# Possibility and Impossibility Results for Receiver Selective Opening Secure PKE in the Multi-Challenge Setting


**Rupeng Yang**
University of Hong Kong

Junzuo Lai
Jinan University

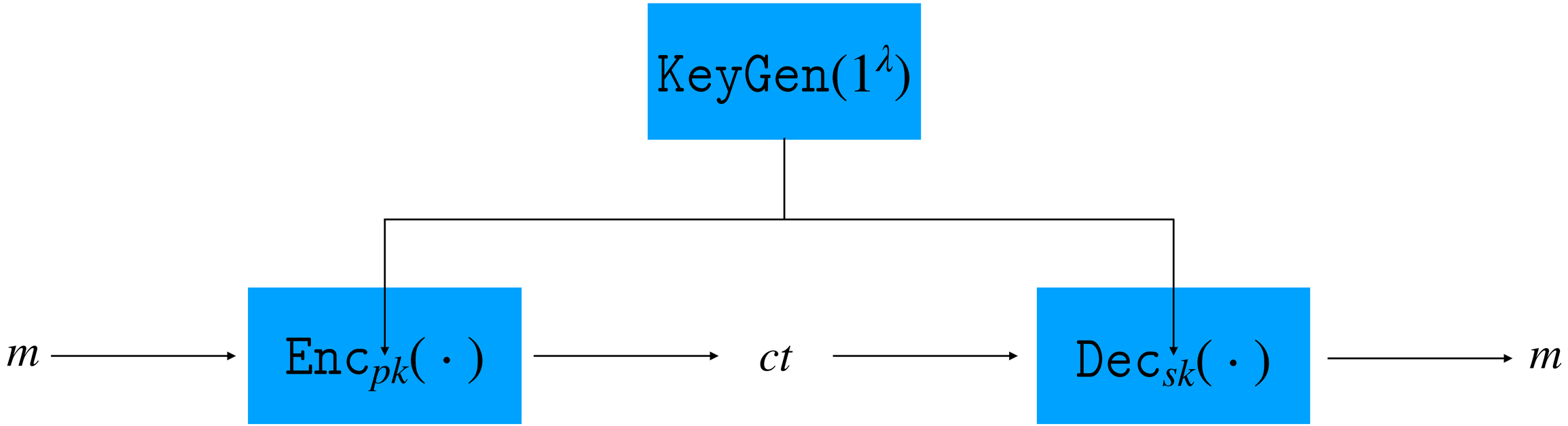
Zhengan Huang
Peng Cheng Laboratory

Man Ho Au
University of Hong Kong

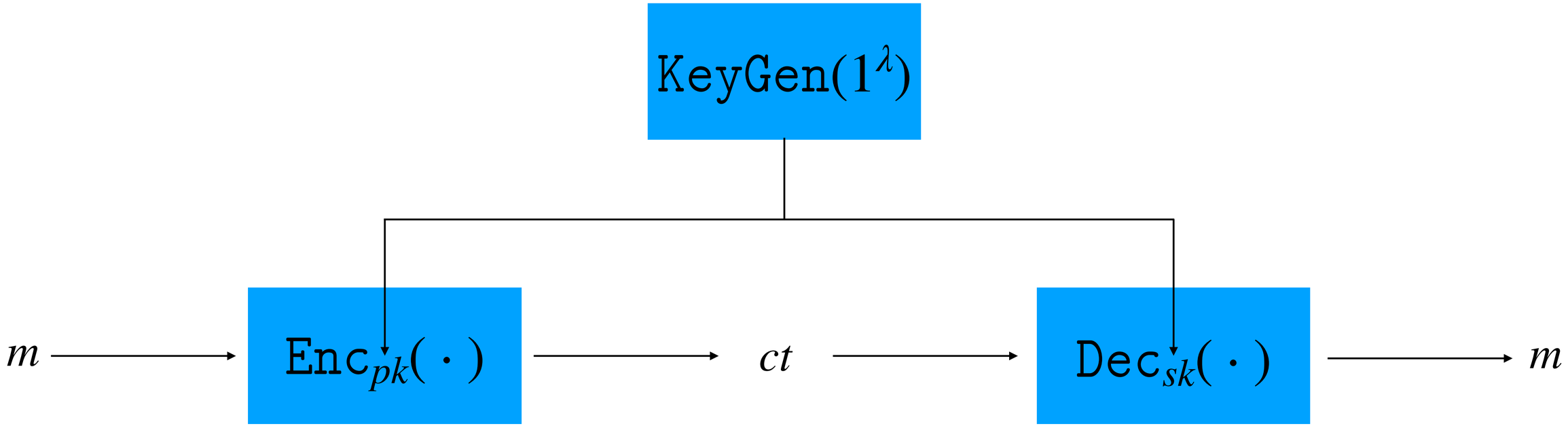
Qiuliang Xu
Shandong University

Willy Susilo
University of Wollongong

# PKE with RSO Security in the Multi-Challenge Setting



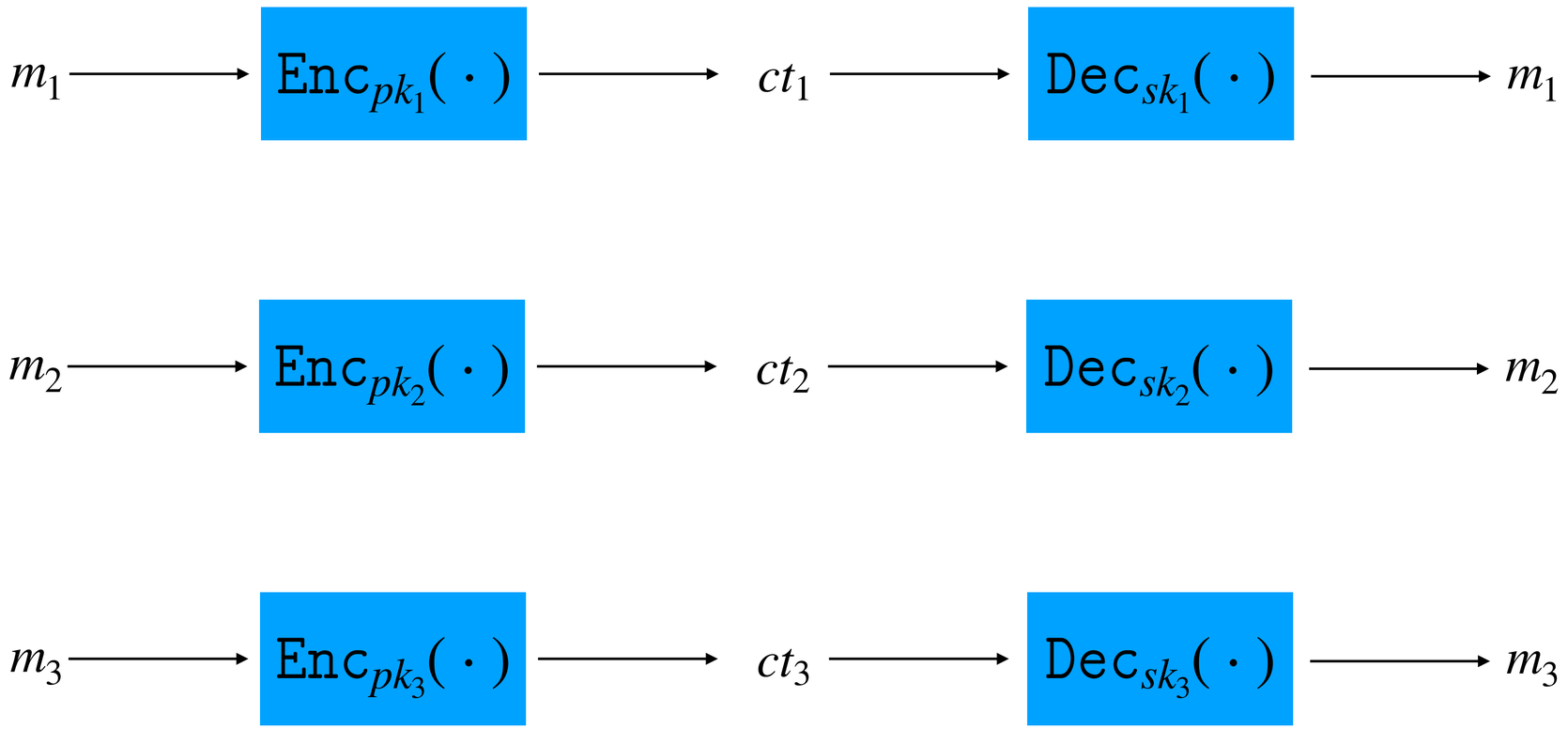
# PKE with RSO Security in the Multi-Challenge Setting




**Correctness:** $\mathtt{Dec}_{sk}(\mathtt{Enc}_{pk}(m)) = m$

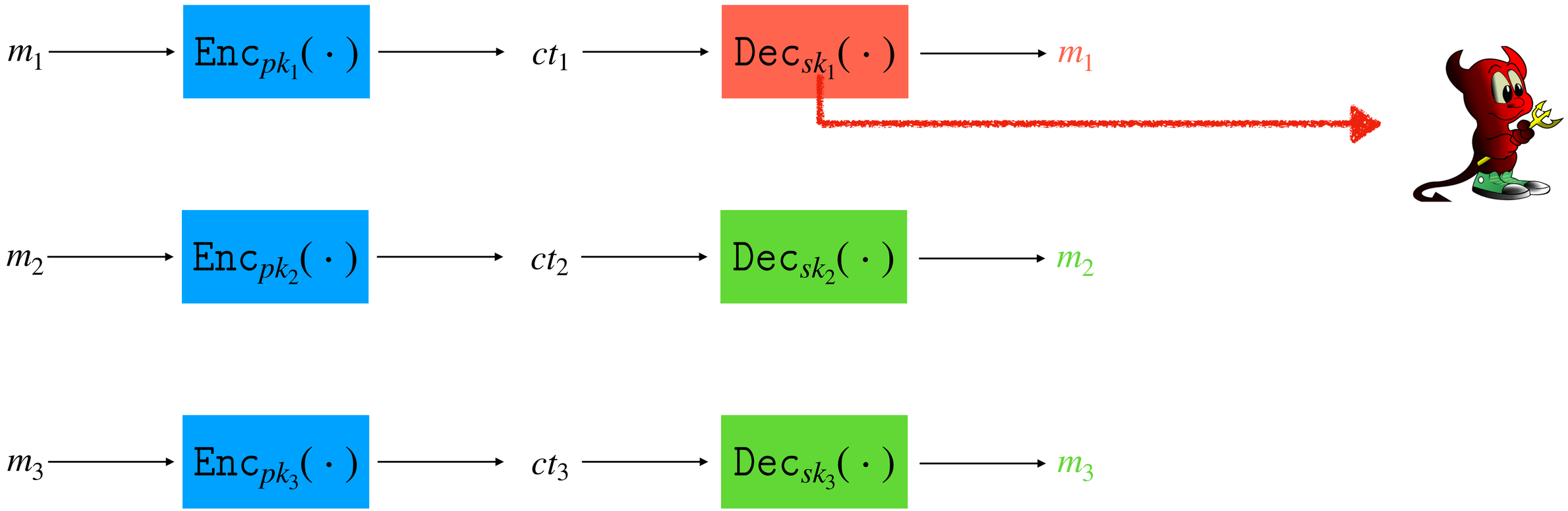
**Semantic Security:** $\mathcal{A}(pk, ct) \approx \mathcal{S}(1^\lambda)$

