# Public-key Encryption with Keyword Search in Multi-User, Multi-Challenge Setting under Adaptive Corruptions

PKC 2024

Yunhao Ling  Kai Zhang  Jie Chen*  Qiong Huang  Haifeng Qian



# Public-key Encryption with Keyword Search (PEKS)

Data Owner 1

Data Owner 2

Data Owner 3

Cloud

Receiver

# Public-key Encryption with Keyword Search (PEKS)

Data Owner 1

Data Owner 2

Data Owner 3

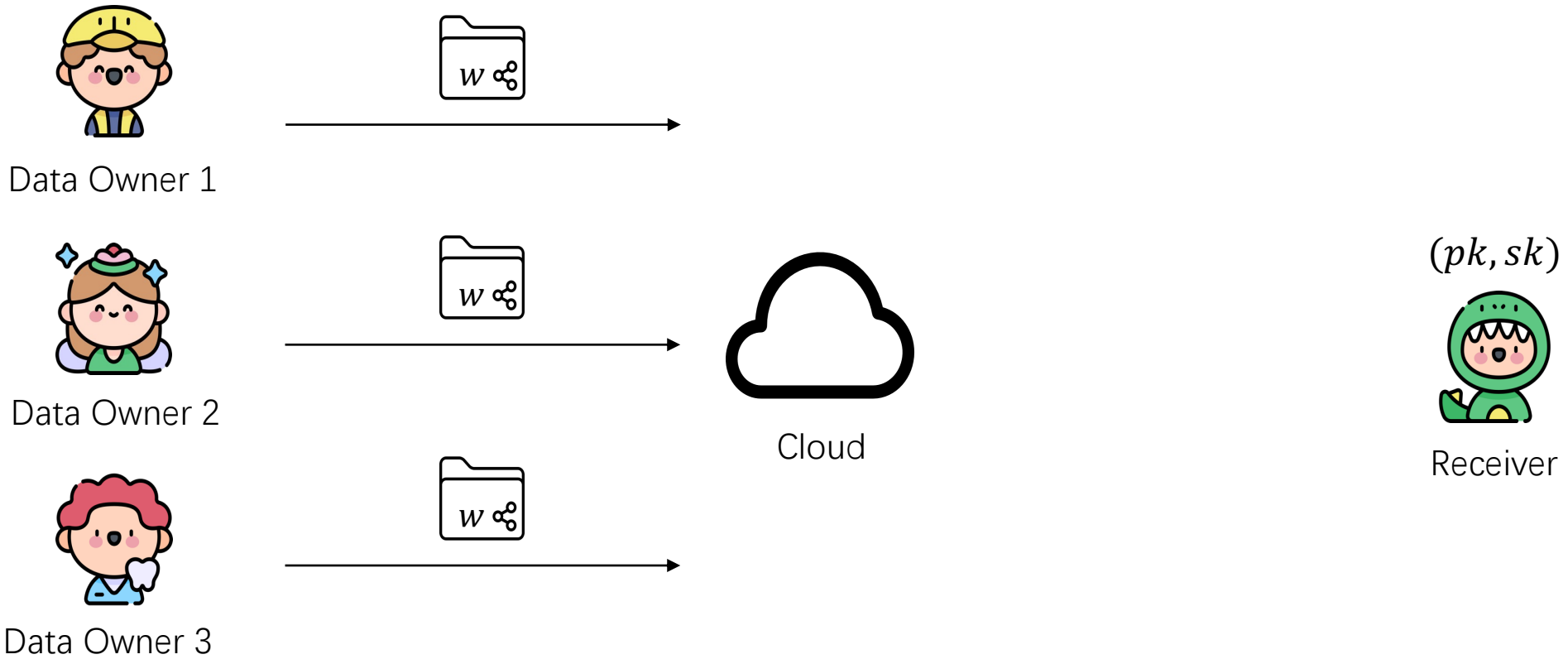
Cloud

$(pk, sk)$

Receiver

# Public-key Encryption with Keyword Search (PEKS)

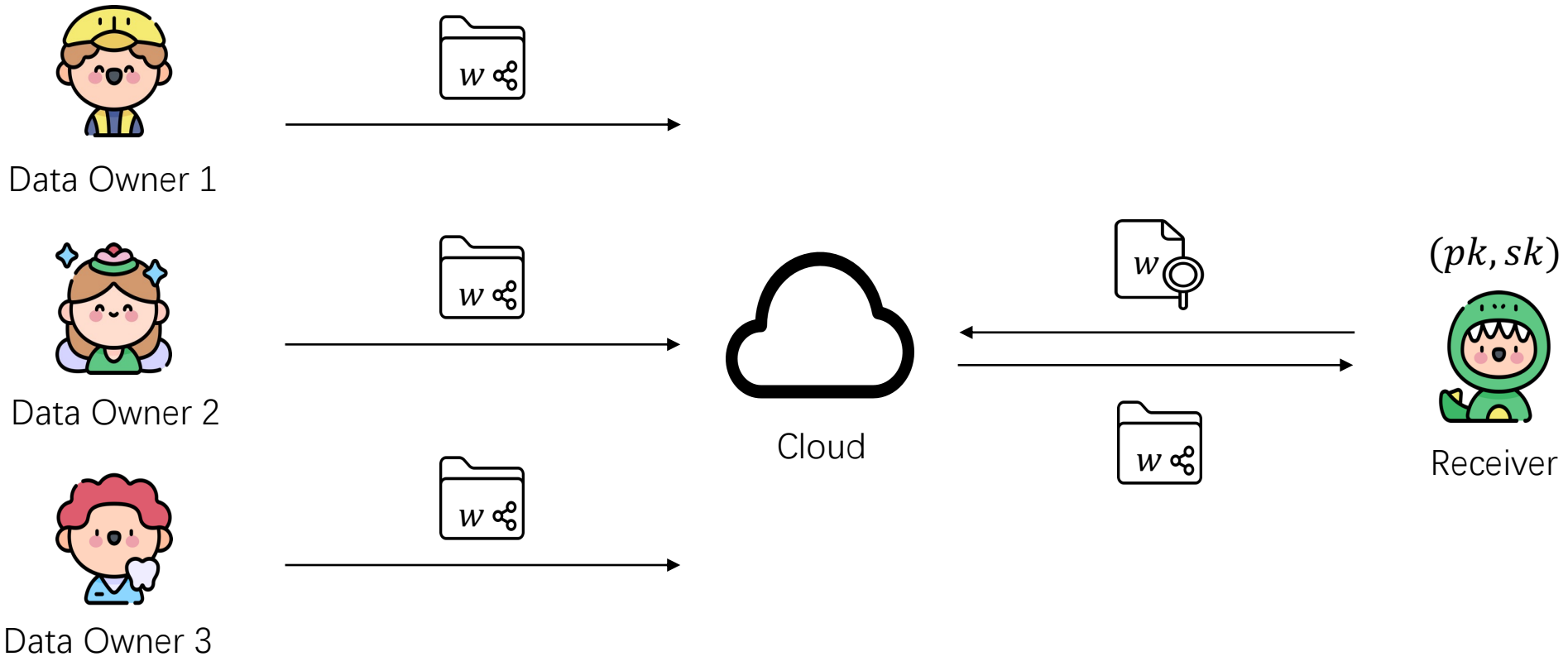
