C}_1, ?)}$$

Sign: Verify ?

$$\mathrm{Dec}(mpk, dk_\rho, \mathsf{snd}, ct) \rightarrow m$$

Construction



$$SKGen : ek_\sigma = g_1^{\eta \mathbf{d_3} + r(\sigma \mathbf{d_3} - \mathbf{d_4})}$$

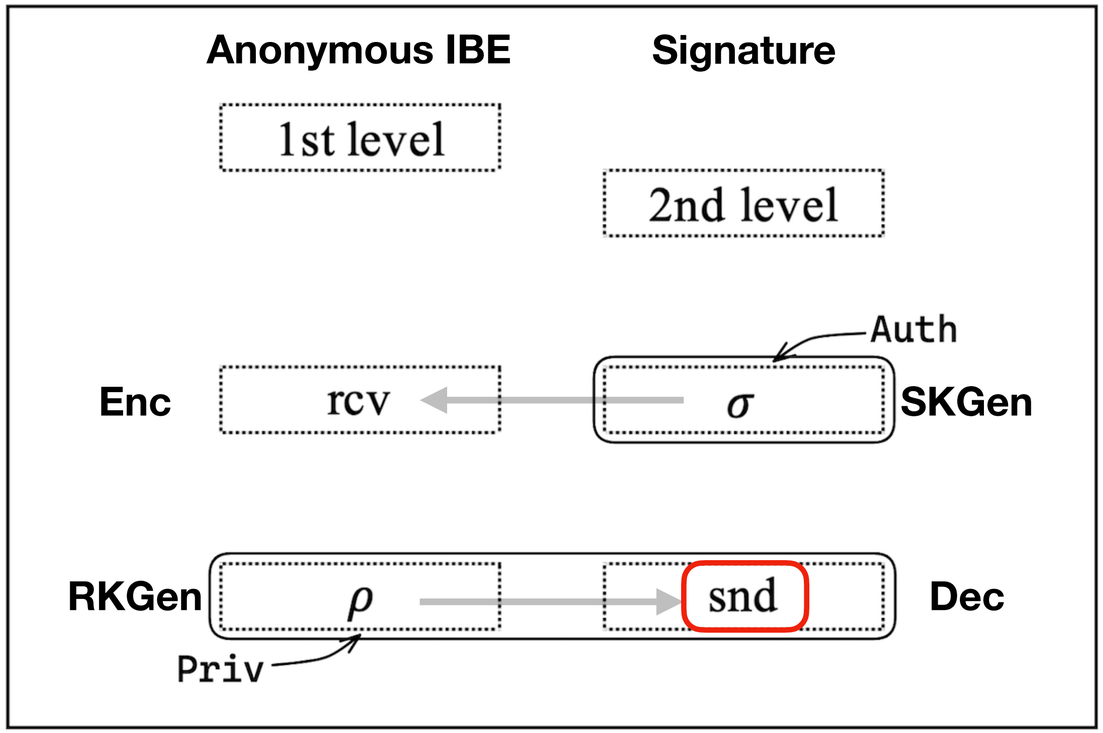
$$RKGen : dk_\rho = g_2^{\alpha \mathbf{d_1^*} + s(\rho \mathbf{d_1^*} - \mathbf{d_2^*})} \qquad g_2^{\mathbf{d_3^*} + \mathsf{snd}\mathbf{d_4^*}} \ \textbf{?}$$

$$CT = \{\mathsf{C} = m \cdot (g_T^\alpha)^z, \mathsf{C}_1 = ek_\sigma \cdot \mathsf{C}_0 = ek_\sigma \cdot g_1^{z(\mathbf{d_1} + \mathsf{rcv}\mathbf{d_2})}\}$$

$$m = \frac{\mathsf{C}}{e(\mathsf{C}_1, ?)}$$

$$\mathrm{Dec}(mpk, dk_\rho, \mathsf{snd}, ct) \rightarrow m$$

Construction



$$SKGen : ek_\sigma = g_1^{\eta \mathbf{d_3} + r(\sigma \mathbf{d_3} - \mathbf{d_4})}$$

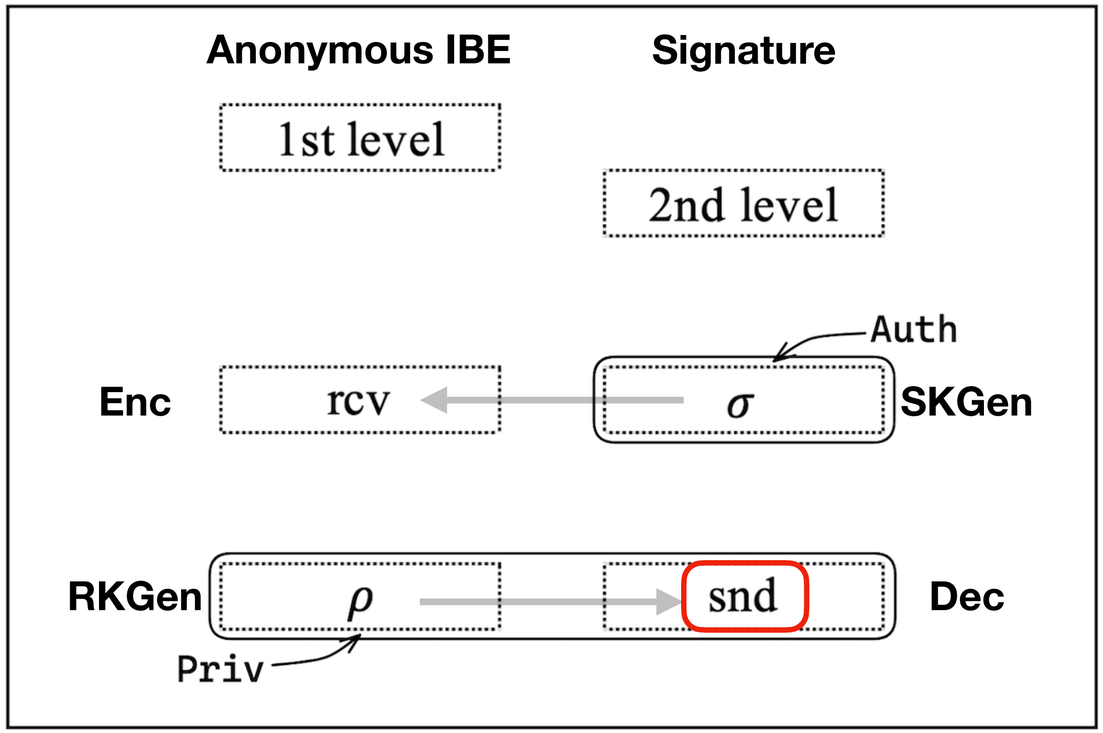
$$RKGen : dk_\rho = g_2^{\alpha \mathbf{d_1^*} + s(\rho \mathbf{d_1^*} - \mathbf{d_2^*})} \qquad g_2^{\mathbf{d_3^*} + \mathrm{snd} \mathbf{d_4^*}} \ \textbf{?}$$

$$CT = \{\mathsf{C} = m \cdot (g_T^\alpha)^z, \mathsf{C}_1 = ek_\sigma \cdot \mathsf{C}_0 = ek_\sigma \cdot g_1^{z(\mathbf{d_1} + \mathrm{rcv} \mathbf{d_2})}\}$$

$$m = \frac{\mathsf{C}}{e(\mathsf{C}_1, ?)}$$

$$\mathrm{Dec}(mpk, dk_\rho, \mathsf{snd}, ct) \rightarrow m$$

Construction



$$SKGen : ek_\sigma = g_1^{\eta \mathbf{d_3} + r(\sigma \mathbf{d_3} - \mathbf{d_4})}$$

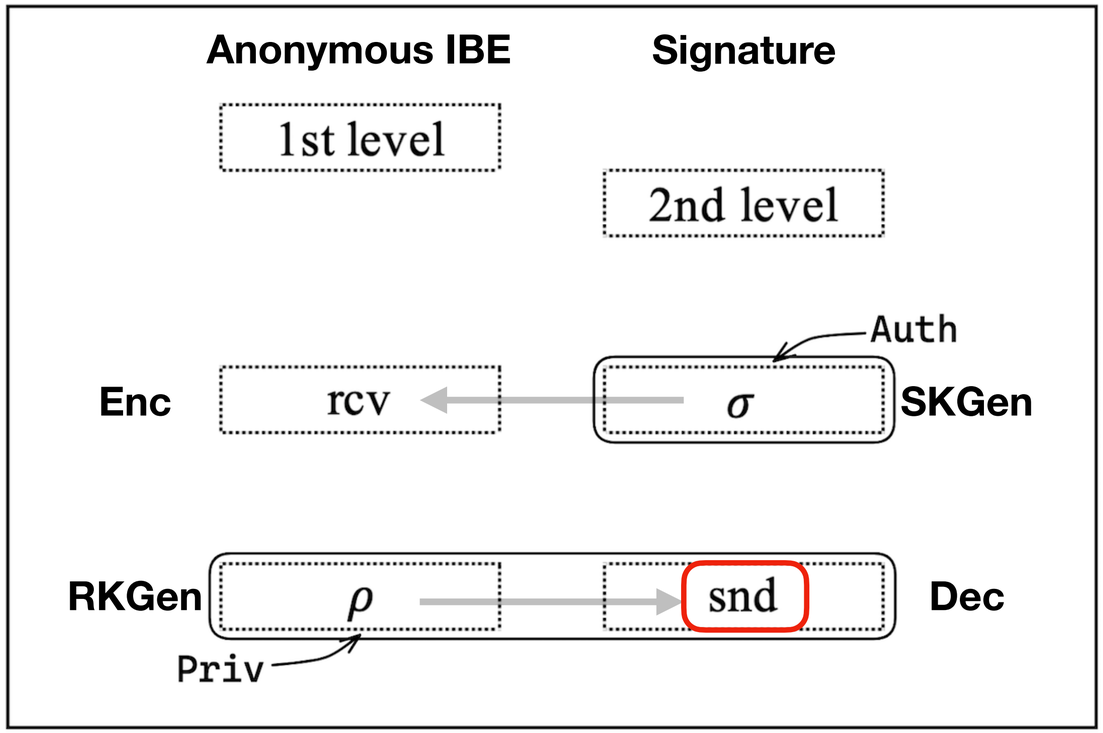
$$RKGen : dk_\rho = g_2^{\alpha \mathbf{d_1^*} + s(\rho \mathbf{d_1^*} - \mathbf{d_2^*})} \qquad g_2^{\mathbf{d_3^*} + \mathrm{snd}\mathbf{d_4^*}} \longrightarrow g_2^{\mathbf{d_3^*}}, g_2^{\mathbf{d_4^*}}$$

$$CT = \{\mathsf{C} = m \cdot (g_T^\alpha)^z, \mathsf{C}_1 = ek_\sigma \cdot \mathsf{C}_0 = ek_\sigma \cdot g_1^{z(\mathbf{d_1} + \mathrm{rcv}\mathbf{d_2})}\}$$

$$m = \frac{\mathsf{C}}{e(\mathsf{C}_1, ?)}$$

$$\mathrm{Dec}(mpk, dk_\rho, \mathsf{snd}, ct) \rightarrow m$$

Construction



$$SKGen : ek_\sigma = g_1^{\eta \mathbf{d_3} + r(\sigma \mathbf{d_3} - \mathbf{d_4})}$$