# PKE with RSO Security in the Multi-Challenge Setting



# PKE with RSO Security

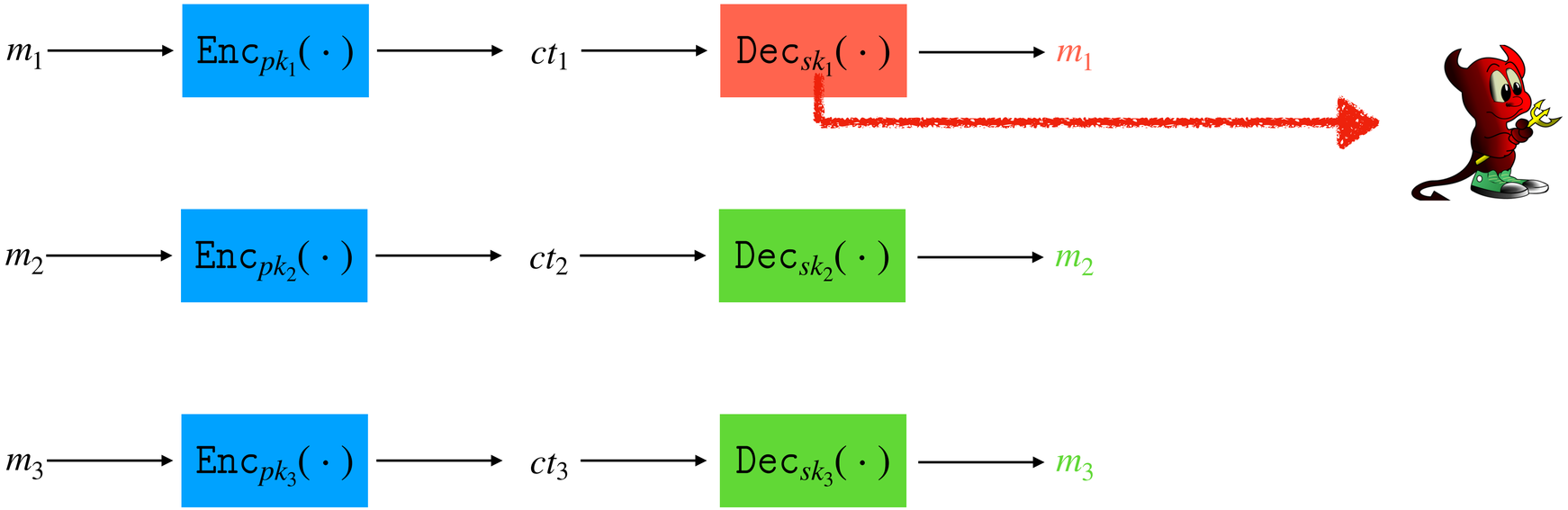
## in the Multi-Challenge Setting




**RSO = Receiver Selective Opening**

# PKE with RSO Security

## in the Multi-Challenge Setting

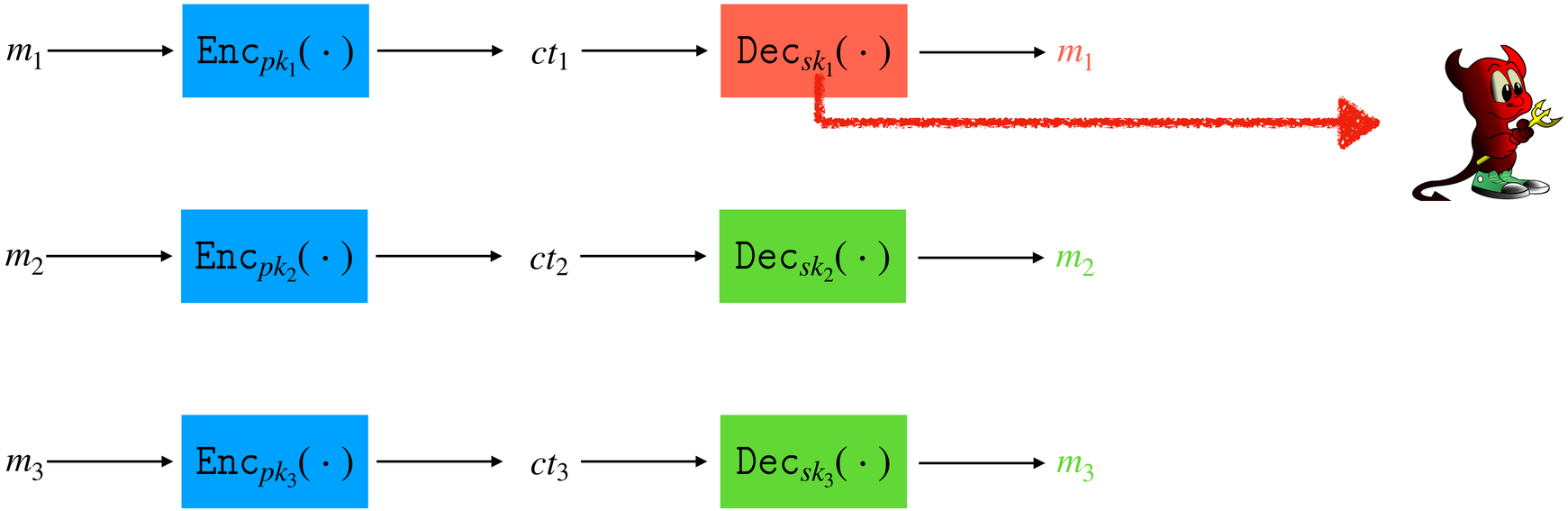





$$\mathscr{M} \leftarrow \mathscr{A}(pk_1, \ldots, pk_n)$$
$$(m_1, \ldots, m_n) \leftarrow \mathscr{M}$$
$$ct_i \leftarrow Enc_{pk_i}(m_i)$$
$$\mathtt{I} \leftarrow \mathscr{A}(ct_1, \ldots, ct_n)$$
$$out \leftarrow \mathscr{A}((sk_i, m_i)_{i \in \mathtt{I}})$$
$$(\mathscr{M}, \mathtt{I}, out, (m_1, \ldots, m_n))$$

# PKE with RSO Security

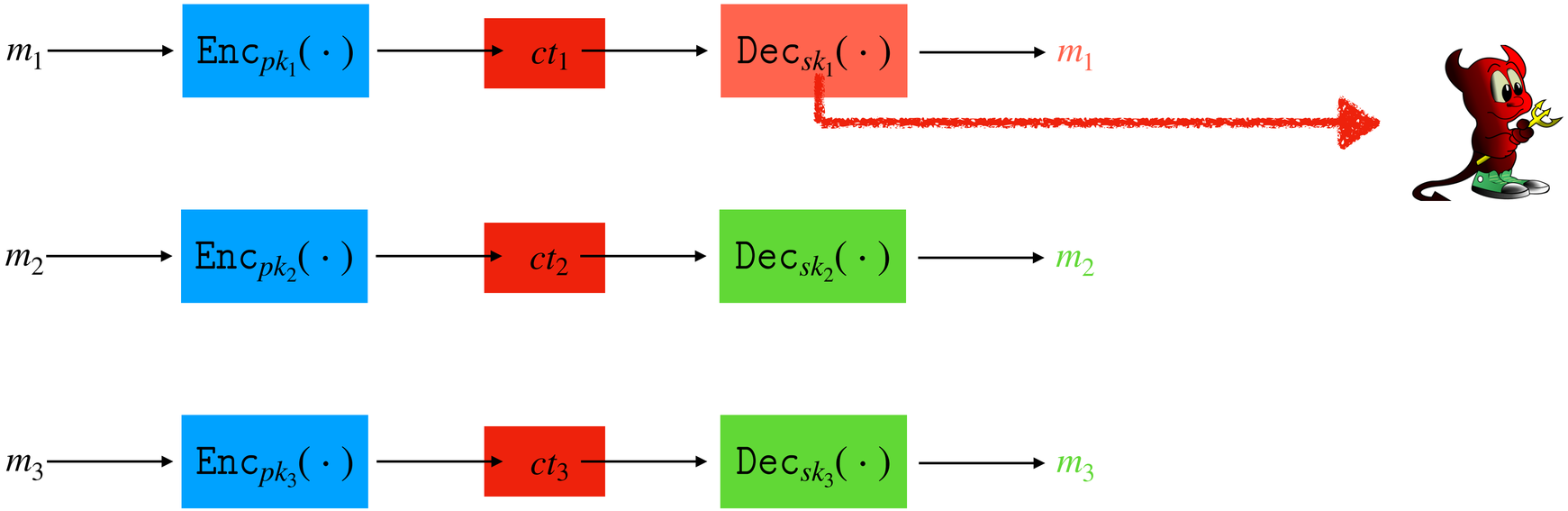
## in the Multi-Challenge Setting




$$
\begin{aligned}
&\mathscr{M} \leftarrow \mathscr{A}(pk_1, \ldots, pk_n) \\
&(m_1, \ldots, m_n) \leftarrow \mathscr{M} \\
&ct_i \leftarrow Enc_{pk_i}(m_i) \\
&\mathtt{I} \leftarrow \mathscr{A}(ct_1, \ldots, ct_n) \\
&out \leftarrow \mathscr{A}((sk_i, m_i)_{i \in \mathtt{I}}) \\
&(\mathscr{M}, \mathtt{I}, out, (m_1, \ldots, m_n))
\end{aligned}
\quad \approx \quad
\begin{aligned}
&\mathscr{M} \leftarrow \mathcal{S}(1^\lambda) \\
&(m_1, \ldots, m_n) \leftarrow \mathscr{M} \\
&\mathtt{I} \leftarrow \mathcal{S}(1^\lambda) \\
&out \leftarrow \mathcal{S}((m_i)_{i \in \mathtt{I}}) \\
&(\mathscr{M}, \mathtt{I}, out, (m_1, \ldots, m_n))
\end{aligned}
$$

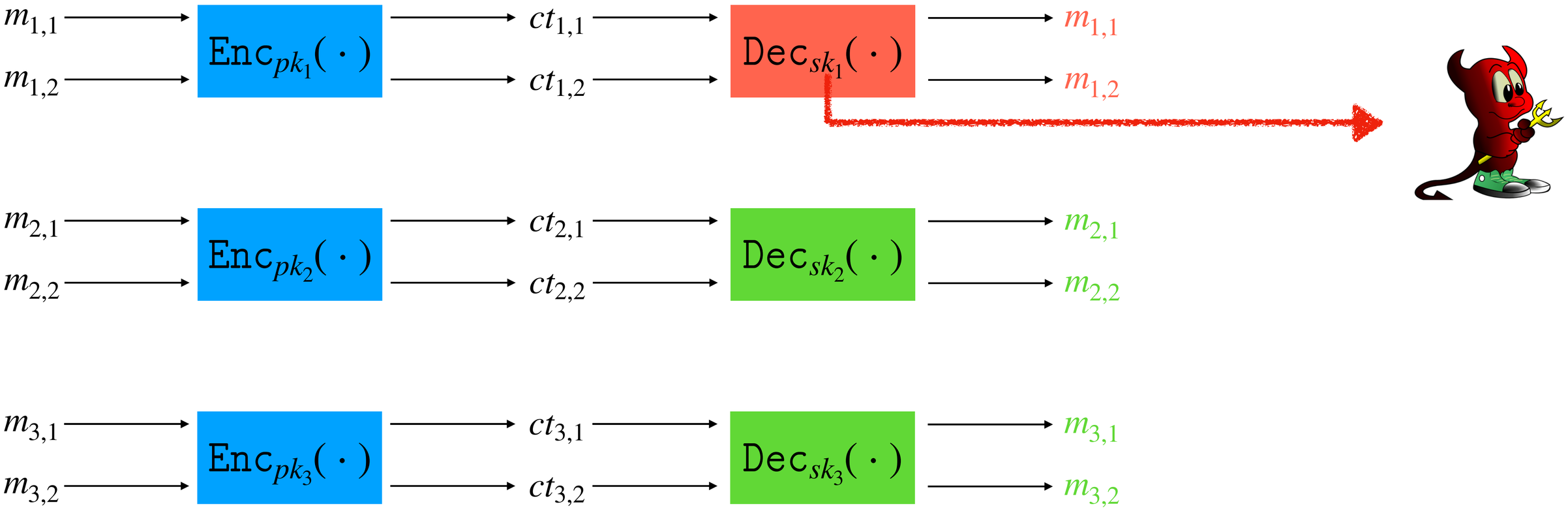
# PKE with RSO Security

## in the Multi-Challenge Setting

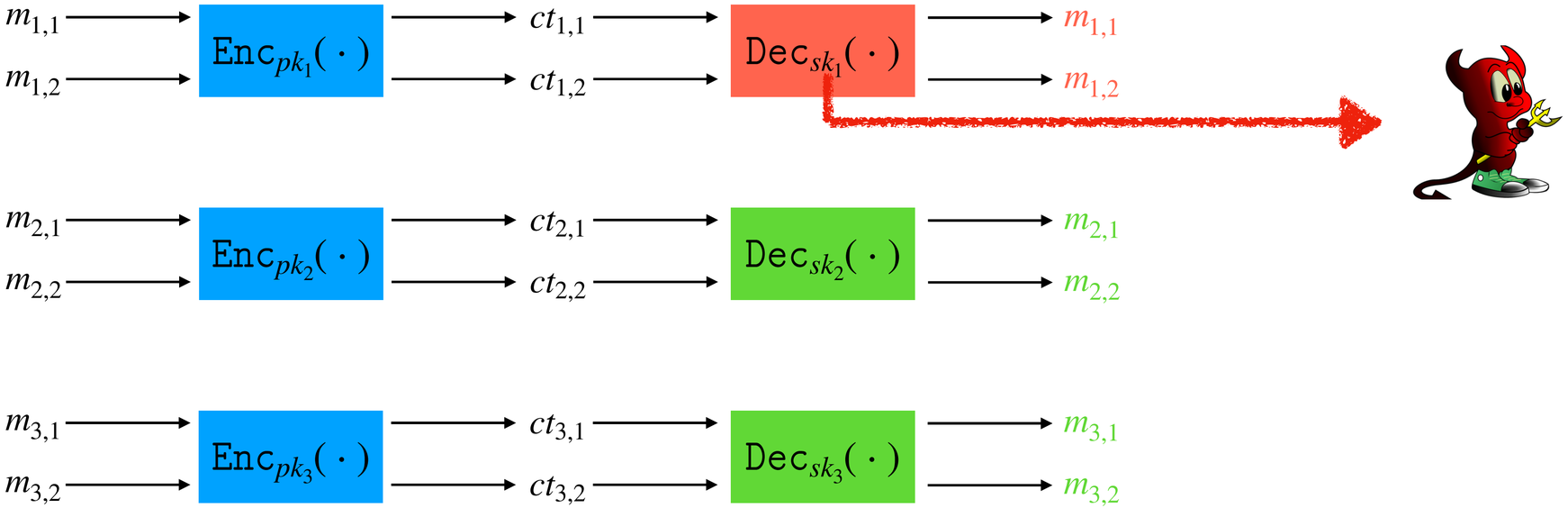



$$
\begin{array}{l}
\mathscr{M} \leftarrow \mathscr{A}(pk_1, \ldots, pk_n) \\
(m_1, \ldots, m_n) \leftarrow \mathscr{M} \\
ct_i \leftarrow Enc_{pk_i}(m_i) \\
\mathtt{I} \leftarrow \mathscr{A}(ct_1, \ldots, ct_n) \\
out \leftarrow \mathscr{A}((sk_i, m_i)_{i \in \mathtt{I}}) \\
(\mathscr{M}, \mathtt{I}, out, (m_1, \ldots, m_n))
\end{array}
\quad \approx \quad
\begin{array}{l}
\mathscr{M} \leftarrow \mathcal{S}(1^\lambda) \\
(m_1, \ldots, m_n) \leftarrow \mathscr{M} \\
\mathtt{I} \leftarrow \mathcal{S}(1^\lambda) \\
out \leftarrow \mathcal{S}((m_i)_{i \in \mathtt{I}}) \\
(\mathscr{M}, \mathtt{I}, out, (m_1, \ldots, m_n))
\end{array}
$$