$ct \leftarrow Enc(pk, w)$



# Public-key Encryption with Keyword Search (PEKS)

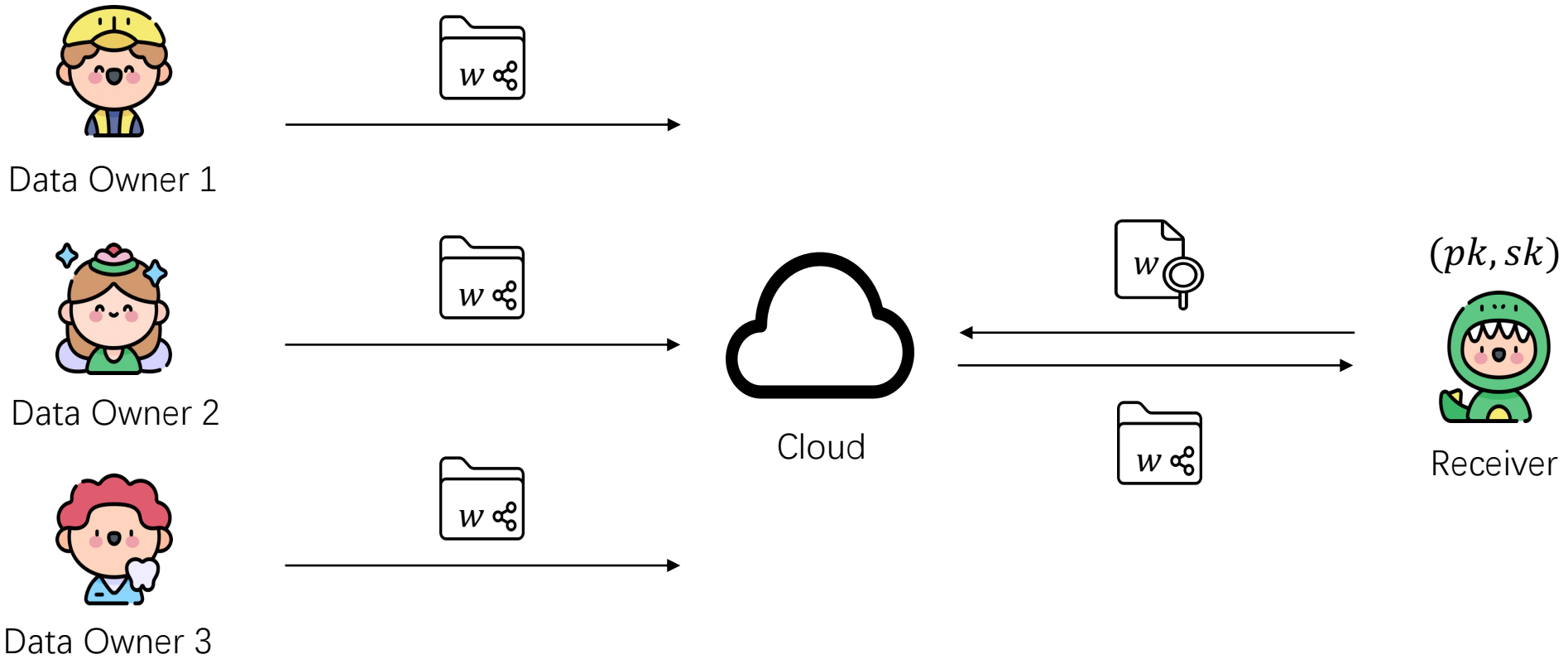
$ct \leftarrow Enc(pk, w)$

$T_w \leftarrow Trapdoor(sk, w)$



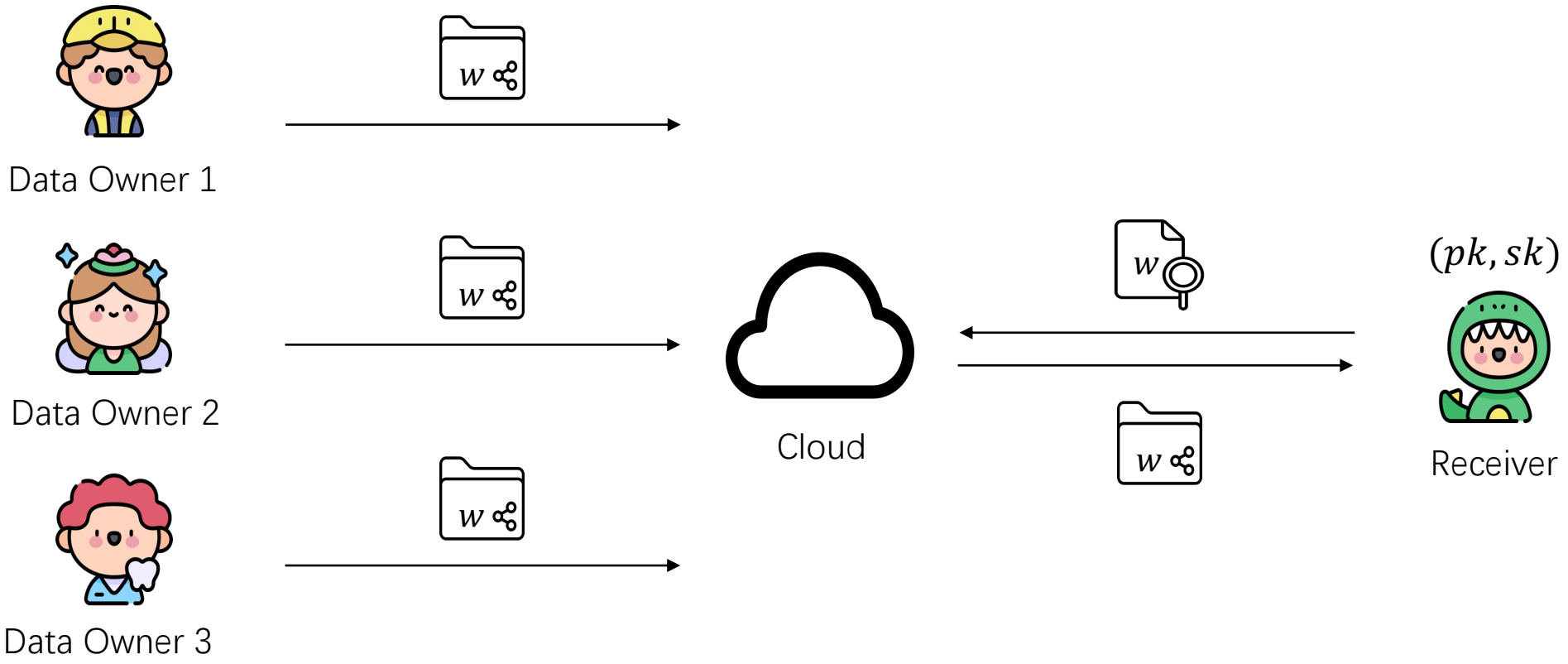
# Public-key Encryption with Keyword Search (PEKS)