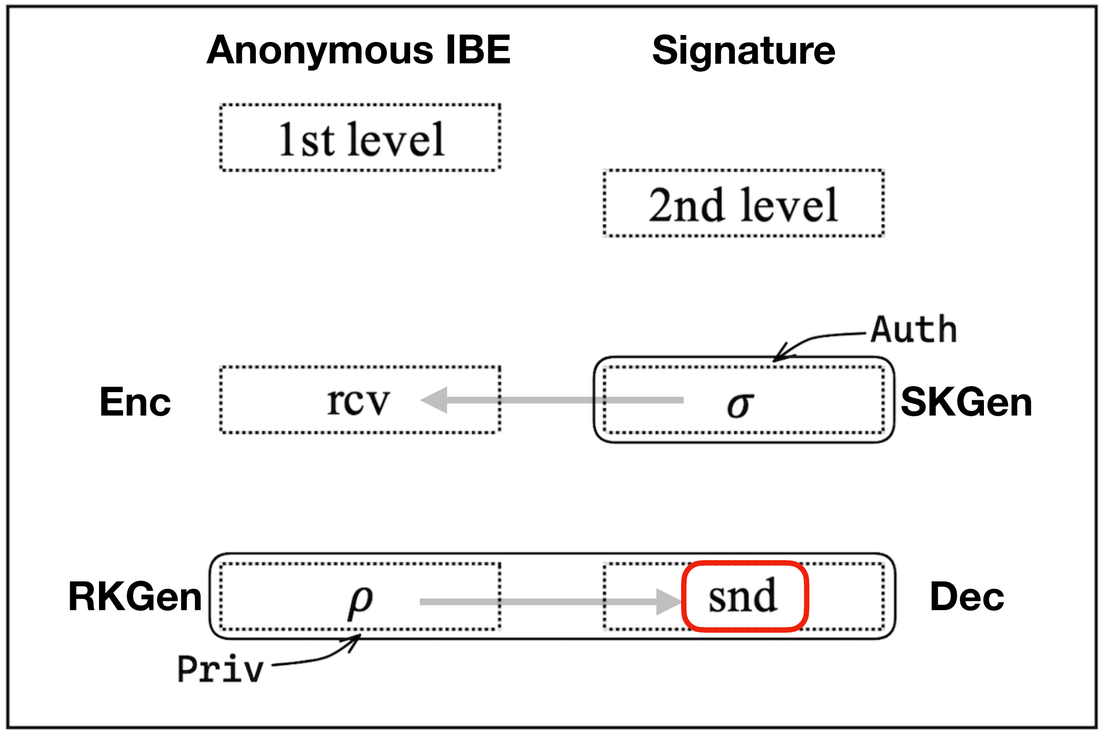
$$RKGen : dk_\rho = g_2^{\alpha \mathbf{d_1^*} + s(\rho \mathbf{d_1^*} - \mathbf{d_2^*})} \qquad g_2^{\mathbf{d_3^*} + \mathsf{snd}\mathbf{d_4^*}} \longrightarrow g_2^{\mathbf{d_3^*}}, g_2^{\mathbf{d_4^*}}$$

$$CT = \{\mathsf{C} = m \cdot (g_T^\alpha)^z, \mathsf{C}_1 = ek_\sigma \cdot \mathsf{C}_0 = ek_\sigma \cdot g_1^{z(\mathbf{d_1} + \mathsf{rcv}\mathbf{d_2})}\}$$

$$m = \frac{\mathsf{C}}{e(\mathsf{C}_1, ?)}$$

$$\mathrm{Dec}(mpk, dk_\rho, \mathsf{snd}, ct) \rightarrow m$$

Construction



$$SKGen : ek_\sigma = g_1^{\eta \mathbf{d_3} + r(\sigma \mathbf{d_3} - \mathbf{d_4})}$$

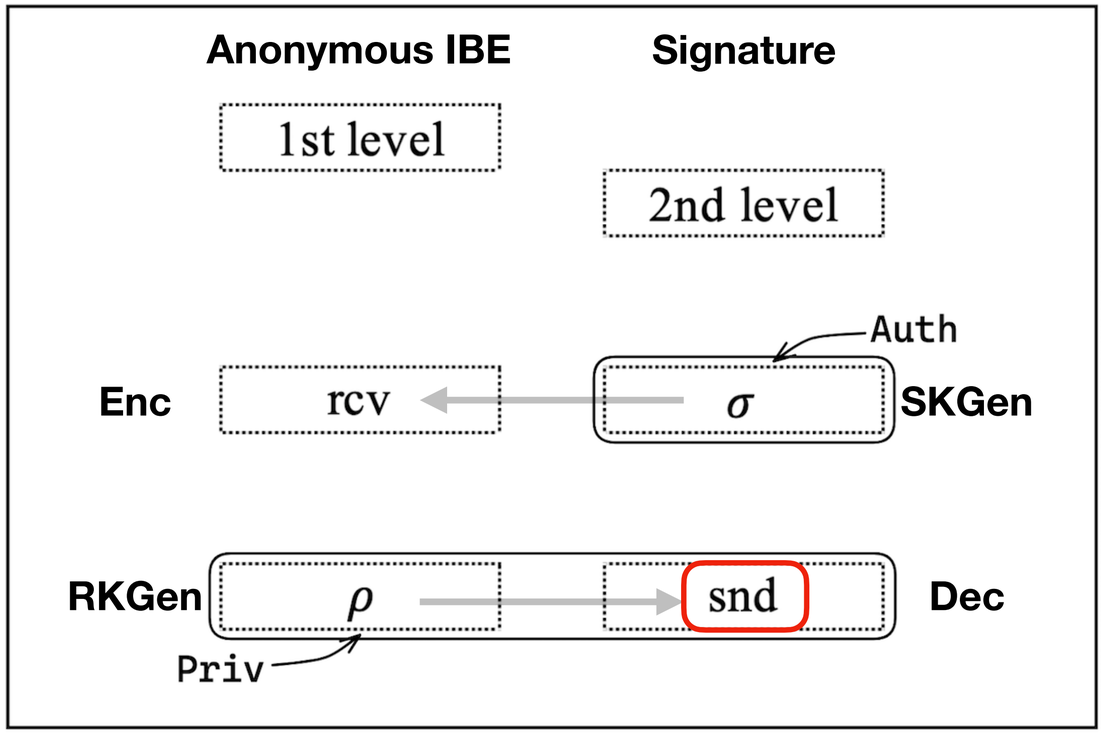
$$RKGen : dk_\rho = g_2^{\alpha \mathbf{d_1^*} + s(\rho \mathbf{d_1^*} - \mathbf{d_2^*})} \qquad g_2^{\mathbf{d_3^*} + \mathsf{snd}\mathbf{d_4^*}} \longrightarrow g_2^{\mathbf{d_3^*}}, g_2^{\mathbf{d_4^*}}$$

$$CT = \{\mathsf{C} = m \cdot (g_T^\alpha)^z, \mathsf{C}_1 = ek_\sigma \cdot \mathsf{C}_0 = ek_\sigma \cdot g_1^{z(\mathbf{d_1} + \mathsf{rcv}\mathbf{d_2})}\}$$

$$m = \frac{\mathsf{C}}{e(\mathsf{C}_1, ?)}$$

$$\mathrm{Dec}(mpk, dk_\rho, \mathsf{snd}, ct) \rightarrow m$$

Construction



$$SKGen : ek_\sigma = g_1^{\eta \mathbf{d_3} + r(\sigma \mathbf{d_3} - \mathbf{d_4})}$$