# PKE with RSO Security in the Multi-Challenge Setting



# PKE with RSO Security in the Multi-Challenge Setting




$$\mathscr{M} \leftarrow \mathscr{A}(pk_1, \ldots, pk_n)$$
$$(m_{i,j})_{i\in[n],j\in[k]} \leftarrow \mathscr{M}$$
$$ct_{i,j} \leftarrow Enc_{pk_i}(m_{i,j})$$
$$\mathtt{I} \leftarrow \mathscr{A}(ct_{1,1}, \ldots, ct_{n,k})$$
$$out \leftarrow \mathscr{A}((sk_i, (m_{i,j})_{j\in[k]})_{i\in\mathtt{I}})$$
$$(\mathscr{M}, \mathtt{I}, out, (m_{i,j})_{i\in[n],j\in[k]})$$

$\approx$

$$\mathscr{M} \leftarrow \mathcal{S}(1^\lambda)$$
$$(m_{i,j})_{i\in[n],j\in[k]} \leftarrow \mathscr{M}$$
$$\mathtt{I} \leftarrow \mathcal{S}(1^\lambda)$$
$$out \leftarrow \mathcal{S}((m_{i,j})_{i\in\mathtt{I},j\in[k]})$$
$$(\mathscr{M}, \mathtt{I}, out, (m_{i,j})_{i\in[n],j\in[k]})$$

# Our Results

- RSO security in the single-challenge setting $\not\Longrightarrow$ RSO security in the multi-challenge setting
- RSO secure PKE in the multi-challenge setting
- Lower bound on secret key length for PKE schemes with RSO security in the $k$-challenge setting
- RSO secure PKE with nearly optimal secret key length

# Our Results

- RSO security in the single-challenge setting $\not\Longrightarrow$ RSO security in the multi-challenge setting ☞
- RSO secure PKE in the multi-challenge setting
- Lower bound on secret key length for PKE schemes with RSO security in the $k$-challenge setting
- RSO secure PKE with nearly optimal secret key length

# The Counterexample

E is a PKE scheme s.t.

1. Each public key has only one valid secret key
2. It is easy to check relation between public key and secret key
3. Perfect correctness

# The Counterexample

E is a PKE scheme s.t.

1. Each public key has only one valid secret key
2. It is easy to check relation between public key and secret key
3. Perfect correctness

Example: ElGamal Encryption

# The Counterexample

$\mathsf{E}$ is a PKE scheme s.t.

1. Each public key has only one valid secret key
2. It is easy to check relation between public key and secret key
3. Perfect correctness

**$\Pi$:**

$\mathtt{KeyGen}(1^\lambda)$ :

$(pk_1, sk_1) \leftarrow \mathsf{E}.\mathtt{KeyGen}(1^\lambda)$

$(pk_2, sk_2) \leftarrow \mathsf{E}.\mathtt{KeyGen}(1^\lambda)$

$s \leftarrow \{1,2\}$

$SK = (s, sk_s)$

$PK = (pk_1, pk_2)$

# The Counterexample

$\mathsf{E}$ is a PKE scheme s.t.

1. Each public key has only one valid secret key
2. It is easy to check relation between public key and secret key
3. Perfect correctness

**$\Pi$:**

$\mathtt{KeyGen}(1^\lambda)$ :
$(pk_1, sk_1) \leftarrow \mathsf{E}.\mathtt{KeyGen}(1^\lambda)$
$(pk_2, sk_2) \leftarrow \mathsf{E}.\mathtt{KeyGen}(1^\lambda)$
$s \leftarrow \{1,2\}$
$SK = (s, sk_s)$
$PK = (pk_1, pk_2)$

$\mathtt{Enc}(PK = (pk_1, pk_2), m \in \{0,1\})$ :
$ct_1 \leftarrow \mathsf{E}.\mathtt{Enc}(pk_1, m)$
$ct_2 \leftarrow \mathsf{E}.\mathtt{Enc}(pk_2, m)$
$CT = (ct_1, ct_2)$

# The Counterexample

$\mathsf{E}$ is a PKE scheme s.t.

1. Each public key has only one valid secret key
2. It is easy to check relation between public key and secret key
3. Perfect correctness

**$\Pi$:**

$\mathtt{KeyGen}(1^\lambda)$ :
$(pk_1, sk_1) \leftarrow \mathsf{E}.\mathtt{KeyGen}(1^\lambda)$
$(pk_2, sk_2) \leftarrow \mathsf{E}.\mathtt{KeyGen}(1^\lambda)$
$s \leftarrow \{1,2\}$
$SK = (s, sk_s)$
$PK = (pk_1, pk_2)$

$\mathtt{Enc}(PK = (pk_1, pk_2), m \in \{0,1\})$ :
$ct_1 \leftarrow \mathsf{E}.\mathtt{Enc}(pk_1, m)$
$ct_2 \leftarrow \mathsf{E}.\mathtt{Enc}(pk_2, m)$
$CT = (ct_1, ct_2)$

$\mathtt{Dec}(SK = (s, sk_s), CT = (ct_1, ct_2))$ :
$m \leftarrow \mathsf{E}.\mathtt{Dec}(sk_s, ct_s)$

# Security in the Single-Challenge Setting

$PK_1, \ldots, PK_n$

$\mathscr{M}$

$(m_1, \ldots, m_n) \leftarrow \mathscr{M}$

$CT_i \leftarrow Enc_{PK_i}(m_i)$

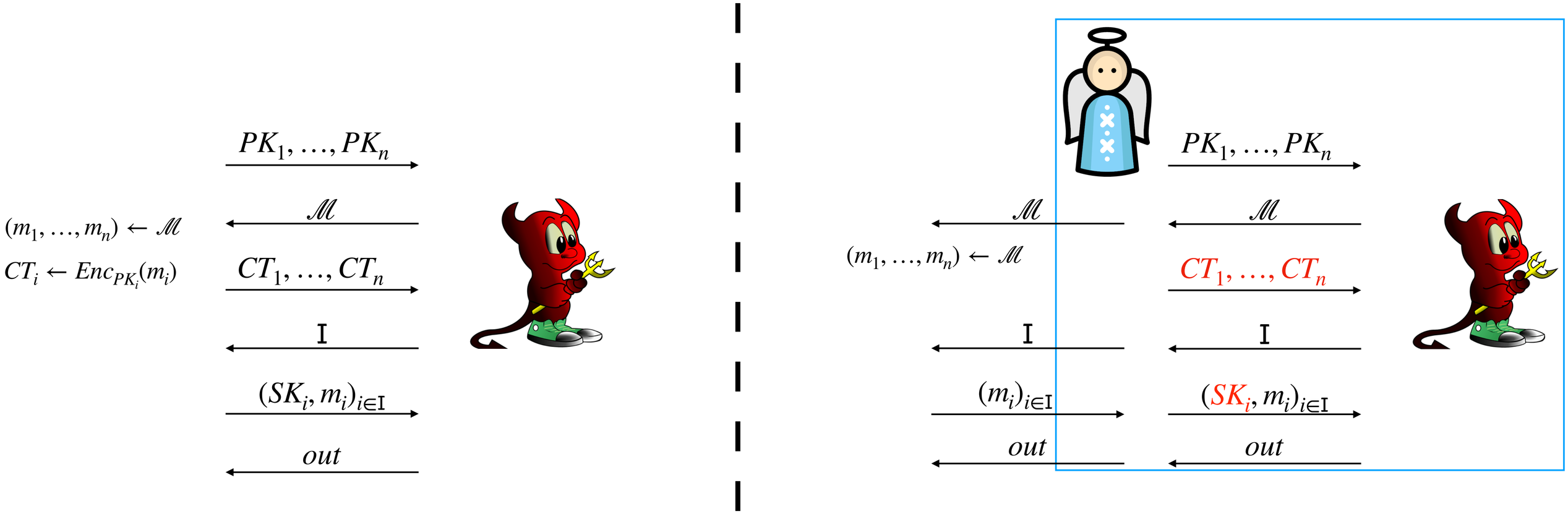
$CT_1, \ldots, CT_n$

$\mathtt{I}$

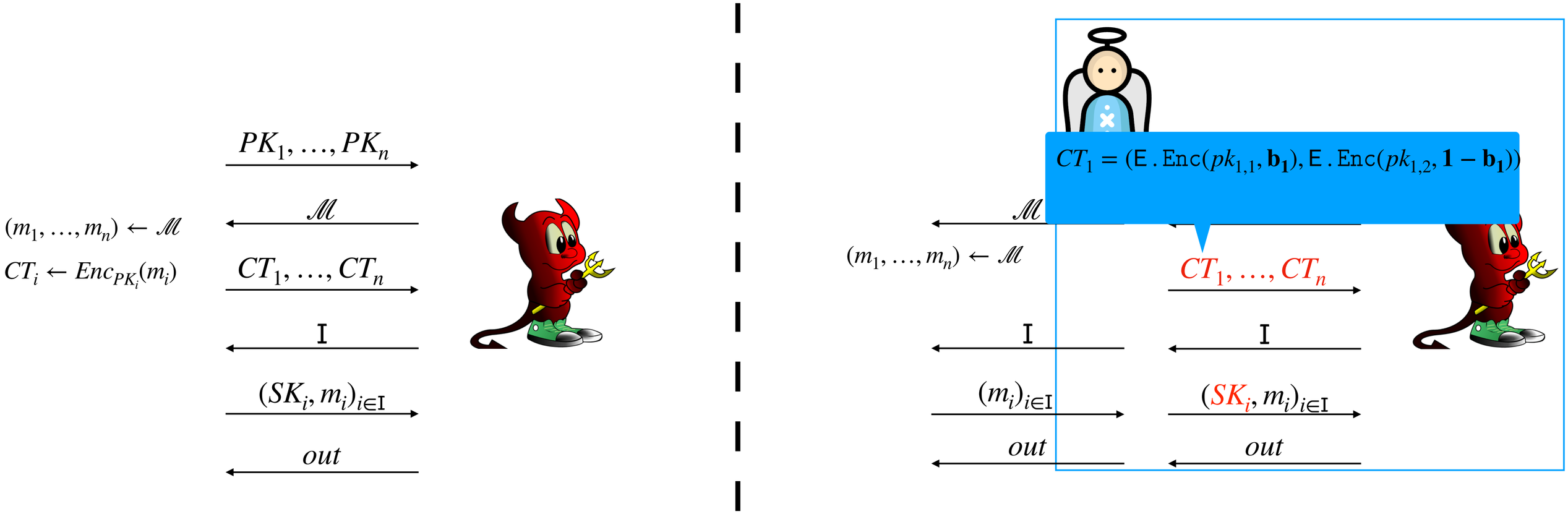
$(SK_i, m_i)_{i \in \mathtt{I}}$

$out$

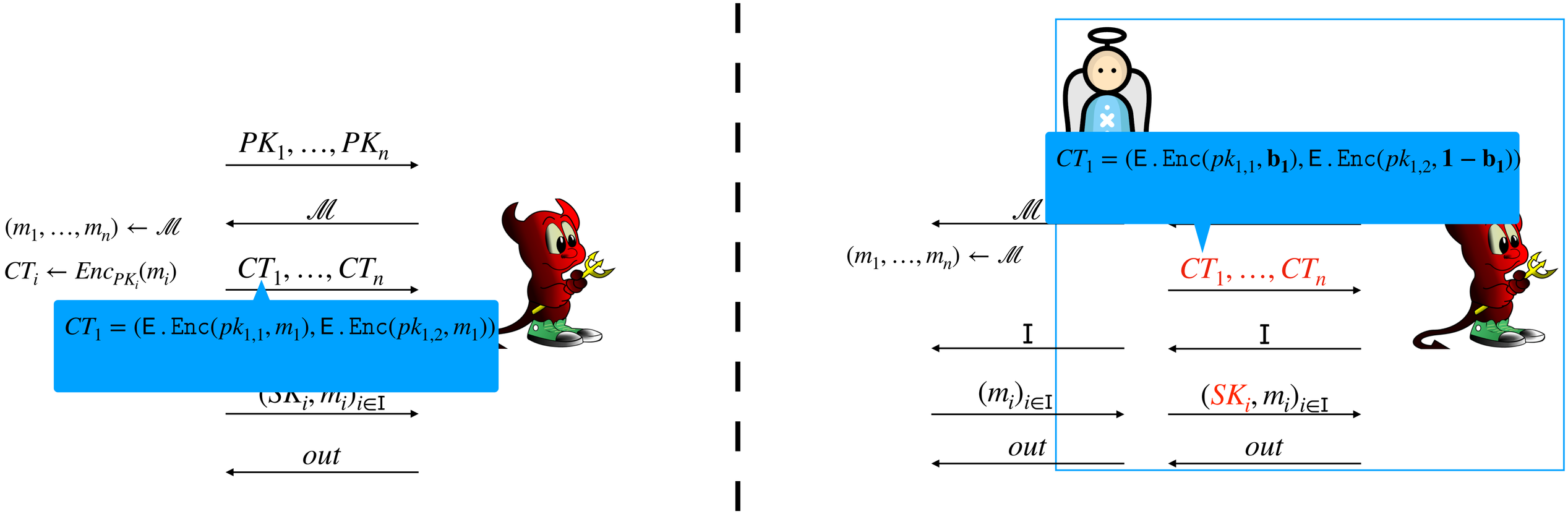
# Security in the Single-Challenge Setting