$ct \leftarrow Enc(pk, w)$ $0/1 \leftarrow Test(T_w, ct)$ $T_w \leftarrow Trapdoor(sk, w)$



# Public-key Encryption with Keyword Search (PEKS)

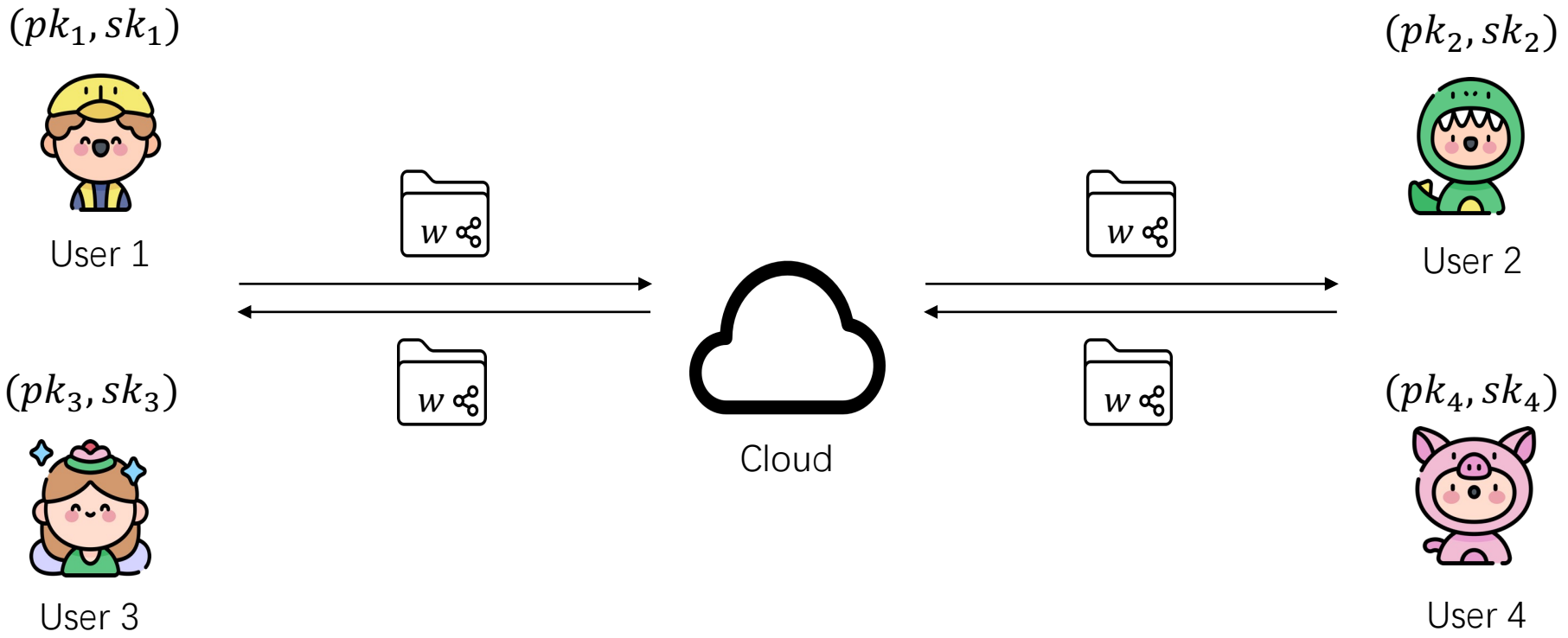
$ct \leftarrow Enc(pk, w)$ $0/1 \leftarrow Test(T_w, ct)$ $T_w \leftarrow Trapdoor(sk, w)$