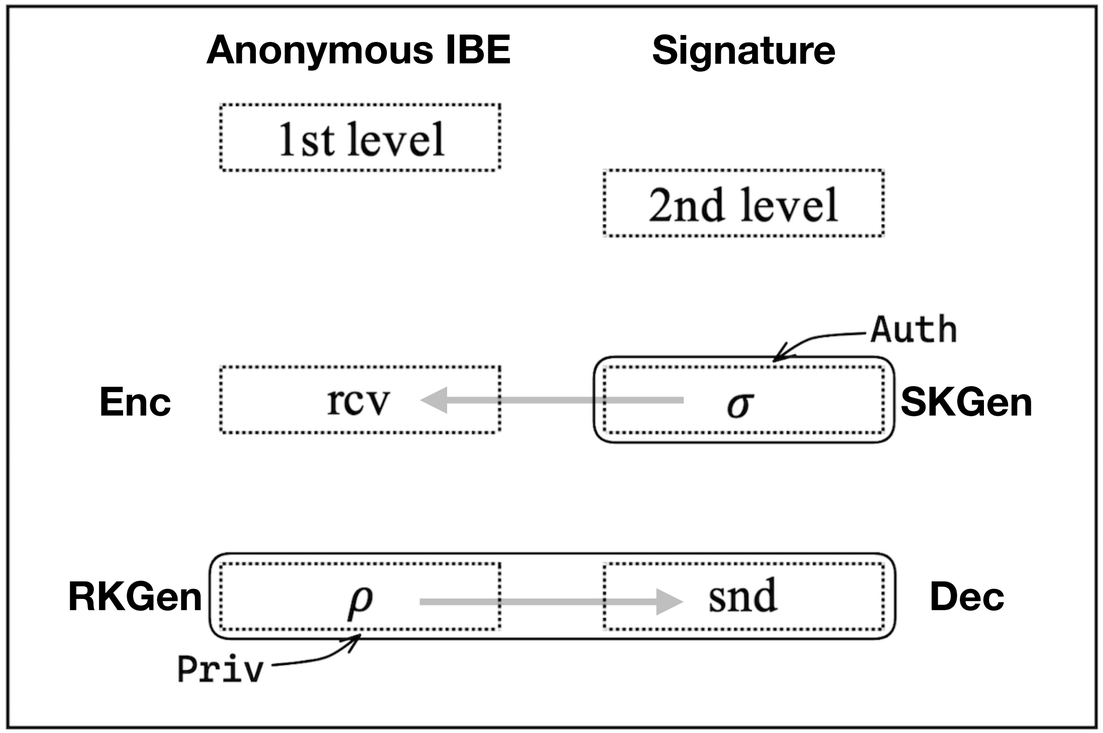
$$RKGen : dk_\rho = g_2^{\alpha \mathbf{d_1^*} + s(\rho \mathbf{d_1^*} - \mathbf{d_2^*})}$$

$$CT = \{\mathsf{C} = m \cdot (g_T^\alpha)^z, \mathsf{C}_1 = ek_\sigma \cdot \mathsf{C}_0 = ek_\sigma \cdot g_1^{z(\mathbf{d_1} + \mathrm{rcv}\mathbf{d_2})}\}$$

$$m = \frac{\mathsf{C}}{e(\mathsf{C}_1, ?)} \leftarrow g_2^{\mathbf{d_3^*} + \mathrm{snd}\mathbf{d_4^*}} \leftarrow g_2^{\mathbf{d_3^*}}, g_2^{\mathbf{d_4^*}}$$

$$\mathrm{Dec}(mpk, dk_\rho, \mathsf{snd}, ct) \rightarrow m$$

Construction



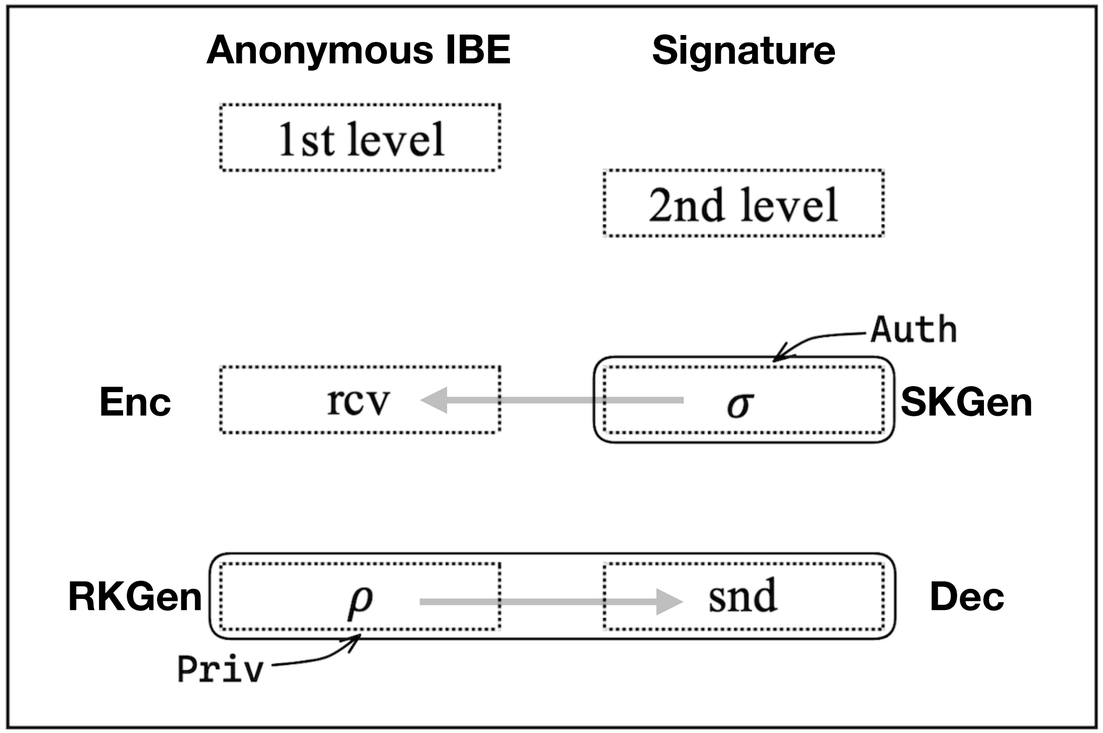
$$SKGen : ek_\sigma = g_1^{\eta \mathbf{d_3} + r(\sigma \mathbf{d_3} - \mathbf{d_4})}$$

$$RKGen : dk_\rho = \{k_1 = g_2^{\alpha \mathbf{d_1^*} + s_1(\rho \mathbf{d_1^*} - \mathbf{d_2^*}) + s \mathbf{d_3^*}}, k_2 = g_2^{s_2(\rho \mathbf{d_1^*} - \mathbf{d_2^*}) + s \mathbf{d_4^*}}\}$$

$$CT = \{\mathsf{C} = m \cdot (g_T^\alpha)^z, \mathsf{C}_1 = ek_\sigma \cdot \mathsf{C}_0 = ek_\sigma \cdot g_1^{z(\mathbf{d_1} + \mathsf{rcv} \mathbf{d_2})}\}$$

$$m = \frac{\mathsf{C}}{e(\mathsf{C}_1, k_1 \cdot k_2^{\mathsf{snd}})}$$

Construction



$$mpk = \mathbb{G}; g_T^{\alpha}, g_1^{\mathbf{d_1}}, g_1^{\mathbf{d_2}}, g_T^{\eta}$$

$$msk = \alpha, g_2^{\mathbf{d_1^*}}, g_2^{\mathbf{d_2^*}}, \eta, g_1^{\mathbf{d_3}}, g_1^{\mathbf{d_4}}, g_2^{\mathbf{d_3^*}}, g_2^{\mathbf{d_4^*}}$$

$$SKGen : ek_{\sigma} = g_1^{\eta\mathbf{d_3}+r(\sigma\mathbf{d_3}-\mathbf{d_4})}$$

$$RKGen : dk_{\rho} = \{k_1 = g_2^{\alpha\mathbf{d_1^*}+s_1(\rho\mathbf{d_1^*}-\mathbf{d_2^*})+s\mathbf{d_3^*}}, k_2 = g_2^{s_2(\rho\mathbf{d_1^*}-\mathbf{d_2^*})+s\mathbf{d_4^*}}, k_3 = (g_T^{\eta})^s\}$$

$$CT = \{\mathsf{C} = m \cdot (g_T^{\alpha})^z, \mathsf{C}_1 = ek_{\sigma} \cdot \mathsf{C}_0 = ek_{\sigma} \cdot g_1^{z(\mathbf{d_1}+\mathsf{rcv}\mathbf{d_2})}\}$$

$$m = \frac{\mathsf{C}}{e(\mathsf{C}_1, k_1 \cdot k_2^{\mathsf{snd}}) \cdot k_3^{-1}}$$

Proof

$\mathbf{G}^{\text{ib-priv}}_{\Pi,\mathsf{A}}(\lambda)$ **Privacy**

$(\mathsf{mpk}, \mathsf{msk}) \leftarrow\!\!\$\ \mathsf{Setup}(1^\lambda)$

$(m_0, m_1, \mathsf{rcv}_0, \mathsf{rcv}_1, \sigma_0, \sigma_1, \alpha) \leftarrow\!\!\$\ \mathsf{A}_1^{\mathsf{O}_1,\mathsf{O}_2}(1^\lambda, \mathsf{mpk})$

$b \leftarrow\!\!\$\ \{0,1\}$

$\mathsf{ek}_{\sigma_b} \leftarrow\!\!\$\ \mathsf{SKGen}(\mathsf{msk}, \sigma_b)$

$c \leftarrow\!\!\$\ \mathsf{Enc}(\mathsf{ek}_{\sigma_b}, \mathsf{rcv}_b, m_b)$

$b' \leftarrow\!\!\$\ \mathsf{A}_2^{\mathsf{O}_1,\mathsf{O}_2}(1^\lambda, c, \alpha)$

If $(b' = b)$ **return** 1

Else **return** 0

$\mathbf{G}^{\text{ib-auth}}_{\Pi,\mathsf{A}}(\lambda)$ **Authenticity**

$(\mathsf{mpk}, \mathsf{msk}) \leftarrow\!\!\$\ \mathsf{Setup}(1^\lambda)$

$(c, \rho, \mathsf{snd}) \leftarrow\!\!\$\ \mathsf{A}^{\mathsf{O}_1,\mathsf{O}_2}(1^\lambda, \mathsf{mpk})$