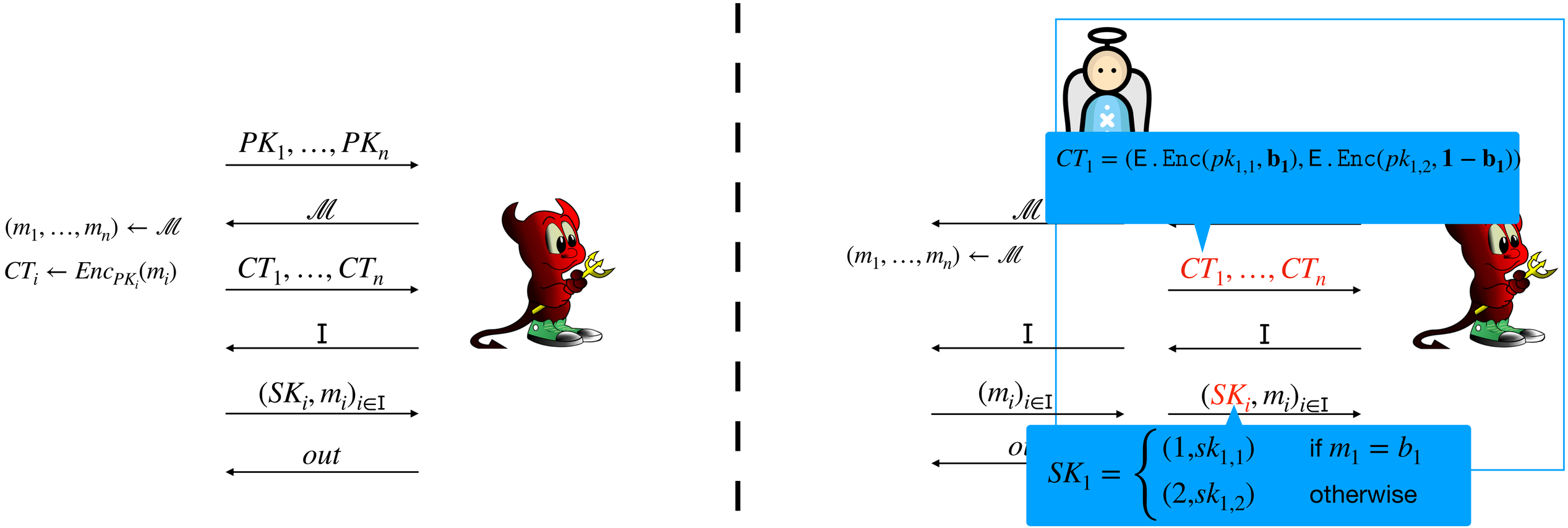
# Security in the Single-Challenge Setting



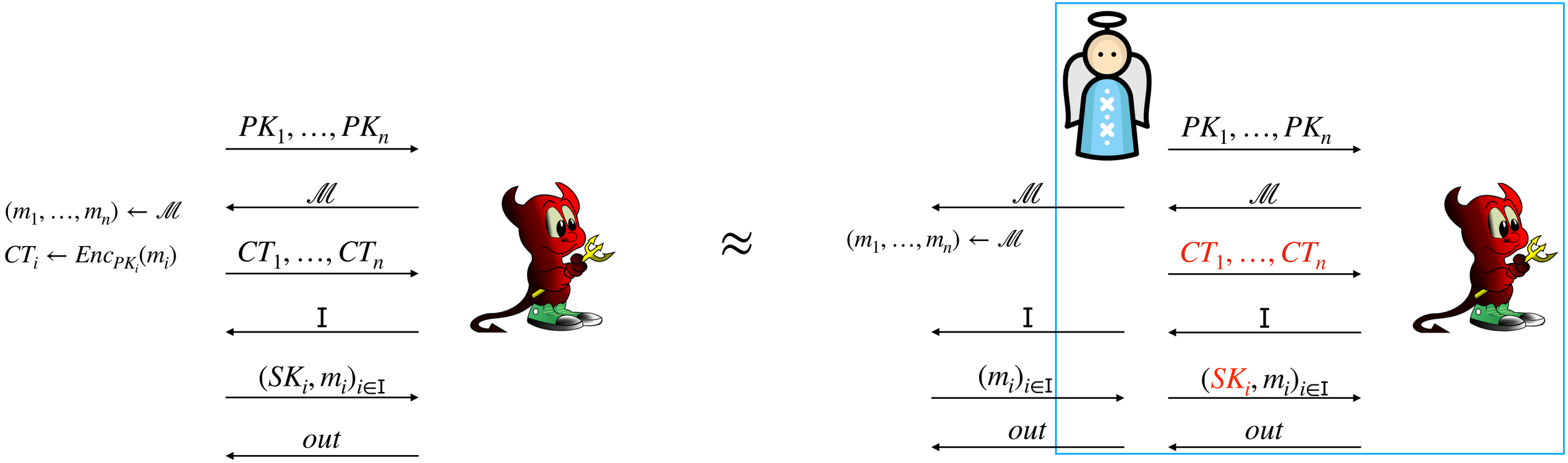
# Security in the Single-Challenge Setting



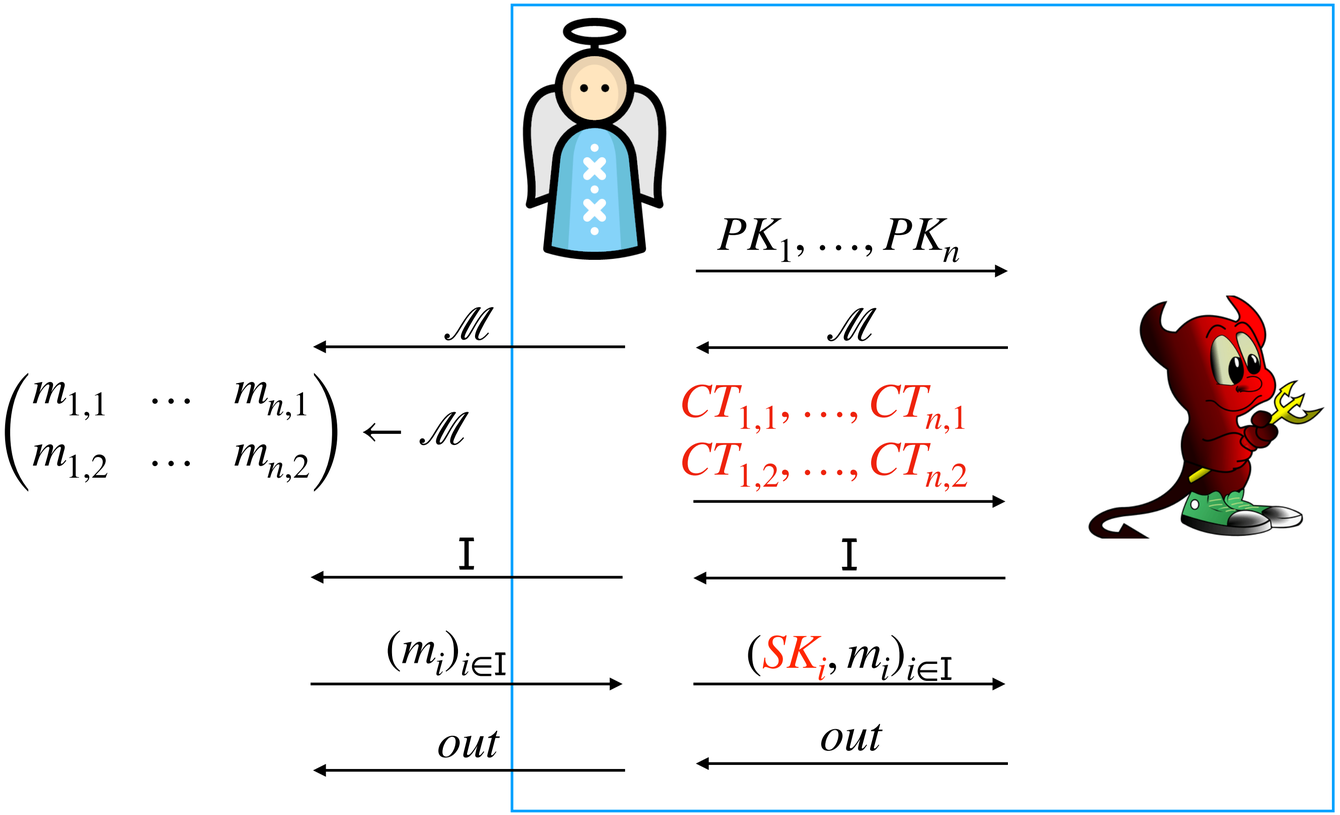
# Security in the Single-Challenge Setting



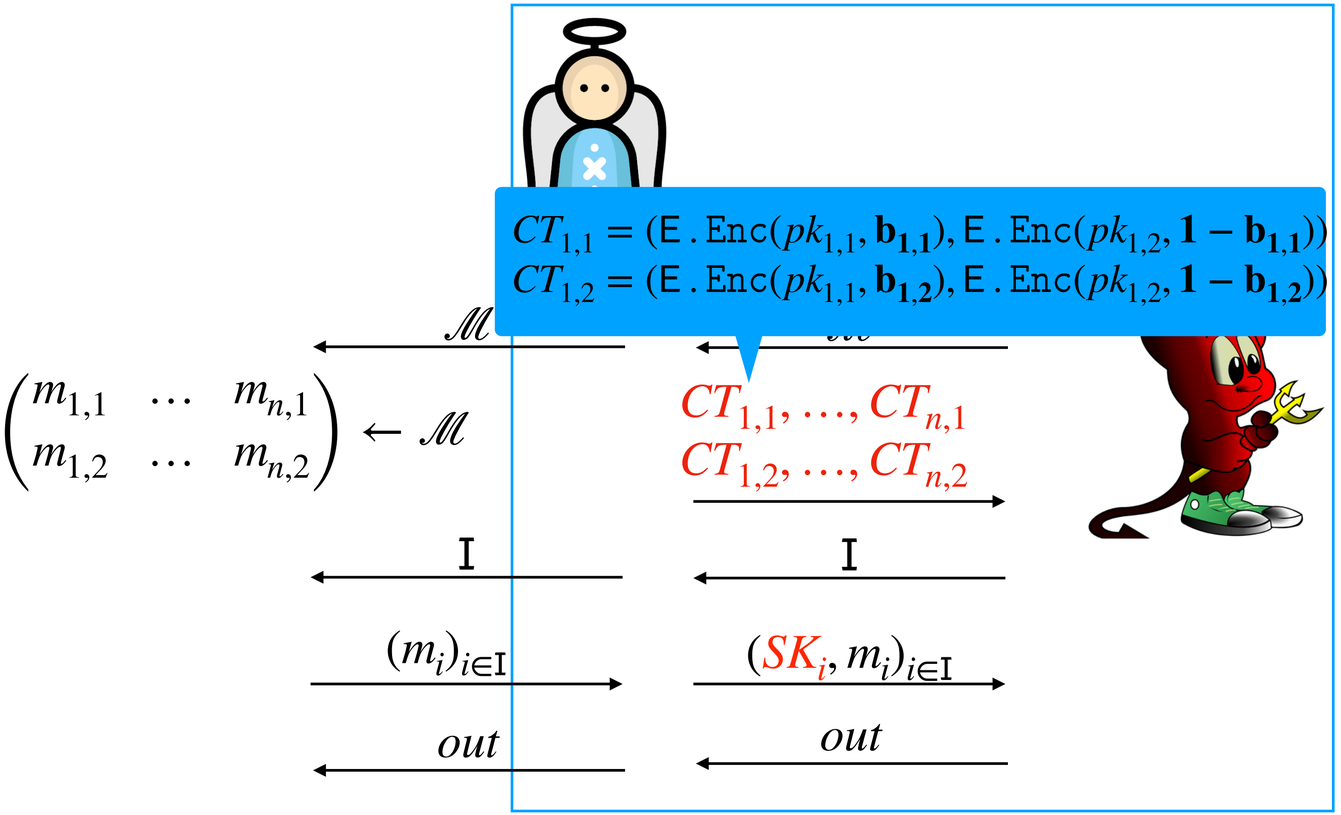
# Security in the Single-Challenge Setting