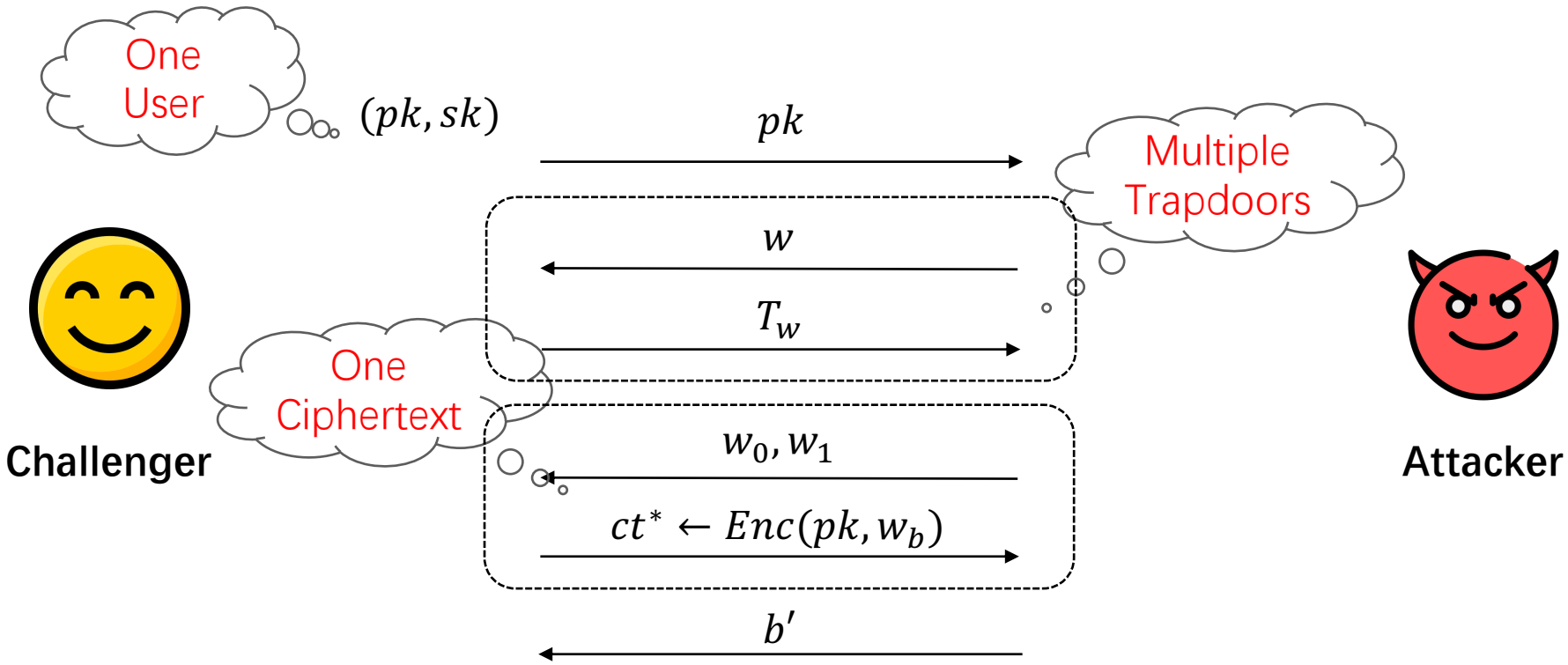

But only one user can be the receiver!