$\mathsf{dk}_\rho \leftarrow\!\!\$\ \mathsf{RKGen}(\mathsf{msk}, \rho)$

$m = \mathsf{Dec}(\mathsf{dk}_\rho, \mathsf{snd}, c)$

If $\forall \sigma \in \mathcal{Q}_{\mathsf{O}_1} : (\sigma \neq \mathsf{snd}) \wedge (m \neq \perp)$

  return 1

Else **return** 0

Proof of Privacy

$IB\text{-}ME\_mpk$, $IB\text{-}ME\_msk$

$$ek_\sigma = g_1^{\eta\mathbf{d_3}+r(\sigma\mathbf{d_3}-\mathbf{d_4})}$$

$$dk_\rho = \{k_1 = g_2^{\alpha\mathbf{d_1^*}+s_1(\rho\mathbf{d_1^*}-\mathbf{d_2^*})+s\mathbf{d_3^*}}, k_2 = g_2^{s_2(\rho\mathbf{d_1^*}-\mathbf{d_2^*})+s\mathbf{d_4^*}}, k_3 = (g_T^\eta)^s\}$$

$$ct = \{\mathsf{C} = m \cdot (g_T^\alpha)^z, \mathsf{C}_0 = ek_\sigma \cdot g_1^{z(\mathbf{d_1}+\mathsf{rcv}\mathbf{d_2})}\}$$

$$m = \frac{\mathsf{C}}{e(\mathsf{C}_0, k_1 \cdot k_2^{\mathsf{snd}}) \cdot k_3^{-1}}$$

Anonymous Identity-Based Encryption

Dual System Encryption

[Waters09]: Waters, B.: Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. CRYPTO 2009
[CLLWW14]: Chen, J., Lim, H.W., Ling, S., Wang, H., Wee, H.: Shorter identity-based encryption via asymmetric pairings. Des. Codes Cryptogr. 2014

Proof of Privacy

IB-ME_mpk, IB-ME_msk

$ek_\sigma = g_1^{\eta \mathbf{d_3} + r(\sigma \mathbf{d_3} - \mathbf{d_4})}$

$dk_\rho = \{k_1 = g_2^{\alpha \mathbf{d_1^*} + s_1(\rho \mathbf{d_1^*} - \mathbf{d_2^*}) + s\mathbf{d_3^*}}, k_2 = g_2^{s_2(\rho \mathbf{d_1^*} - \mathbf{d_2^*}) + s\mathbf{d_4^*}}, k_3 = (g_T^\eta)^s\}$

$ct = \{\mathsf{C} = m \cdot (g_T^\alpha)^z, \mathsf{C}_0 = ek_\sigma \cdot g_1^{z(\mathbf{d_1} + \mathsf{rcv}\mathbf{d_2})}\}$

$m = \dfrac{\mathsf{C}}{e(\mathsf{C}_0, k_1 \cdot k_2^{\mathsf{snd}}) \cdot k_3^{-1}}$

EncryptSF: The algorithm picks $z, r, r_5, r_6, r_7, r_8 \xleftarrow{R} \mathbb{Z}_q$ and forms a semi-functional ciphertext as

$$ek_\sigma := g_1^{\eta \mathbf{d_3} + r(\sigma \mathbf{d_3} - \mathbf{d_4})}$$

$$\begin{aligned}\mathsf{CT}^{(\mathsf{SF})}_{ek_\sigma, \mathsf{rcv}} := \{\mathsf{C} :&= m \cdot (g_T^\alpha)^z, \mathsf{C}_0 := ek_\sigma \cdot g_1^{z(\mathbf{d_1} + \mathsf{rcv}\mathbf{d_2}) + [r_5\mathbf{d_5} + r_6\mathbf{d_6} + r_7\mathbf{d_7} + r_8\mathbf{d_8}]} \\ &= g_1^{\eta \mathbf{d_3} + r(\sigma \mathbf{d_3} - \mathbf{d_4}) + z(\mathbf{d_1} + \mathsf{rcv}\mathbf{d_2}) + [r_5\mathbf{d_5} + r_6\mathbf{d_6} + r_7\mathbf{d_7} + r_8\mathbf{d_8}]}\}.\end{aligned}$$

Proof of Privacy

IB-ME_mpk, IB-ME_msk

$ek_\sigma = g_1^{\eta \mathbf{d_3} + r(\sigma \mathbf{d_3} - \mathbf{d_4})}$

$dk_\rho = \{k_1 = g_2^{\alpha \mathbf{d_1^*} + s_1(\rho \mathbf{d_1^*} - \mathbf{d_2^*}) + s \mathbf{d_3^*}}, k_2 = g_2^{s_2(\rho \mathbf{d_1^*} - \mathbf{d_2^*}) + s \mathbf{d_4^*}}, k_3 = (g_T^\eta)^s\}$

$ct = \{\mathsf{C} = m \cdot (g_T^\alpha)^z, \mathsf{C}_0 = ek_\sigma \cdot g_1^{z(\mathbf{d_1} + \mathsf{rcv} \mathbf{d_2})}\}$

$$m = \frac{\mathsf{C}}{e(\mathsf{C}_0, k_1 \cdot k_2^{\mathsf{snd}}) \cdot k_3^{-1}}$$

EncryptSF: The algorithm picks $z, r, r_5, r_6, r_7, r_8 \xleftarrow{R} \mathbb{Z}_q$ and forms a semi-functional ciphertext as

$$ek_\sigma := g_1^{\eta \mathbf{d_3} + r(\sigma \mathbf{d_3} - \mathbf{d_4})}$$

$$\begin{aligned} \mathsf{CT}^{(\mathsf{SF})}_{ek_\sigma, \mathsf{rcv}} := \{\mathsf{C} :&= m \cdot (g_T^\alpha)^z, \mathsf{C}_0 := ek_\sigma \cdot g_1^{z(\mathbf{d_1} + \mathsf{rcv} \mathbf{d_2}) + [r_5 \mathbf{d_5} + r_6 \mathbf{d_6} + r_7 \mathbf{d_7} + r_8 \mathbf{d_8}]} \\ &= g_1^{\eta \mathbf{d_3} + r(\sigma \mathbf{d_3} - \mathbf{d_4}) + z(\mathbf{d_1} + \mathsf{rcv} \mathbf{d_2}) + [r_5 \mathbf{d_5} + r_6 \mathbf{d_6} + r_7 \mathbf{d_7} + r_8 \mathbf{d_8}]}\}. \end{aligned}$$

Proof of Privacy

IB-ME_mpk, IB-ME_msk

$ek_\sigma = g_1^{\eta \mathbf{d_3} + r(\sigma \mathbf{d_3} - \mathbf{d_4})}$

$dk_\rho = \{k_1 = g_2^{\alpha \mathbf{d_1^*} + s_1(\rho \mathbf{d_1^*} - \mathbf{d_2^*}) + s \mathbf{d_3^*}}, k_2 = g_2^{s_2(\rho \mathbf{d_1^*} - \mathbf{d_2^*}) + s \mathbf{d_4^*}}, k_3 = (g_T^\eta)^s\}$

$ct = \{\mathsf{C} = m \cdot (g_T^\alpha)^z, \mathsf{C}_0 = ek_\sigma \cdot g_1^{z(\mathbf{d_1} + \mathsf{rcv} \mathbf{d_2})}\}$

$$m = \frac{\mathsf{C}}{e(\mathsf{C}_0, k_1 \cdot k_2^{\mathsf{snd}}) \cdot k_3^{-1}}$$

EncryptSF: The algorithm picks $z, r, r_5, r_6, r_7, r_8 \xleftarrow{R} \mathbb{Z}_q$ and forms a semi-functional ciphertext as

$$ek_\sigma := g_1^{\eta \mathbf{d_3} + r(\sigma \mathbf{d_3} - \mathbf{d_4})}$$

$$\begin{aligned} \mathsf{CT}^{(\mathsf{SF})}_{ek_\sigma, \mathsf{rcv}} := \{\mathsf{C} := m \cdot (g_T^\alpha)^z, \mathsf{C}_0 := ek_\sigma \cdot g_1^{z(\mathbf{d_1} + \mathsf{rcv} \mathbf{d_2}) + [r_5 \mathbf{d_5} + r_6 \mathbf{d_6} + r_7 \mathbf{d_7} + r_8 \mathbf{d_8}]} \\ = g_1^{\eta \mathbf{d_3} + r(\sigma \mathbf{d_3} - \mathbf{d_4}) + z(\mathbf{d_1} + \mathsf{rcv} \mathbf{d_2}) + [r_5 \mathbf{d_5} + r_6 \mathbf{d_6} + r_7 \mathbf{d_7} + r_8 \mathbf{d_8}]}\}. \end{aligned}$$

KeyGenSF: The algorithm picks $s, s_1, s_2, \{s_{i,1}\}_{i=5,\ldots,8} \xleftarrow{R} \mathbb{Z}_q$ and forms the inter-semi-functional secret key as

$$\begin{aligned} \mathsf{dk}_\rho^{(\mathsf{inter\text{-}SF})} := \{\ k_1 = g_2^{\alpha \mathbf{d_1^*} + s_1(\rho \mathbf{d_1^*} - \mathbf{d_2^*}) + s \mathbf{d_3^*} + [s_{5,1} \mathbf{d_5^*} + s_{6,1} \mathbf{d_6^*} + s_{7,1} \mathbf{d_7^*}]}, \\ k_2 = g_2^{s_2(\rho \mathbf{d_1^*} - \mathbf{d_2^*}) + s \mathbf{d_4^*}},\ k_3 = (g_T^\eta)^s\}; \end{aligned}$$

Proof of Privacy

IB-ME_mpk, IB-ME_msk

$$ek_\sigma = g_1^{\eta \mathbf{d_3} + r(\sigma \mathbf{d_3} - \mathbf{d_4})}$$

$$dk_\rho = \{k_1 = g_2^{\alpha \mathbf{d_1^*} + s_1(\rho \mathbf{d_1^*} - \mathbf{d_2^*}) + s\mathbf{d_3^*}}, k_2 = g_2^{s_2(\rho \mathbf{d_1^*} - \mathbf{d_2^*}) + s\mathbf{d_4^*}}, k_3 = (g_T^\eta)^s\}$$

$$ct = \{\mathsf{C} = m \cdot (g_T^\alpha)^z, \mathsf{C}_0 = ek_\sigma \cdot g_1^{z(\mathbf{d_1} + \mathsf{rcv}\mathbf{d_2})}\}$$

$$m = \frac{\mathsf{C}}{e(\mathsf{C}_0, k_1 \cdot k_2^{\mathsf{snd}}) \cdot k_3^{-1}}$$