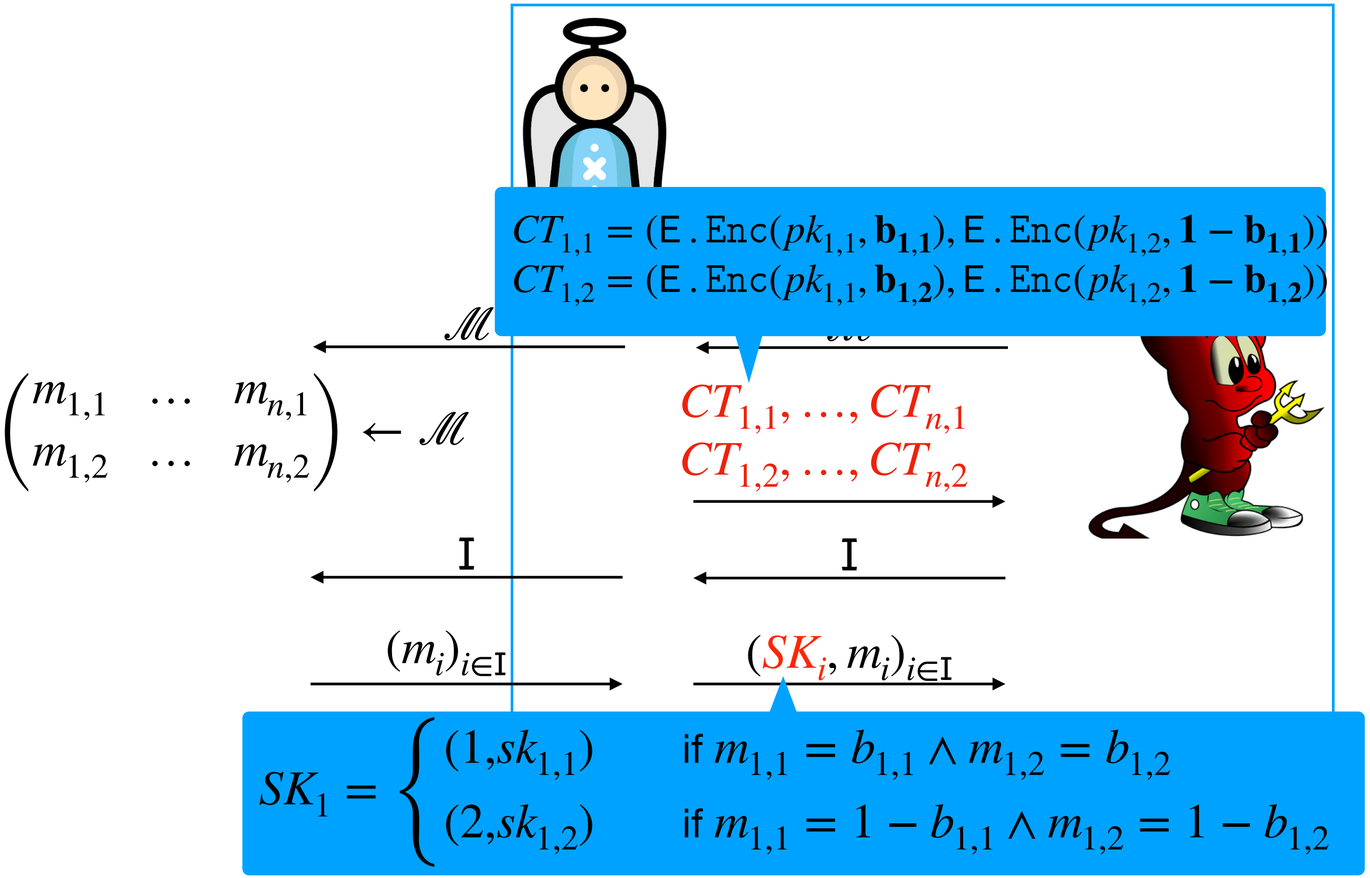
# Insecurity in the Multi-Challenge Setting



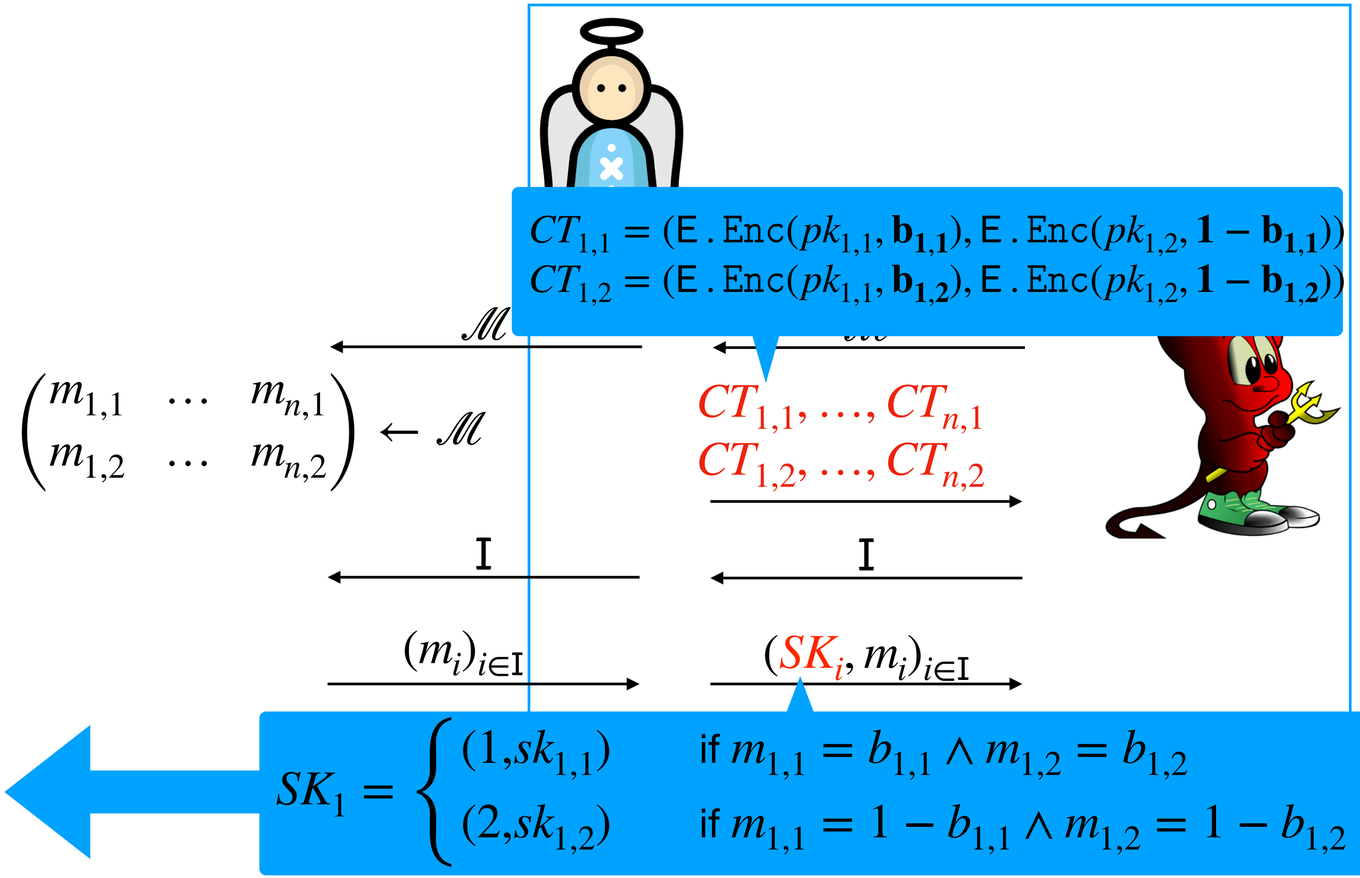
# Insecurity in the Multi-Challenge Setting



# Insecurity in the Multi-Challenge Setting

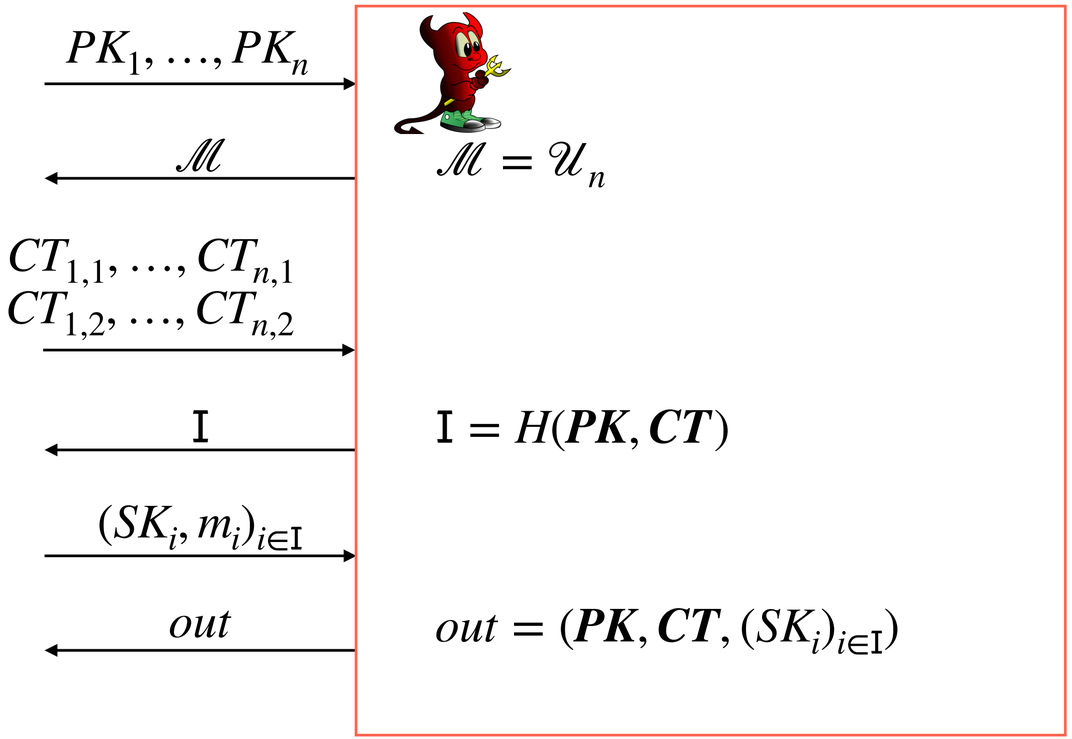


# Insecurity in the Multi-Challenge Setting

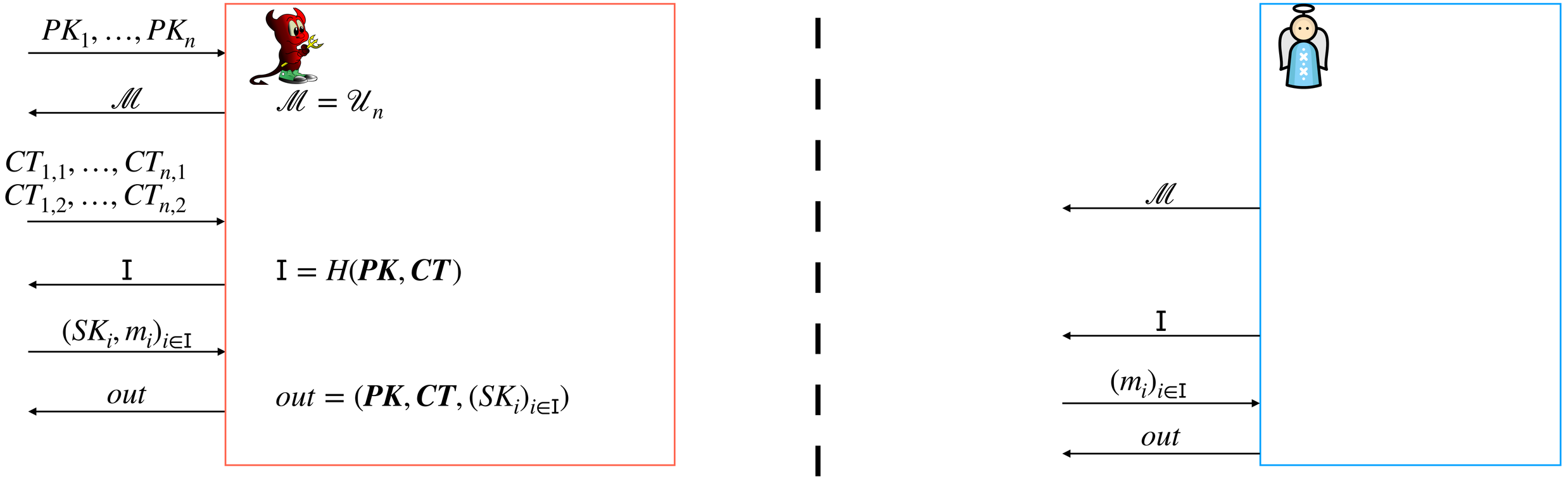



| $m_{1,1}$ | $m_{1,2}$ |
|---|---|
| $b_{1,1}$ | $b_{1,2}$ |
| $1 - b_{1,1}$ | $1 - b_{1,2}$ |
| $1 - b_{1,1}$ | $b_{1,2}$ |
| $b_{1,1}$ | $1 - b_{1,2}$ |