# PEKS in multi-user setting (MU-PEKS)

- **Motivation:** any user can be the receiver



# Insufficient security model of PEKS

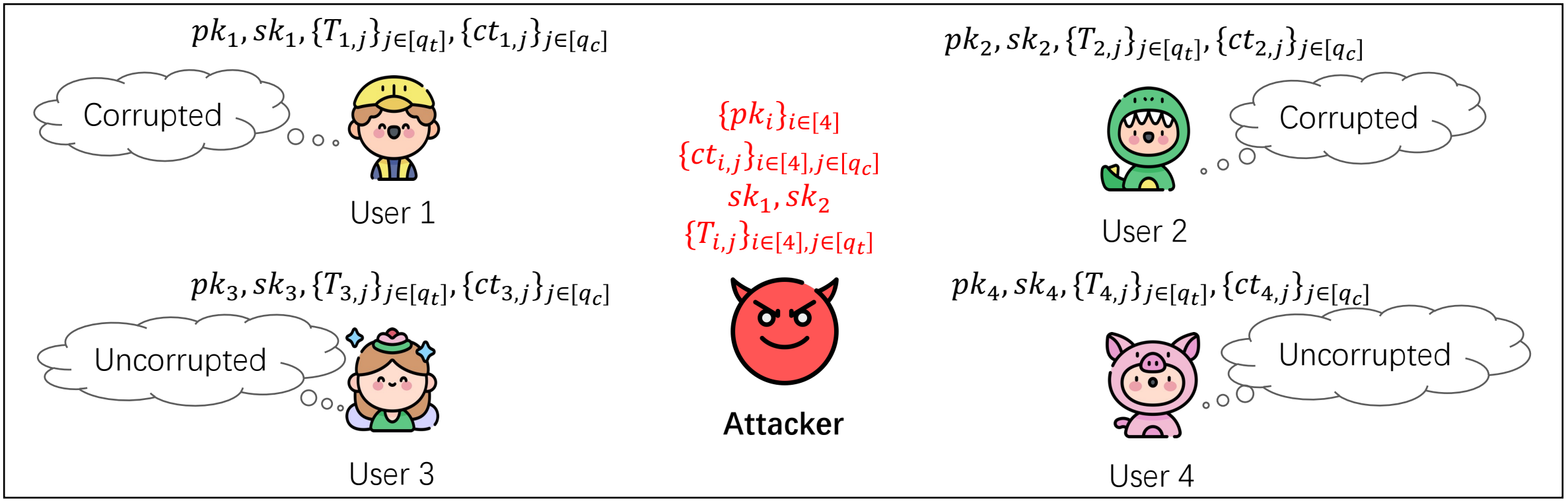



- **Observation:**

  - one user, one ciphertext, multiple trapdoors

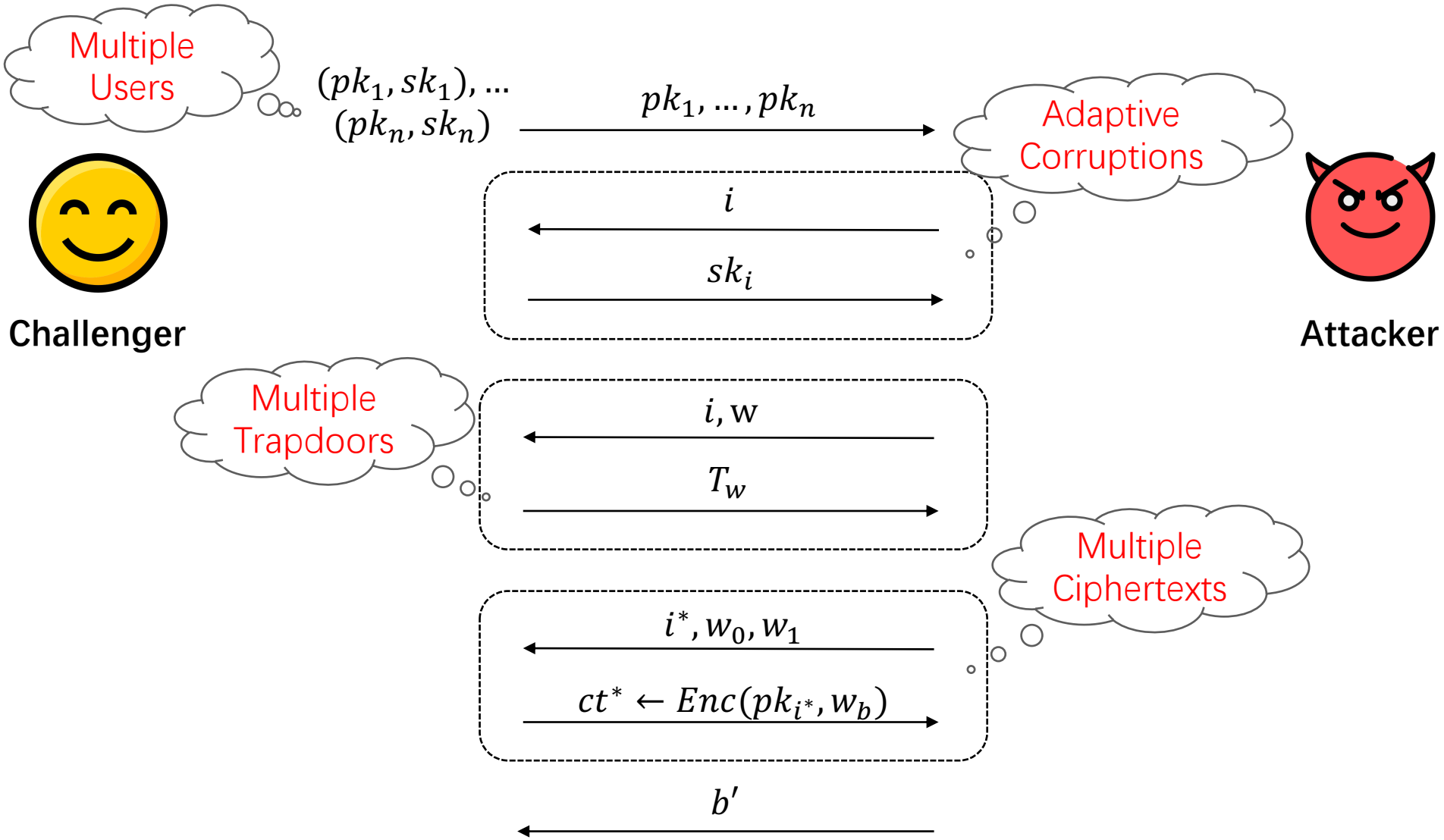
- **So:** cover one-user, one-ciphertext, multi-trapdoor scenario without corruption