EncryptSF: The algorithm picks $z, r, r_5, r_6, r_7, r_8 \xleftarrow{R} \mathbb{Z}_q$ and forms a semi-functional ciphertext as

$$ek_\sigma := g_1^{\eta \mathbf{d_3} + r(\sigma \mathbf{d_3} - \mathbf{d_4})}$$

$$\begin{aligned}\mathsf{CT}^{(\mathsf{SF})}_{ek_\sigma, \mathsf{rcv}} := \{\mathsf{C} :&= m \cdot (g_T^\alpha)^z, \mathsf{C}_0 := ek_\sigma \cdot g_1^{z(\mathbf{d_1} + \mathsf{rcv}\mathbf{d_2}) + [r_5\mathbf{d_5} + r_6\mathbf{d_6} + r_7\mathbf{d_7} + r_8\mathbf{d_8}]} \\ &= g_1^{\eta \mathbf{d_3} + r(\sigma \mathbf{d_3} - \mathbf{d_4}) + z(\mathbf{d_1} + \mathsf{rcv}\mathbf{d_2}) + [r_5\mathbf{d_5} + r_6\mathbf{d_6} + r_7\mathbf{d_7} + r_8\mathbf{d_8}]}\}.\end{aligned}$$

KeyGenSF: The algorithm picks $s, s_1, s_2, \{s_{i,1}\}_{i=5,\ldots,8} \xleftarrow{R} \mathbb{Z}_q$ and forms the inter-semi-functional secret key as

$$\begin{aligned}\mathsf{dk}^{(\mathsf{inter\text{-}SF})}_\rho := \{\ k_1 &= g_2^{\alpha \mathbf{d_1^*} + s_1(\rho \mathbf{d_1^*} - \mathbf{d_2^*}) + s\mathbf{d_3^*} + [s_{5,1}\mathbf{d_5^*} + s_{6,1}\mathbf{d_6^*} + s_{7,1}\mathbf{d_7^*}]}, \\ k_2 &= g_2^{s_2(\rho \mathbf{d_1^*} - \mathbf{d_2^*}) + s\mathbf{d_4^*}},\ k_3 = (g_T^\eta)^s\};\end{aligned}$$

The algorithm picks $s, s_1, s_2, \{s_{i,j}\}_{i=5,\ldots,8;j=1,2} \xleftarrow{R} \mathbb{Z}_q$ and forms the semi-functional secret key as

$$\begin{aligned}\mathsf{dk}^{(\mathsf{SF})}_\rho := \{\ k_1 &= g_2^{\alpha \mathbf{d_1^*} + s_1(\rho \mathbf{d_1^*} - \mathbf{d_2^*}) + s\mathbf{d_3^*} + [s_{5,1}\mathbf{d_5^*} + s_{6,1}\mathbf{d_6^*} + s_{7,1}\mathbf{d_7^*}]}, \\ k_2 &= g_2^{s_2(\rho \mathbf{d_1^*} - \mathbf{d_2^*}) + s\mathbf{d_4^*} + [s_{5,2}\mathbf{d_5^*} + s_{6,2}\mathbf{d_6^*} + s_{8,2}\mathbf{d_8^*}]},\ k_3 = (g_T^\eta)^s\}.\end{aligned}$$

Hereafter we will ignore k_3 since it is always correctly generated.

Proof of Privacy

IB-ME_mpk, *IB-ME_msk*

$ek_\sigma = g_1^{\eta \mathbf{d_3} + r(\sigma \mathbf{d_3} - \mathbf{d_4})}$

$dk_\rho = \{k_1 = g_2^{\alpha \mathbf{d_1^*} + s_1(\rho \mathbf{d_1^*} - \mathbf{d_2^*}) + s \mathbf{d_3^*}}, k_2 = g_2^{s_2(\rho \mathbf{d_1^*} - \mathbf{d_2^*}) + s \mathbf{d_4^*}}, k_3 = (g_T^\eta)^s\}$

$ct = \{\mathsf{C} = m \cdot (g_T^\alpha)^z, \mathsf{C}_0 = ek_\sigma \cdot g_1^{z(\mathbf{d_1} + \mathsf{rcv} \mathbf{d_2})}\}$

$$m = \frac{\mathsf{C}}{e(\mathsf{C}_0, k_1 \cdot k_2^{\mathsf{snd}}) \cdot k_3^{-1}}$$

– $\mathsf{Game}_{\mathsf{Real}}$: is the real security game.

Proof of Privacy

IB-ME_mpk, IB-ME_msk

$ek_\sigma = g_1^{\eta \mathbf{d_3} + r(\sigma \mathbf{d_3} - \mathbf{d_4})}$

$dk_\rho = \{k_1 = g_2^{\alpha \mathbf{d}_1^* + s_1(\rho \mathbf{d}_1^* - \mathbf{d}_2^*) + s \mathbf{d}_3^*}, k_2 = g_2^{s_2(\rho \mathbf{d}_1^* - \mathbf{d}_2^*) + s \mathbf{d}_4^*}, k_3 = (g_T^\eta)^s\}$

$ct = \{\mathsf{C} = m \cdot (g_T^\alpha)^z, \mathsf{C}_0 = ek_\sigma \cdot g_1^{z(\mathbf{d_1} + \mathsf{rcv} \mathbf{d_2})}\}$

$$m = \frac{\mathsf{C}}{e(\mathsf{C}_0, k_1 \cdot k_2^{\mathsf{snd}}) \cdot k_3^{-1}}$$

- $\mathsf{Game}_{\mathsf{Real}}$: is the real security game.
- Game_0: is the same as $\mathsf{Game}_{\mathsf{Real}}$ except that the challenge ciphertext is semi-functional.

Proof of Privacy

IB-ME_mpk, IB-ME_msk

$ek_\sigma = g_1^{\eta \mathbf{d_3} + r(\sigma \mathbf{d_3} - \mathbf{d_4})}$

$dk_\rho = \{k_1 = g_2^{\alpha \mathbf{d_1^*} + s_1(\rho \mathbf{d_1^*} - \mathbf{d_2^*}) + s \mathbf{d_3^*}}, k_2 = g_2^{s_2(\rho \mathbf{d_1^*} - \mathbf{d_2^*}) + s \mathbf{d_4^*}}, k_3 = (g_T^\eta)^s\}$

$ct = \{\mathsf{C} = m \cdot (g_T^\alpha)^z, \mathsf{C}_0 = ek_\sigma \cdot g_1^{z(\mathbf{d_1} + \mathsf{rcv} \mathbf{d_2})}\}$

$$m = \frac{\mathsf{C}}{e(\mathsf{C}_0, k_1 \cdot k_2^{\mathsf{snd}}) \cdot k_3^{-1}}$$

- $\mathsf{Game}_{\mathsf{Real}}$: is the real security game.
- Game_0: is the same as $\mathsf{Game}_{\mathsf{Real}}$ except that the challenge ciphertext is semi-functional.
- $\mathsf{Game}_{\kappa,1}$: for κ from 1 to ν, $\mathsf{Game}_{\kappa,1}$ is the same as Game_0 except that the first κ-1 keys are semi-functional, the κ-th key is inter-semi-functional and the remaining keys are normal.

Proof of Privacy

IB-ME_mpk, IB-ME_msk

$ek_\sigma = g_1^{\eta \mathbf{d_3} + r(\sigma \mathbf{d_3} - \mathbf{d_4})}$

$dk_\rho = \{k_1 = g_2^{\alpha \mathbf{d_1^*} + s_1(\rho \mathbf{d_1^*} - \mathbf{d_2^*}) + s \mathbf{d_3^*}}, k_2 = g_2^{s_2(\rho \mathbf{d_1^*} - \mathbf{d_2^*}) + s \mathbf{d_4^*}}, k_3 = (g_T^\eta)^s\}$

$ct = \{\mathsf{C} = m \cdot (g_T^\alpha)^z, \mathsf{C}_0 = ek_\sigma \cdot g_1^{z(\mathbf{d_1} + \mathsf{rcv} \mathbf{d_2})}\}$

$$m = \frac{\mathsf{C}}{e(\mathsf{C}_0, k_1 \cdot k_2^{\mathsf{snd}}) \cdot k_3^{-1}}$$

- $\mathsf{Game}_{\mathsf{Real}}$: is the real security game.
- Game_0: is the same as $\mathsf{Game}_{\mathsf{Real}}$ except that the challenge ciphertext is semi-functional.
- $\mathsf{Game}_{\kappa,1}$: for κ from 1 to ν, $\mathsf{Game}_{\kappa,1}$ is the same as Game_0 except that the first κ-1 keys are semi-functional, the κ-th key is inter-semi-functional and the remaining keys are normal.
- $\mathsf{Game}_{\kappa,2}$: for κ from 1 to ν, $\mathsf{Game}_{\kappa,2}$ is the same as Game_0 except that the first κ keys are semi-functional and the remaining keys are normal.

Proof of Privacy

IB-ME_mpk, IB-ME_msk

$$ek_\sigma = g_1^{\eta \mathbf{d_3} + r(\sigma \mathbf{d_3} - \mathbf{d_4})}$$

$$dk_\rho = \{k_1 = g_2^{\alpha \mathbf{d_1^*} + s_1(\rho \mathbf{d_1^*} - \mathbf{d_2^*}) + s \mathbf{d_3^*}}, k_2 = g_2^{s_2(\rho \mathbf{d_1^*} - \mathbf{d_2^*}) + s \mathbf{d_4^*}}, k_3 = (g_T^\eta)^s\}$$

$$ct = \{\mathsf{C} = m \cdot (g_T^\alpha)^z, \mathsf{C}_0 = ek_\sigma \cdot g_1^{z(\mathbf{d_1} + \mathsf{rcv} \mathbf{d_2})}\}$$

$$m = \frac{\mathsf{C}}{e(\mathsf{C}_0, k_1 \cdot k_2^{\mathsf{snd}}) \cdot k_3^{-1}}$$

- $\mathsf{Game}_{\mathsf{Real}}$: is the real security game.
- Game_0: is the same as $\mathsf{Game}_{\mathsf{Real}}$ except that the challenge ciphertext is semi-functional.
- $\mathsf{Game}_{\kappa,1}$: for κ from 1 to ν, $\mathsf{Game}_{\kappa,1}$ is the same as Game_0 except that the first κ-1 keys are semi-functional, the κ-th key is inter-semi-functional and the remaining keys are normal.
- $\mathsf{Game}_{\kappa,2}$: for κ from 1 to ν, $\mathsf{Game}_{\kappa,2}$ is the same as Game_0 except that the first κ keys are semi-functional and the remaining keys are normal.
- $\mathsf{Game}_{\mathsf{Final}}$: is the same as $\mathsf{Game}_{\nu,2}$, except that the challenge ciphertext is a semi-functional encryption of a random message in G_T and under two random identities in $\mathbb{Z}_q$. We denote the challenge ciphertext in $\mathsf{Game}_{\mathsf{Final}}$ as $\mathsf{CT}^{(\mathsf{R})}_{ek_{\sigma_\mathsf{R}}, \mathsf{rcv}_\mathsf{R}}$.