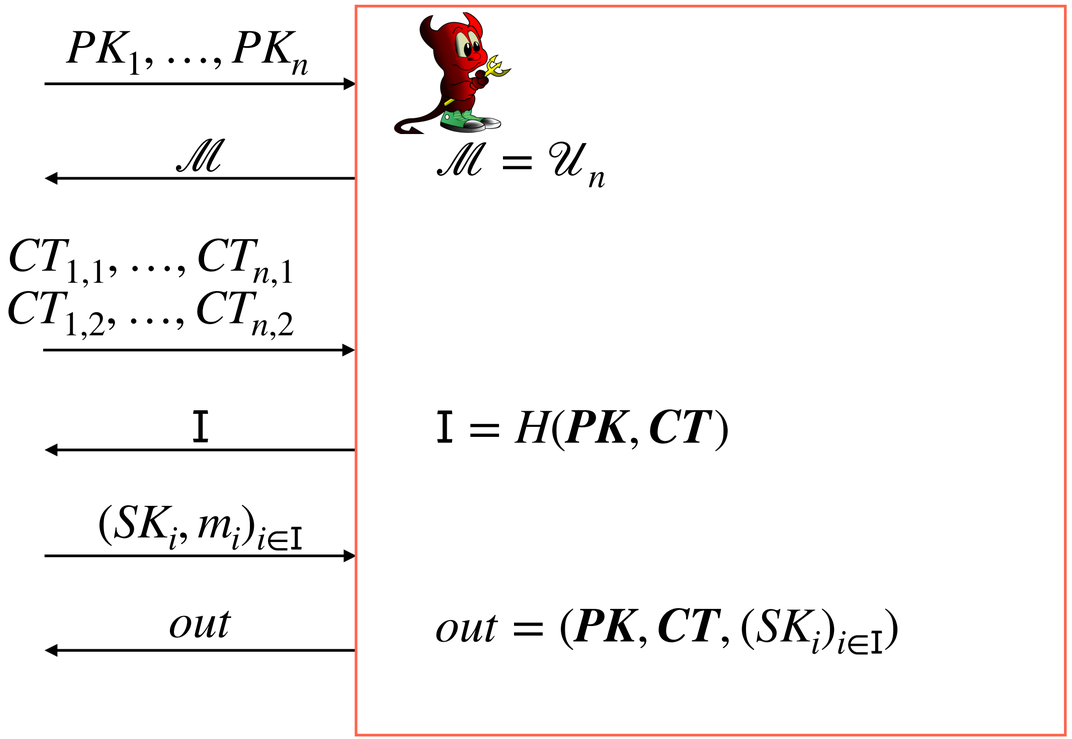
# Insecurity in the Multi-Challenge Setting

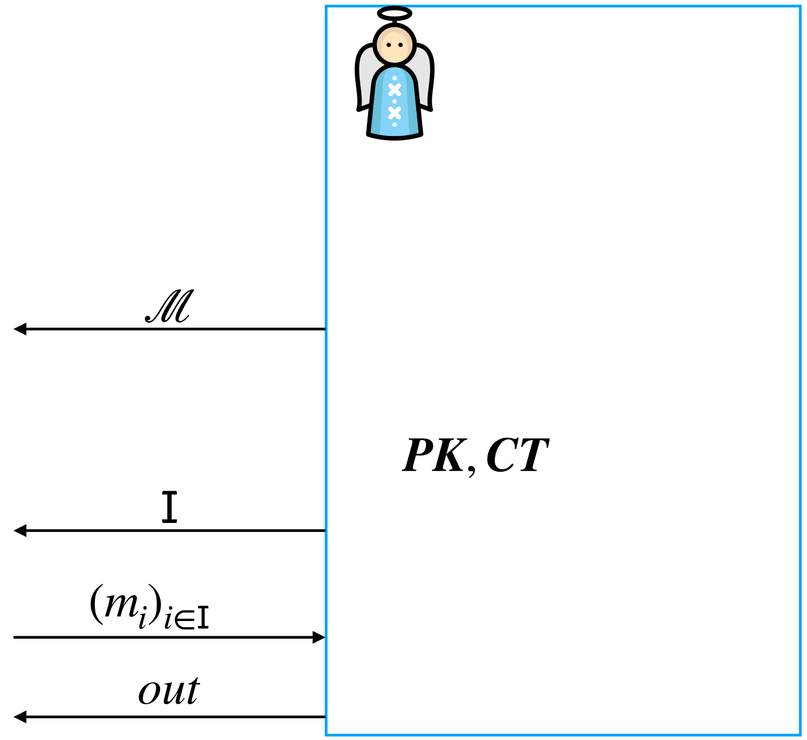


# Insecurity in the Multi-Challenge Setting



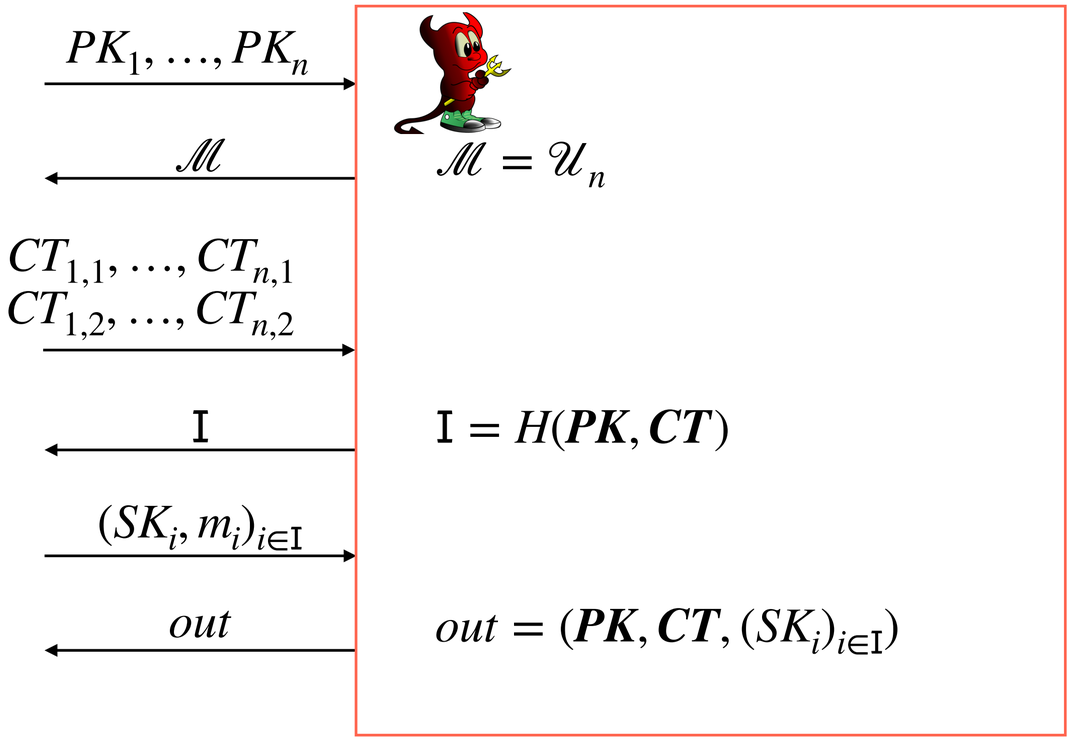
# Insecurity in the Multi-Challenge Setting

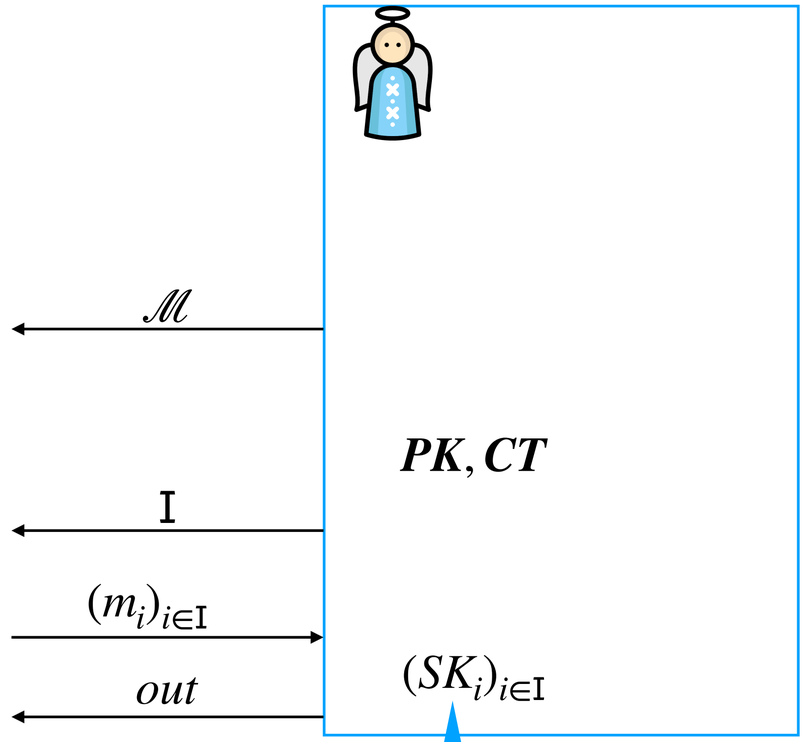



**Security of hash $H$**

# Insecurity in the Multi-Challenge Setting

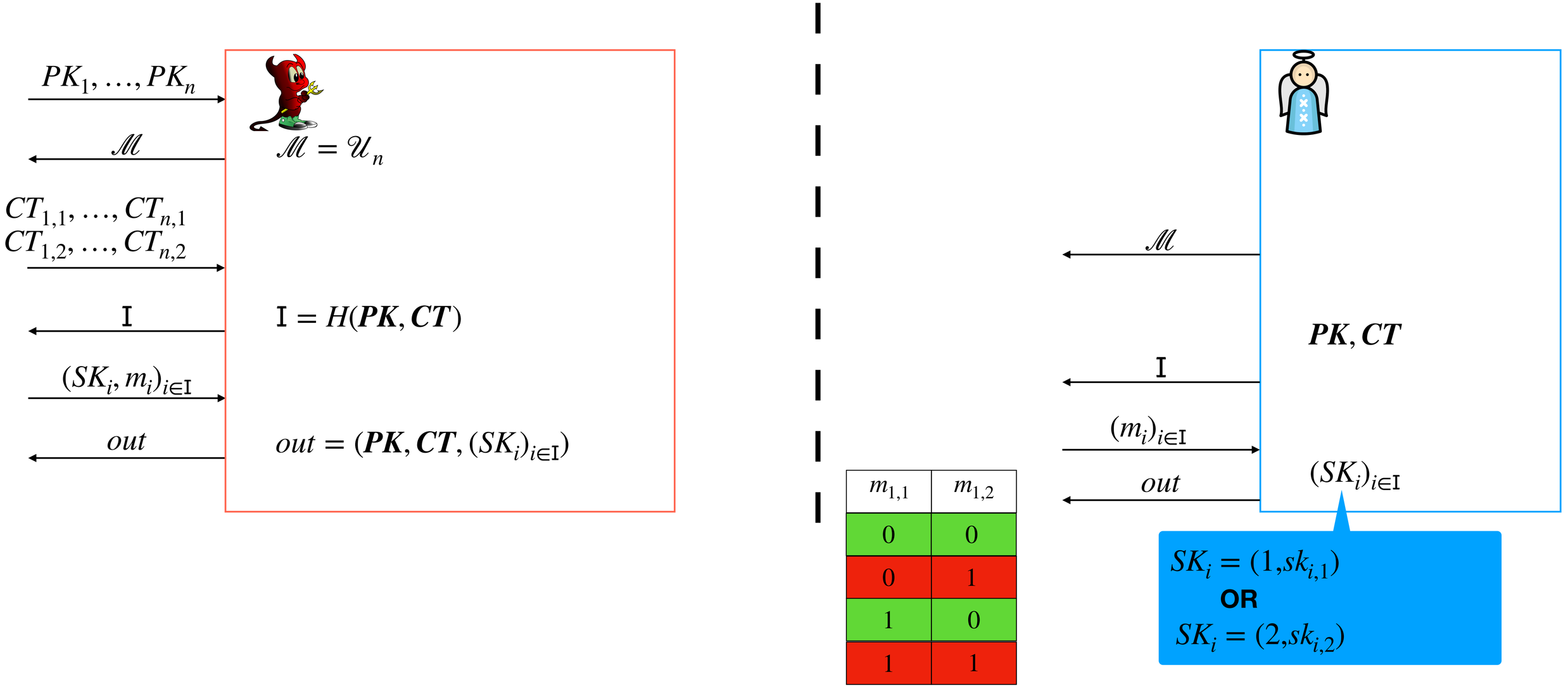



**Uniqueness of secret key**

$SK_i = (1, sk_{i,1})$
**OR**
$SK_i = (2, sk_{i,2})$

# Insecurity in the Multi-Challenge Setting



# Our Results

- RSO security in the single-challenge setting $\not\Longrightarrow$ RSO security in the multi-challenge setting
- RSO secure PKE in the multi-challenge setting ☜
- Lower bound on secret key length for PKE schemes with RSO security in the $k$-challenge setting
- RSO secure PKE with nearly optimal secret key length