# Real-world attack in MU-PEKS



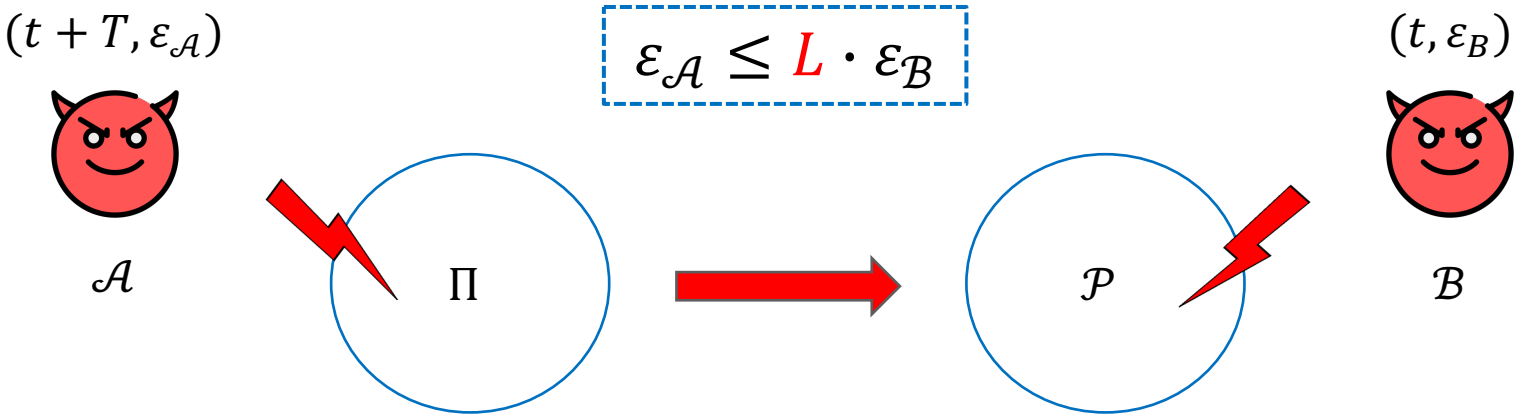

- **Observation:**
  - multi-user, multi-ciphertext, multi-trapdoor scenario with corruptions
- **The goal:** security guarantee for uncorrupted users
- **So:** security model in Multi-User, Multi-Challenge setting with Adaptive Corruption (MUMC-C)

# Our security model in MUMC-C



# Tight security

- **Security proof via security reduction**
  - $\mathcal{A}$ breaking the scheme $\Pi \Rightarrow \mathcal{B}$ solving the hard problem $\mathcal{P}$




  - $L$: security loss
  - $L$ in general is in the number of users and queries made by $\mathcal{A}$
  - **but:** larger $L \Rightarrow$ lower efficiency

- **Tight security:**
  - tight: $L = \mathcal{O}(1)$
  - enable scenario where the setting is huge or unknown

# Our contribution

- **Security model in MUMC-C for MU-PEKS**

- **Two MU-PEKS schemes over composite-order groups:**
  - tight security
  - standard model
  - simple assumptions

  *not yet practical, but theoretical progress*

- **New technique for proving multi-user security**

# Difficulty

- **[ABC+]:** any anonymous IBE scheme can be transformed into a secure PEKS scheme
  - what about MU-PEKS?