Proof of Authenticity

$\mathbf{G}^{\text{ib-priv}}_{\Pi,\mathsf{A}}(\lambda)$ **Privacy**

$(\mathsf{mpk}, \mathsf{msk}) \leftarrow\!\!\$\ \mathsf{Setup}(1^\lambda)$

$(m_0, m_1, \mathsf{rcv}_0, \mathsf{rcv}_1, \sigma_0, \sigma_1, \alpha) \leftarrow\!\!\$\ \mathsf{A}_1^{\mathsf{O}_1,\mathsf{O}_2}(1^\lambda, \mathsf{mpk})$

$b \leftarrow\!\!\$\ \{0,1\}$

$\mathsf{ek}_{\sigma_b} \leftarrow\!\!\$\ \mathsf{SKGen}(\mathsf{msk}, \sigma_b)$

$c \leftarrow\!\!\$\ \mathsf{Enc}(\mathsf{ek}_{\sigma_b}, \mathsf{rcv}_b, m_b)$

$b' \leftarrow\!\!\$\ \mathsf{A}_2^{\mathsf{O}_1,\mathsf{O}_2}(1^\lambda, c, \alpha)$

If $(b' = b)$ **return** 1

Else **return** 0

$\mathbf{G}^{\text{ib-auth}}_{\Pi,\mathsf{A}}(\lambda)$ **Authenticity**

$(\mathsf{mpk}, \mathsf{msk}) \leftarrow\!\!\$\ \mathsf{Setup}(1^\lambda)$

$(c, \rho, \mathsf{snd}) \leftarrow\!\!\$\ \mathsf{A}^{\mathsf{O}_1,\mathsf{O}_2}(1^\lambda, \mathsf{mpk})$

$\mathsf{dk}_\rho \leftarrow\!\!\$\ \mathsf{RKGen}(\mathsf{msk}, \rho)$

$m = \mathsf{Dec}(\mathsf{dk}_\rho, \mathsf{snd}, c)$

If $\forall \sigma \in \mathcal{Q}_{\mathsf{O}_1} : (\sigma \neq \mathsf{snd}) \wedge (m \neq \perp)$