# Starting Point

$\Pi$:

$\texttt{KeyGen}(1^\lambda)$ :
$(pk_1, sk_1) \leftarrow \mathsf{E}.\texttt{KeyGen}(1^\lambda)$
$(pk_2, sk_2) \leftarrow \mathsf{E}.\texttt{KeyGen}(1^\lambda)$
$s \leftarrow \{1,2\}$
$SK = (s, sk_s)$
$PK = (pk_1, pk_2)$

$\texttt{Enc}(PK = (pk_1, pk_2), m \in \{0,1\})$ :
$ct_1 \leftarrow \mathsf{E}.\texttt{Enc}(pk_1, m)$
$ct_2 \leftarrow \mathsf{E}.\texttt{Enc}(pk_2, m)$
$CT = (ct_1, ct_2)$

$\texttt{Dec}(SK = (s, sk_s), CT = (ct_1, ct_2))$ :
$m \leftarrow \mathsf{E}.\texttt{Dec}(sk_s, ct_s)$

# Starting Point

**Π:**

$\texttt{KeyGen}(1^\lambda)$ :
$(pk_1, sk_1) \leftarrow \mathsf{E}.\texttt{KeyGen}(1^\lambda)$
$(pk_2, sk_2) \leftarrow \mathsf{E}.\texttt{KeyGen}(1^\lambda)$
$s \leftarrow \{1,2\}$
$SK = (s, sk_s)$
$PK = (pk_1, pk_2)$

$\texttt{Enc}(PK = (pk_1, pk_2), m \in \{0,1\})$ :
$ct_1 \leftarrow \mathsf{E}.\texttt{Enc}(pk_1, m)$
$ct_2 \leftarrow \mathsf{E}.\texttt{Enc}(pk_2, m)$
$CT = (ct_1, ct_2)$

$\texttt{Dec}(SK = (s, sk_s), CT = (ct_1, ct_2))$ :
$m \leftarrow \mathsf{E}.\texttt{Dec}(sk_s, ct_s)$

$CT = ( \; b \; , \; 1 - b \; )$

$$SK = \begin{cases} (1, sk_{1,1}) & \text{if } m = b \\ (2, sk_{1,2}) & \text{otherwise} \end{cases}$$

# Construction of PKE with RSO Security in the $k$-challenge Setting

**$\Pi'$:**

$\mathtt{KeyGen}(1^\lambda)$ :

For $i \in [1,k]$ :

$(pk_{i,1}, sk_{i,1}) \leftarrow \mathsf{E}.\mathtt{KeyGen}(1^\lambda)$

$(pk_{i,2}, sk_{i,2}) \leftarrow \mathsf{E}.\mathtt{KeyGen}(1^\lambda)$

$s_i \leftarrow \{1,2\}$

$SK = (s_i, sk_{i,s_i})_{i\in[1,k]}$

$PK = (pk_{i,1}, pk_{i,2})_{i\in[1,k]}$

**$\Pi$:**

$\mathtt{KeyGen}(1^\lambda)$ :

$(pk_1, sk_1) \leftarrow \mathsf{E}.\mathtt{KeyGen}(1^\lambda)$

$(pk_2, sk_2) \leftarrow \mathsf{E}.\mathtt{KeyGen}(1^\lambda)$

$s \leftarrow \{1,2\}$

$SK = (s, sk_s)$

$PK = (pk_1, pk_2)$

$\mathtt{Enc}(PK = (pk_1, pk_2), m \in \{0,1\})$ :

$ct_1 \leftarrow \mathsf{E}.\mathtt{Enc}(pk_1, m)$

$ct_2 \leftarrow \mathsf{E}.\mathtt{Enc}(pk_2, m)$

$CT = (ct_1, ct_2)$

$\mathtt{Dec}(SK = (s, sk_s), CT = (ct_1, ct_2))$ :

$m \leftarrow \mathsf{E}.\mathtt{Dec}(sk_s, ct_s)$

# Construction of PKE with RSO Security in the $k$-challenge Setting

**$\Pi'$:**

$\mathtt{KeyGen}(1^\lambda)$ :
For $i \in [1,k]$ :
$(pk_{i,1}, sk_{i,1}) \leftarrow \mathsf{E}.\mathtt{KeyGen}(1^\lambda)$
$(pk_{i,2}, sk_{i,2}) \leftarrow \mathsf{E}.\mathtt{KeyGen}(1^\lambda)$
$s_i \leftarrow \{1,2\}$
$SK = (s_i, sk_{i,s_i})_{i\in[1,k]}$
$PK = (pk_{i,1}, pk_{i,2})_{i\in[1,k]}$

$\mathtt{Enc}(PK = (pk_{i,1}, pk_{i,2})_{i\in[1,k]}, m \in \{0,1\})$ :
Sample $p_1, \ldots, p_k \leftarrow \{0,1\}$ s.t.
$p_1 \oplus p_2 \oplus \ldots \oplus p_k = m$
For $i \in [1,k]$:
$ct_{i,1} \leftarrow \mathsf{E}.\mathtt{Enc}(pk_{i,1}, p_i)$
$ct_{i,2} \leftarrow \mathsf{E}.\mathtt{Enc}(pk_{i,2}, p_i)$
$CT = (ct_{i,1}, ct_{i,2})_{i\in[1,k]}$

**$\Pi$:**

$\mathtt{KeyGen}(1^\lambda)$ :
$(pk_1, sk_1) \leftarrow \mathsf{E}.\mathtt{KeyGen}(1^\lambda)$
$(pk_2, sk_2) \leftarrow \mathsf{E}.\mathtt{KeyGen}(1^\lambda)$
$s \leftarrow \{1,2\}$
$SK = (s, sk_s)$
$PK = (pk_1, pk_2)$

$\mathtt{Enc}(PK = (pk_1, pk_2), m \in \{0,1\})$ :
$ct_1 \leftarrow \mathsf{E}.\mathtt{Enc}(pk_1, m)$
$ct_2 \leftarrow \mathsf{E}.\mathtt{Enc}(pk_2, m)$
$CT = (ct_1, ct_2)$

$\mathtt{Dec}(SK = (s, sk_s), CT = (ct_1, ct_2))$ :
$m \leftarrow \mathsf{E}.\mathtt{Dec}(sk_s, ct_s)$

# Construction of PKE with RSO Security in the $k$-challenge Setting

**$\Pi'$:**

$\mathtt{KeyGen}(1^\lambda)$ :

For $i \in [1,k]$ :

$(pk_{i,1}, sk_{i,1}) \leftarrow \mathsf{E}.\mathtt{KeyGen}(1^\lambda)$

$(pk_{i,2}, sk_{i,2}) \leftarrow \mathsf{E}.\mathtt{KeyGen}(1^\lambda)$

$s_i \leftarrow \{1,2\}$

$SK = (s_i, sk_{i,s_i})_{i\in[1,k]}$

$PK = (pk_{i,1}, pk_{i,2})_{i\in[1,k]}$

$\mathtt{Enc}(PK = (pk_{i,1}, pk_{i,2})_{i\in[1,k]}, m \in \{0,1\})$ :

Sample $p_1, \ldots, p_k \leftarrow \{0,1\}$ s.t.

$p_1 \oplus p_2 \oplus \ldots \oplus p_k = m$

For $i \in [1,k]$:

$ct_{i,1} \leftarrow \mathsf{E}.\mathtt{Enc}(pk_{i,1}, p_i)$

$ct_{i,2} \leftarrow \mathsf{E}.\mathtt{Enc}(pk_{i,2}, p_i)$

$CT = (ct_{i,1}, ct_{i,2})_{i\in[1,k]}$

$\mathtt{Dec}(SK = (s_i, sk_{i,s_i})_{i\in[1,k]}, CT = (ct_{i,1}, ct_{i,2})_{i\in[1,k]})$ :

For $i \in [1,k]$:

$p_i \leftarrow \mathsf{E}.\mathtt{Dec}(sk_{i,s_i}, ct_{i,s_i})$

$m = p_1 \oplus p_2 \oplus \ldots \oplus p_k$

**$\Pi$:**

$\mathtt{KeyGen}(1^\lambda)$ :

$(pk_1, sk_1) \leftarrow \mathsf{E}.\mathtt{KeyGen}(1^\lambda)$

$(pk_2, sk_2) \leftarrow \mathsf{E}.\mathtt{KeyGen}(1^\lambda)$

$s \leftarrow \{1,2\}$

$SK = (s, sk_s)$

$PK = (pk_1, pk_2)$

$\mathtt{Enc}(PK = (pk_1, pk_2), m \in \{0,1\})$ :

$ct_1 \leftarrow \mathsf{E}.\mathtt{Enc}(pk_1, m)$

$ct_2 \leftarrow \mathsf{E}.\mathtt{Enc}(pk_2, m)$

$CT = (ct_1, ct_2)$

$\mathtt{Dec}(SK = (s, sk_s), CT = (ct_1, ct_2))$ :

$m \leftarrow \mathsf{E}.\mathtt{Dec}(sk_s, ct_s)$

# Construction of PKE with RSO Security in the $k$-challenge Setting

**$\Pi'$:**

$\texttt{KeyGen}(1^\lambda)$ :

For $i \in [1,k]$ :

$(pk_{i,1}, sk_{i,1}) \leftarrow \mathsf{E}.\texttt{KeyGen}(1^\lambda)$

$(pk_{i,2}, sk_{i,2}) \leftarrow \mathsf{E}.\texttt{KeyGen}(1^\lambda)$

$s_i \leftarrow \{1,2\}$

$SK = (s_i, sk_{i,s_i})_{i\in[1,k]}$

$PK = (pk_{i,1}, pk_{i,2})_{i\in[1,k]}$

$\texttt{Enc}(PK = (pk_{i,1}, pk_{i,2})_{i\in[1,k]}, m \in \{0,1\})$ :

Sample $p_1, \ldots, p_k \leftarrow \{0,1\}$ s.t.