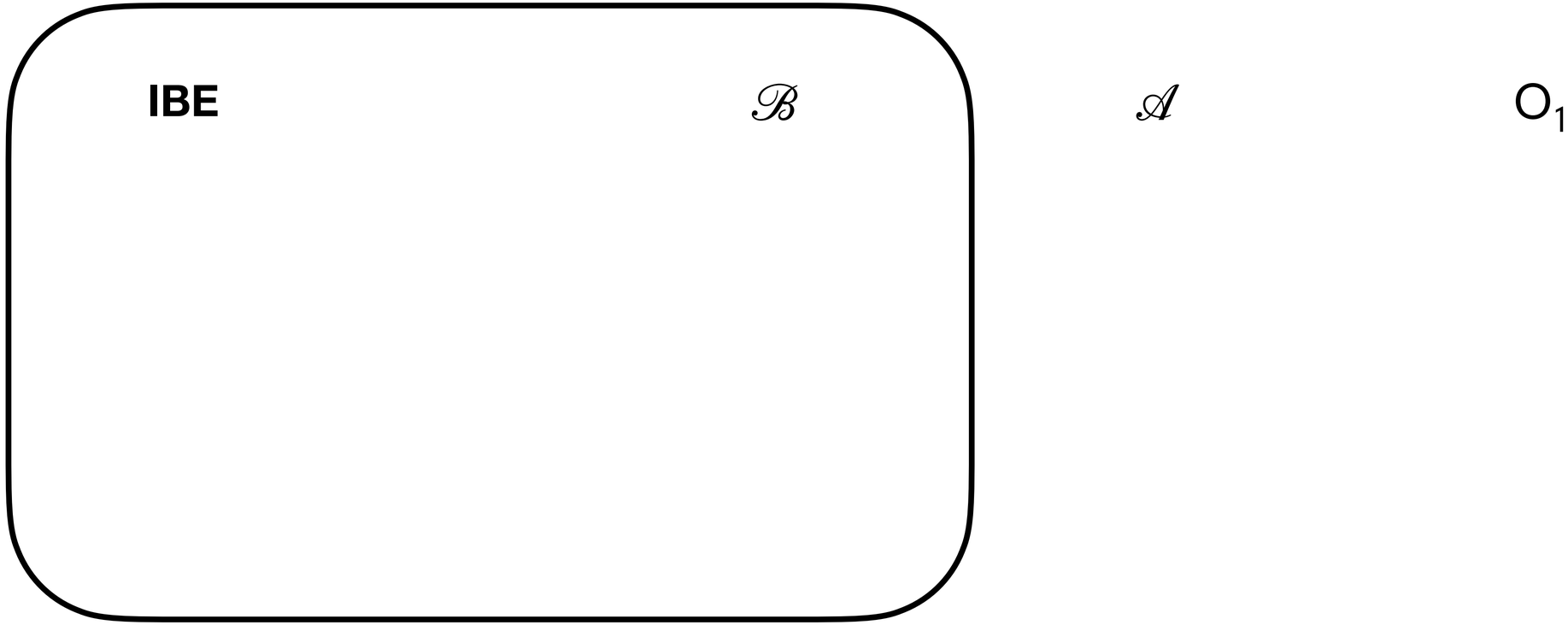
  return 1

Else **return** 0

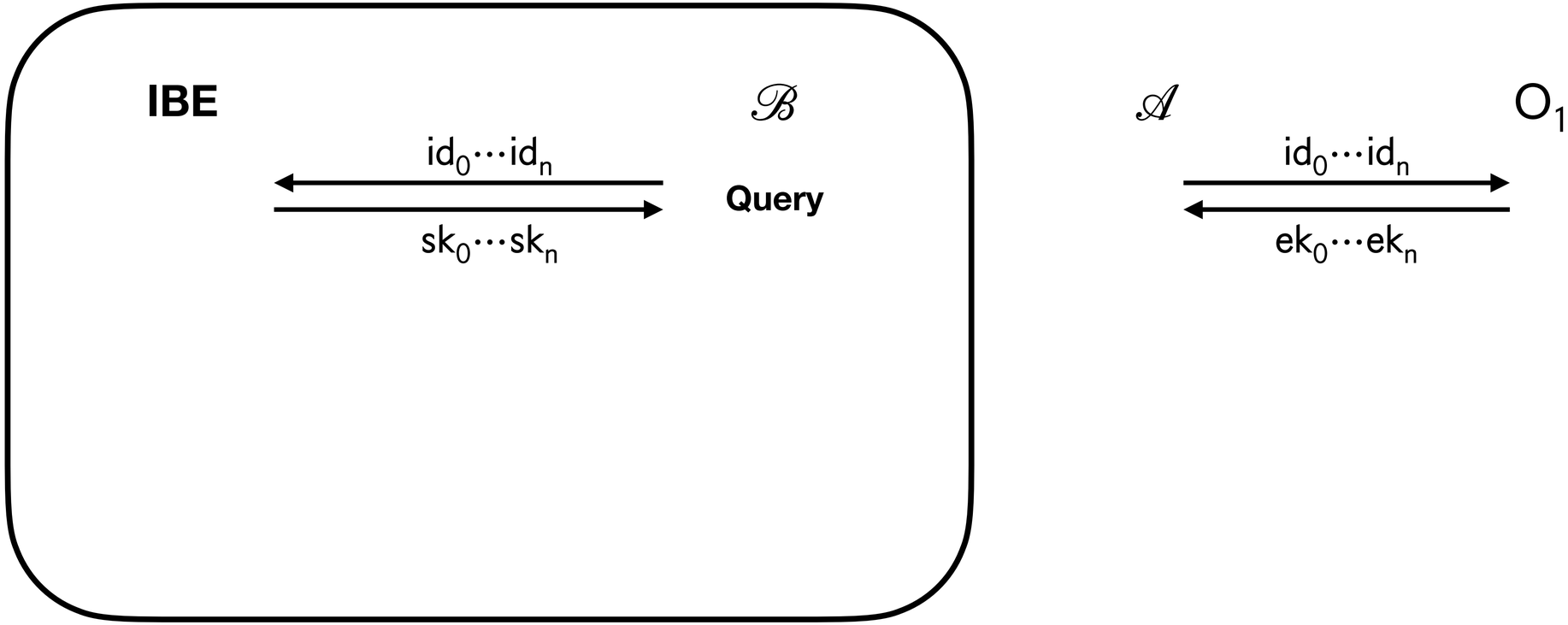
Proof of Authenticity

IBE $\mathscr{B}$ $\mathscr{A}$

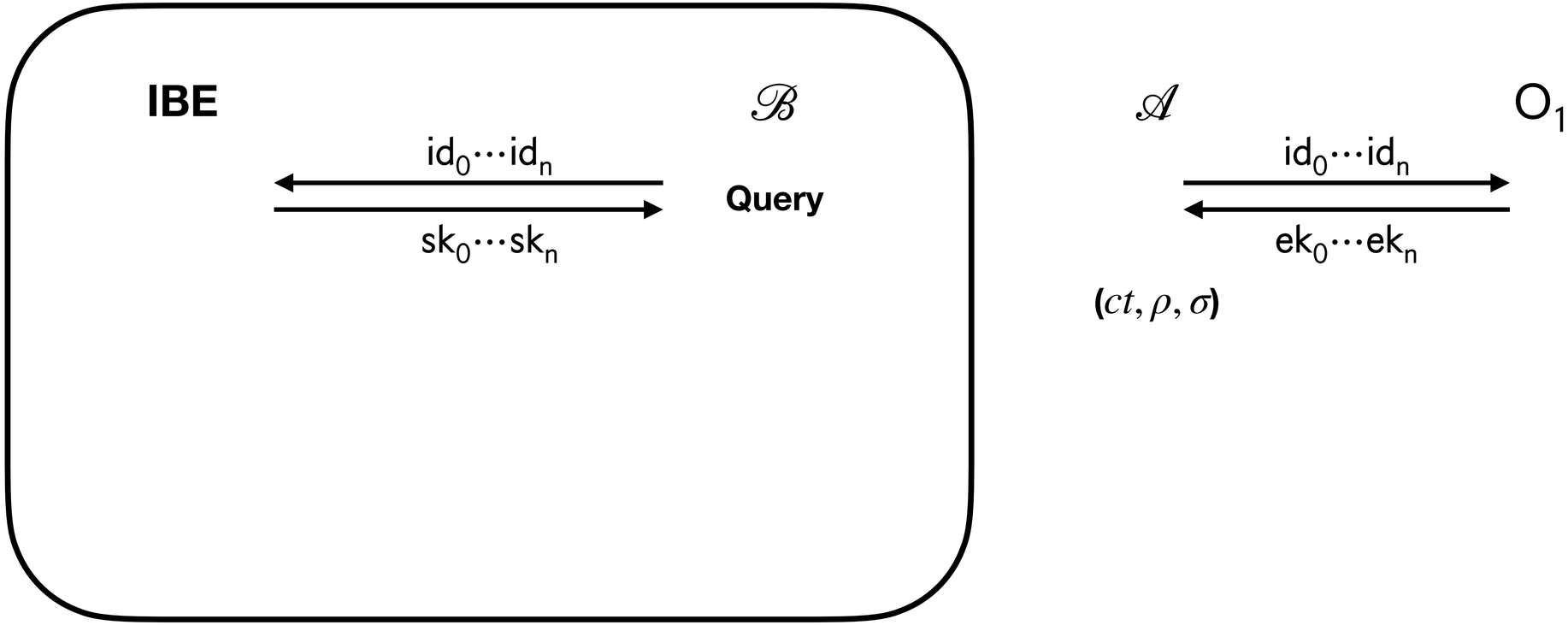
Proof of Authenticity



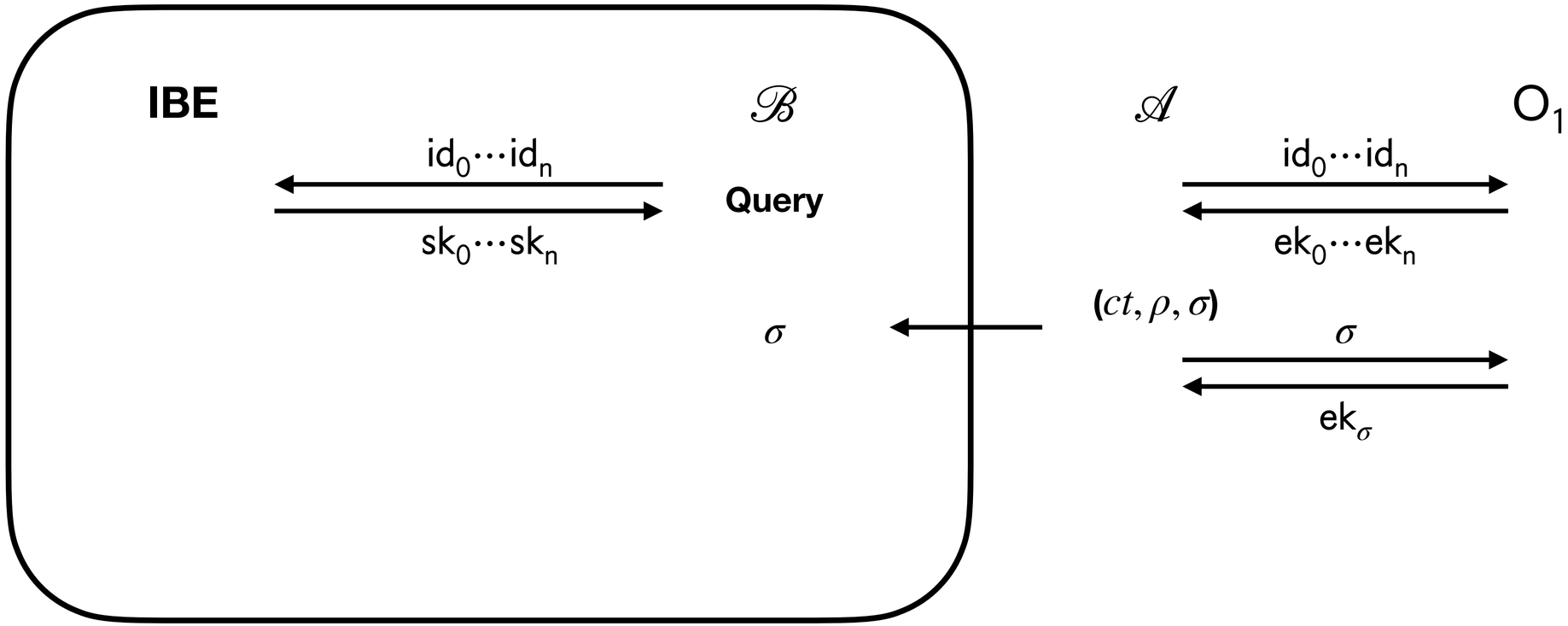
Proof of Authenticity



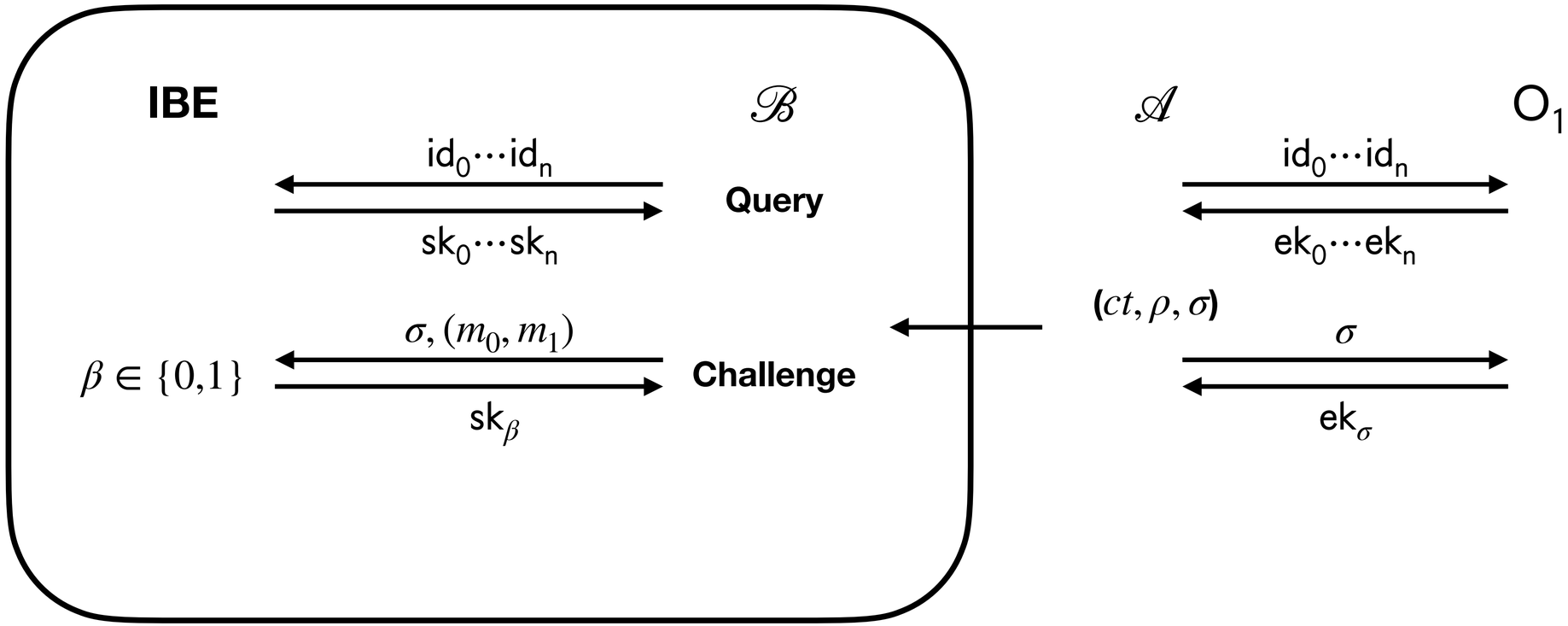
Proof of Authenticity



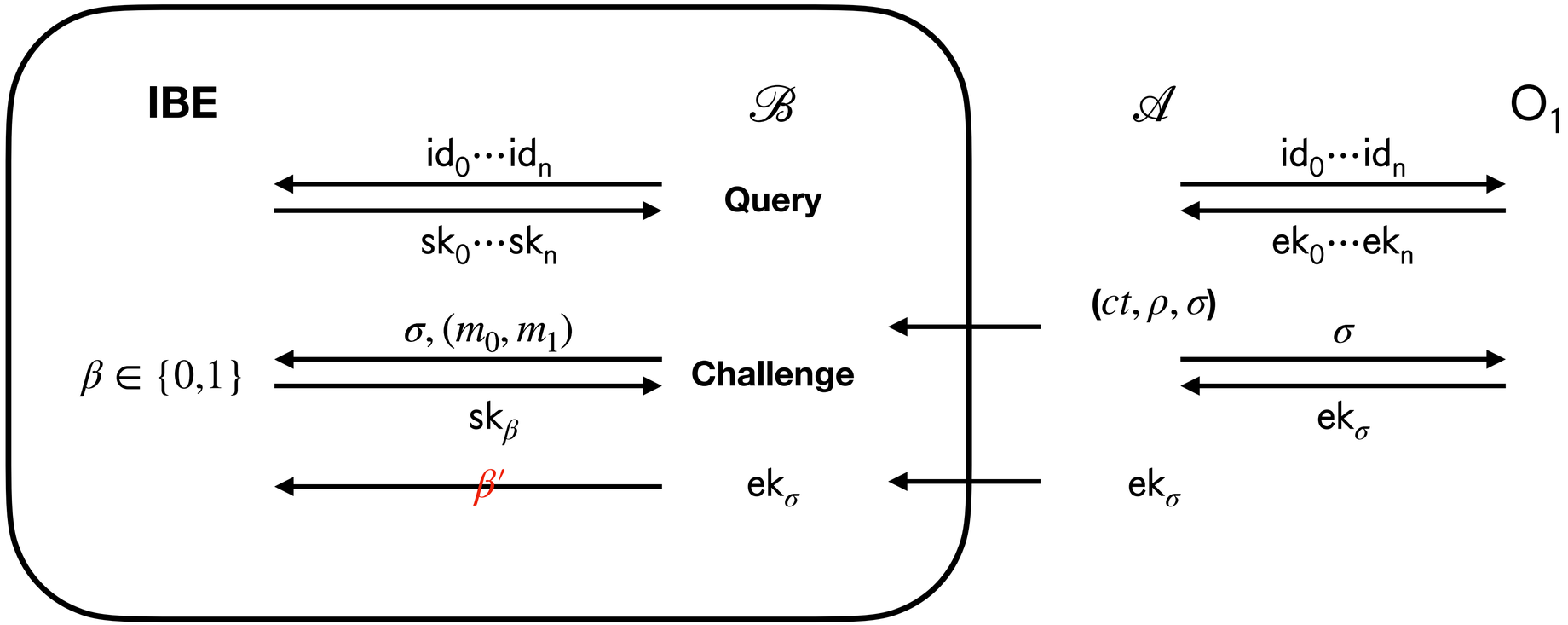
Proof of Authenticity



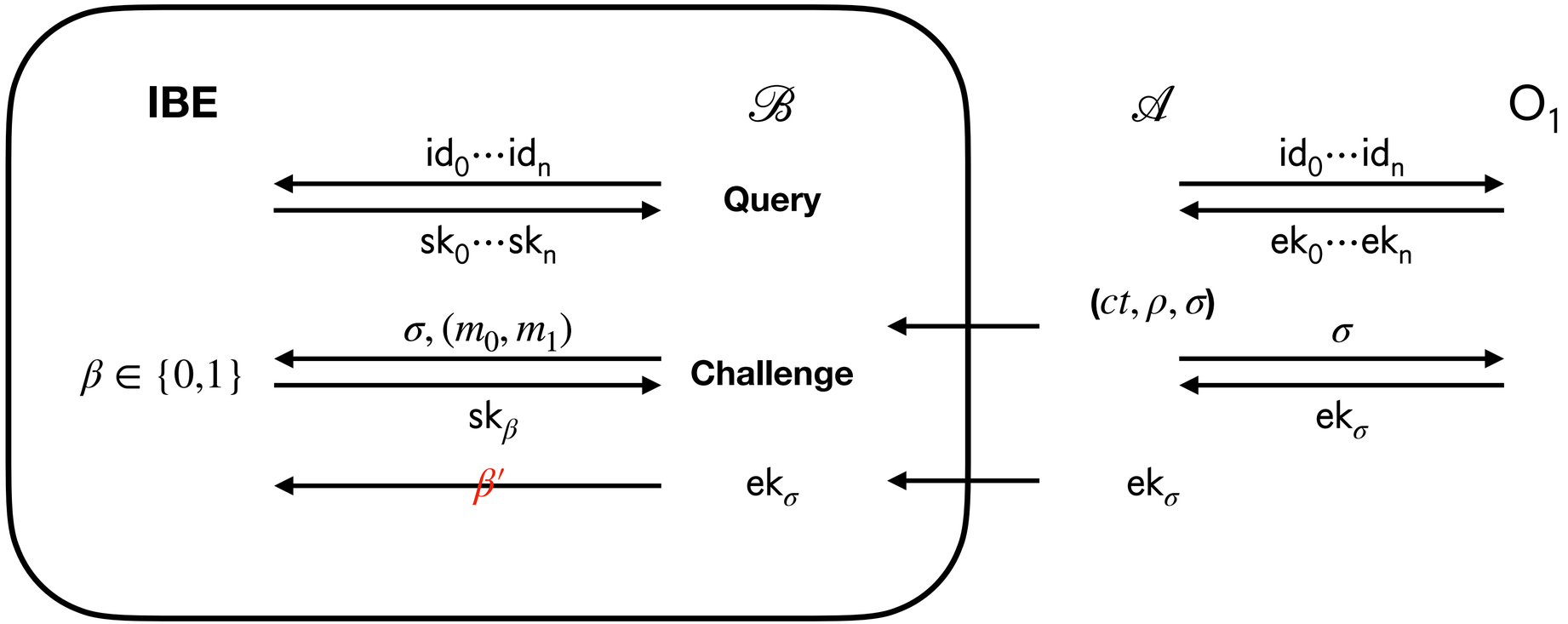
Proof of Authenticity



Proof of Authenticity

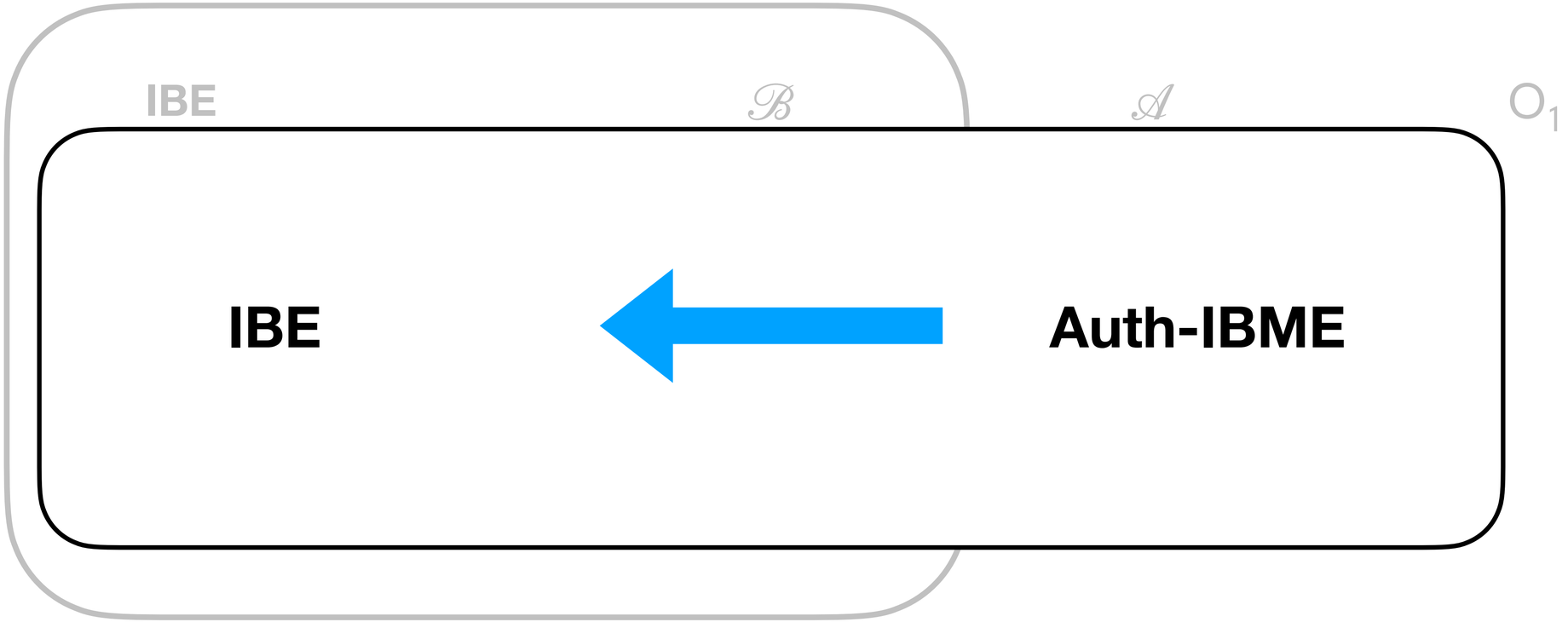


Proof of Authenticity



$$\mathsf{Adv}^{\mathsf{IBE}}_{\mathscr{B}}(\lambda) \geq \mathsf{Adv}^{\mathsf{Game_{ib\text{-}auth}}}_{\mathscr{A}}(\lambda)$$

Proof of Authenticity



$$\mathsf{Adv}^{\mathsf{IBE}}_{\mathscr{B}}(\lambda) \geq \mathsf{Adv}^{\mathsf{Game}_{\mathsf{ib}\text{-}\mathsf{auth}}}_{\mathscr{A}}(\lambda)$$

Summary

IB-ME from SXDH

1. A variant of two-level anonymous IBE,

Summary

IB-ME from SXDH

1. A variant of two-level anonymous IBE,

2. Dual pairing vector spaces, Dual system encryption,

Summary

IB-ME from SXDH

1. A variant of two-level anonymous IBE,
2. Dual pairing vector spaces, Dual system encryption,
3. Efficiency improvement; Practical extensions; Lattice-based realization.

Thank you for your attention!

https://eprint.iacr.org/2022/1246

Any question?