$p_1 \oplus p_2 \oplus \ldots \oplus p_k = m$

For $i \in [1,k]$:

$ct_{i,1} \leftarrow \mathsf{E}.\texttt{Enc}(pk_{i,1}, p_i)$

$ct_{i,2} \leftarrow \mathsf{E}.\texttt{Enc}(pk_{i,2}, p_i)$

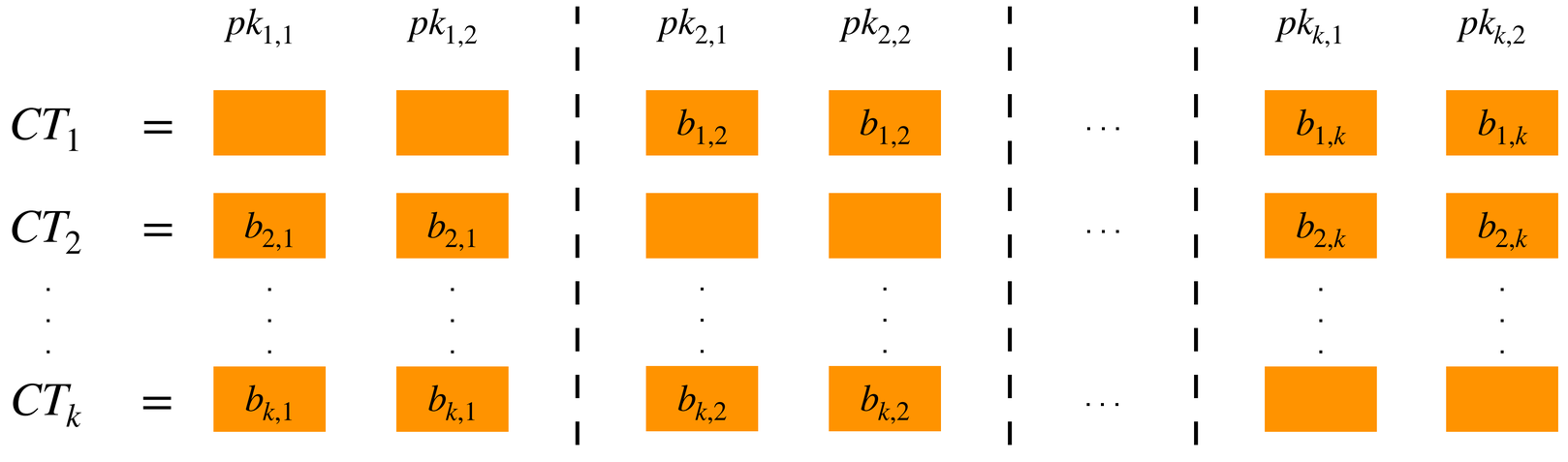
$CT = (ct_{i,1}, ct_{i,2})_{i\in[1,k]}$

$\texttt{Dec}(SK = (s_i, sk_{i,s_i})_{i\in[1,k]}, CT = (ct_{i,1}, ct_{i,2})_{i\in[1,k]})$ :

For $i \in [1,k]$:

$p_i \leftarrow \mathsf{E}.\texttt{Dec}(sk_{i,s_i}, ct_{i,s_i})$

$m = p_1 \oplus p_2 \oplus \ldots \oplus p_k$



# Construction of PKE with RSO Security in the $k$-challenge Setting

$\Pi'$:

$\mathtt{KeyGen}(1^\lambda)$ :

For $i \in [1,k]$ :

$(pk_{i,1}, sk_{i,1}) \leftarrow \mathsf{E}.\mathtt{KeyGen}(1^\lambda)$

$(pk_{i,2}, sk_{i,2}) \leftarrow \mathsf{E}.\mathtt{KeyGen}(1^\lambda)$

$s_i \leftarrow \{1,2\}$

$SK = (s_i, sk_{i,s_i})_{i\in[1,k]}$

$PK = (pk_{i,1}, pk_{i,2})_{i\in[1,k]}$

$\mathtt{Enc}(PK = (pk_{i,1}, pk_{i,2})_{i\in[1,k]}, m \in \{0,1\})$ :

Sample $p_1, \ldots, p_k \leftarrow \{0,1\}$ s.t.

$p_1 \oplus p_2 \oplus \ldots \oplus p_k = m$

For $i \in [1,k]$:

$ct_{i,1} \leftarrow \mathsf{E}.\mathtt{Enc}(pk_{i,1}, p_i)$

$ct_{i,2} \leftarrow \mathsf{E}.\mathtt{Enc}(pk_{i,2}, p_i)$

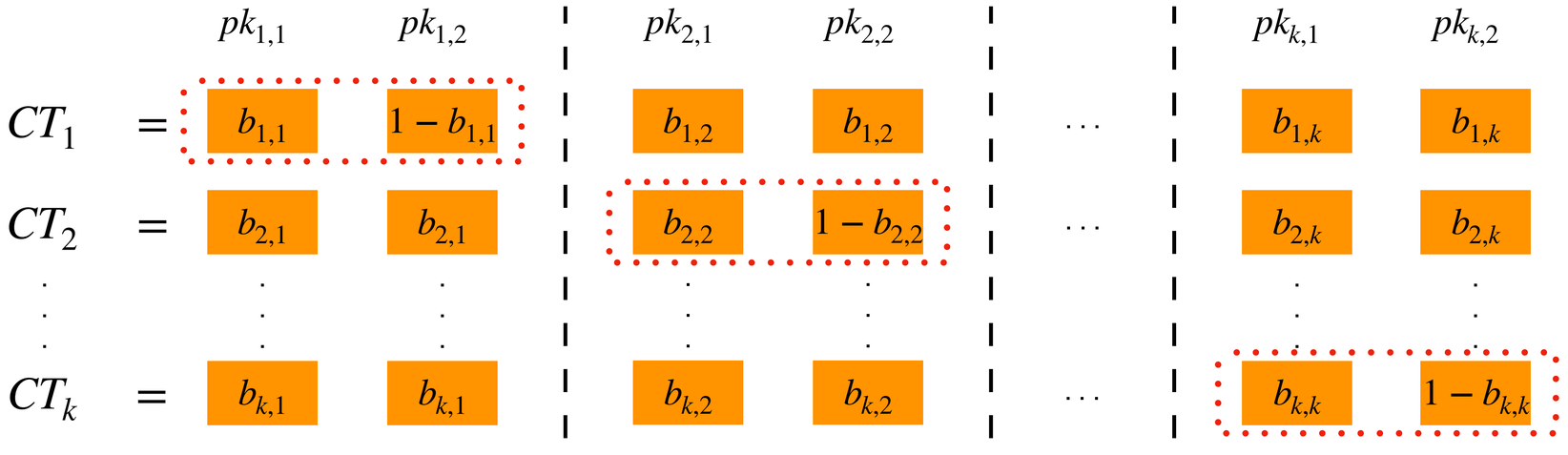
$CT = (ct_{i,1}, ct_{i,2})_{i\in[1,k]}$

$\mathtt{Dec}(SK = (s_i, sk_{i,s_i})_{i\in[1,k]}, CT = (ct_{i,1}, ct_{i,2})_{i\in[1,k]})$ :

For $i \in [1,k]$:

$p_i \leftarrow \mathsf{E}.\mathtt{Dec}(sk_{i,s_i}, ct_{i,s_i})$

$m = p_1 \oplus p_2 \oplus \ldots \oplus p_k$



# Construction of PKE with RSO Security in the $k$-challenge Setting

## $\Pi'$:

$\texttt{KeyGen}(1^\lambda)$ :

For $i \in [1,k]$ :

$(pk_{i,1}, sk_{i,1}) \leftarrow \mathsf{E}.\texttt{KeyGen}(1^\lambda)$

$(pk_{i,2}, sk_{i,2}) \leftarrow \mathsf{E}.\texttt{KeyGen}(1^\lambda)$

$s_i \leftarrow \{1,2\}$

$SK = (s_i, sk_{i,s_i})_{i\in[1,k]}$

$PK = (pk_{i,1}, pk_{i,2})_{i\in[1,k]}$

$\texttt{Enc}(PK = (pk_{i,1}, pk_{i,2})_{i\in[1,k]}, m \in \{0,1\})$ :

Sample $p_1, \ldots, p_k \leftarrow \{0,1\}$ s.t.

$p_1 \oplus p_2 \oplus \ldots \oplus p_k = m$

For $i \in [1,k]$:

$ct_{i,1} \leftarrow \mathsf{E}.\texttt{Enc}(pk_{i,1}, p_i)$

$ct_{i,2} \leftarrow \mathsf{E}.\texttt{Enc}(pk_{i,2}, p_i)$

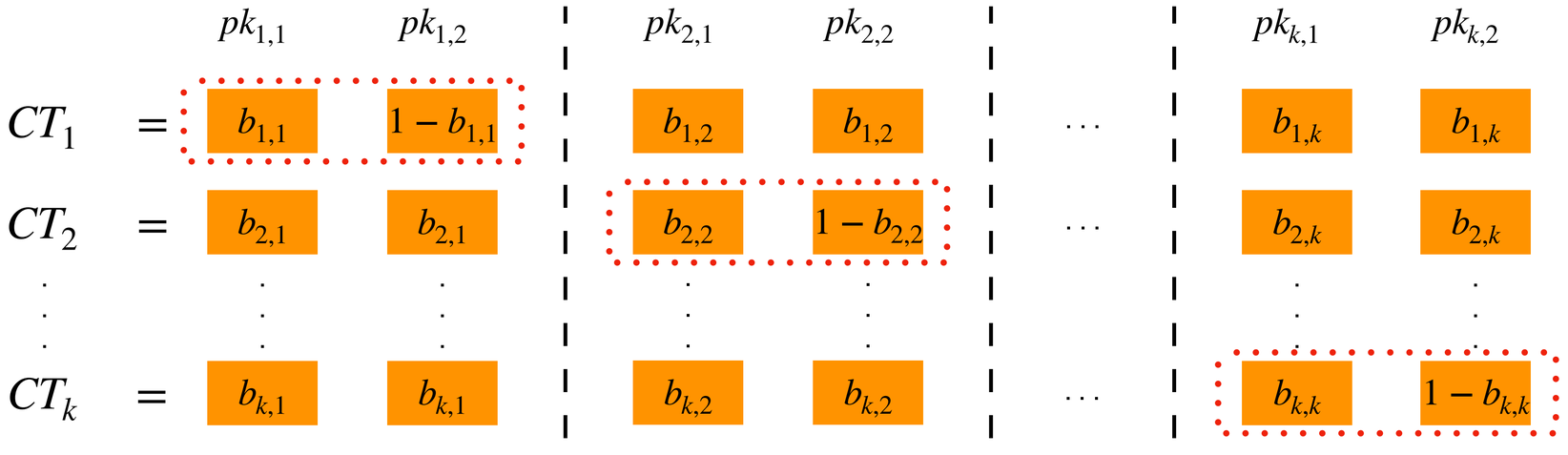
$CT = (ct_{i,1}, ct_{i,2})_{i\in[1,k]}$

$\texttt{Dec}(SK = (s_i, sk_{i,s_i})_{i\in[1,k]}, CT = (ct_{i,1}, ct_{i,2})_{i\in[1,k]})$ :

For $i \in [1,k]$:

$p_i \leftarrow \mathsf{E}.\texttt{Dec}(sk_{i,s_i}, ct_{i,s_i})$

$m = p_1 \oplus p_2 \oplus \ldots \oplus p_k$




$$SK = \begin{pmatrix} \begin{cases} (1,sk_{1,1}) & \text{if } m_1 = b_{1,1} \oplus b_{1,2} \oplus \ldots \oplus b_{1,k} \\ (2,sk_{1,2}) & \text{otherwise} \end{cases} \\ \begin{cases} (1,sk_{2,1}) & \text{if } m_1 = b_{2,1} \oplus b_{2,2} \oplus \ldots \oplus b_{2,k} \\ (2,sk_{2,2}) & \text{otherwise} \end{cases} \\ \vdots \\ \begin{cases} (1,sk_{k,1}) & \text{if } m_1 = b_{k,1} \oplus b_{k,2} \oplus \ldots \oplus b_{k,k} \\ (2,sk_{k,2}) & \text{otherwise} \end{cases} \end{pmatrix}$$

# Our Results

- RSO security in the single-challenge setting $\not\Longrightarrow$ RSO security in the multi-challenge setting
- RSO secure PKE in the multi-challenge setting
- Lower bound on secret key length for PKE schemes with RSO security in the $k$-challenge setting ☜
- RSO secure PKE with nearly optimal secret key length

# Lower Bound for PKE with RSO Security in the $k$-Challenge Setting

**Theorem**

If

#(possible secret keys) $<$ #(possible messages)

then

the scheme is not RSO secure.

# Lower Bound for PKE with RSO Security in the $k$-Challenge Setting

**Theorem**

If

#(possible secret keys) $<$ #(possible messages)

$\leq 2^l$

then

the scheme is not RSO secure.

For a PKE with secret key length $l$

# Lower Bound for PKE with RSO Security in the $k$-Challenge Setting

**Theorem**

If

#(possible secret keys) $\leq 2^l$ $<$ #(possible messages) $= 2^{mk}$

then

the scheme is not RSO secure.

For a PKE with secret key length $l$ and message space $\{0,1\}^m$

# Lower Bound for PKE with RSO Security in the $k$-Challenge Setting

**Theorem**

If

#(possible secret keys) $\leq 2^l$ $<$ #(possible messages) $= 2^{mk}$

then
the scheme is not RSO secure.

For a PKE with secret key length $l$ and message space $\{0,1\}^m$

$$l \geq mk$$

# Our Results

- RSO security in the single-challenge setting $\not\Longrightarrow$ RSO security in the multi-challenge setting
- RSO secure PKE in the multi-challenge setting
- Lower bound on secret key length for PKE schemes with RSO security in the $k$-challenge setting ($l \geq mk$)
- RSO secure PKE with nearly optimal secret key length ($l = (1 + o(1))mk$) ☜

# Our Results

- RSO security in the single-challenge setting $\not\Longrightarrow$ RSO security in the multi-challenge setting
- RSO secure PKE in the multi-challenge setting
- Lower bound on secret key length for PKE schemes with RSO security in the $k$-challenge setting ($l \geq mk$)
- RSO secure PKE with nearly optimal secret key length ($l = (1 + o(1))mk$)

  CCA Security

https://eprint.iacr.org/2020/1080

# Our Results

- RSO security in the single-challenge setting $\not\Longrightarrow$ RSO security in the multi-challenge setting
- RSO secure PKE in the multi-challenge setting
- Lower bound on secret key length for PKE schemes with RSO security in the $k$-challenge setting
- RSO secure PKE with nearly optimal secret key length

Thanks for your Attention!

https://eprint.iacr.org/2020/1080