    MUMC-C ⟺ Multi-Instance, Multi-Challenge setting with adaptive Corruption (MIMC-C)
  - but no known anonymous IBE scheme in MIMC-C

- **State-of-the-art work:**
  - anonymous IBE in MIMC ([GDCC], [CGW], [Wee], …)

    (1) non-tight reduction (2) no corruption
  - IBE in MIMC ([HKS]) (non-anonymous)

    (1) non-tight reduction (2) no corruption
  - **Emphasis:** (1) and (2) *technically difficult*

# Dual system encryption

- **Dual system encryption:** a powerful tool to constructing adaptively secure IBE schemes.
- **Non-anonymous Lewko-Waters IBE scheme via dual system encryption:**

$$
\begin{aligned}
mpk: &\quad g^x, && g^y, && e(g,g)^{\alpha} \\
ct: &\quad g^r, && g^{r(xID+y)}, && e(g,g)^{\alpha r} \cdot m \\
sk: &\quad g^s \cdot R_3, && g^{\alpha+s(xID+y)} \cdot R_3' &&
\end{aligned}
$$

$$g \in G_{p_1}, R_3, R_3' \in G_{p_3},$$

# Proof of LW IBE

- **Security poof via hybrid argument using a sequence of games:**


**Game real**

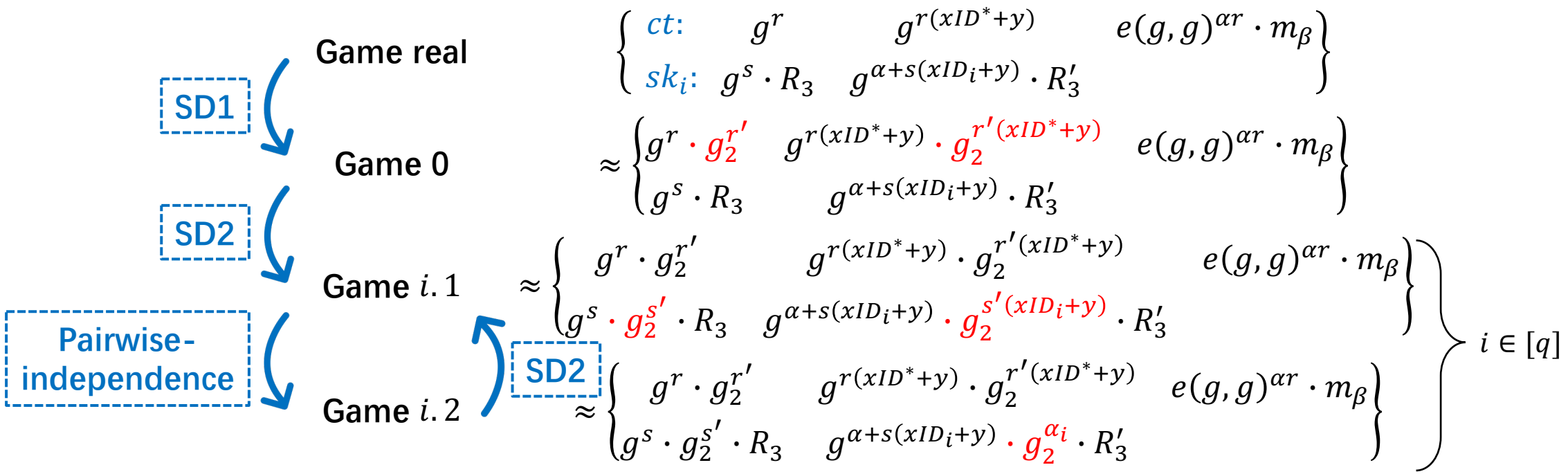
**Game 0**

$$\left\{\begin{array}{lccc} ct: & g^r & g^{r(xID^*+y)} & e(g,g)^{\alpha r}\cdot m_\beta \\ sk_i: & g^s\cdot R_3 & g^{\alpha+s(xID_i+y)}\cdot R_3' & \end{array}\right\}$$

$$\approx \left\{\begin{array}{lcc} g^r\cdot g_2^{r'} & g^{r(xID^*+y)}\cdot g_2^{r'(xID^*+y)} & e(g,g)^{\alpha r}\cdot m_\beta \\ g^s\cdot R_3 & g^{\alpha+s(xID_i+y)}\cdot R_3' & \end{array}\right\}$$

# Proof of LW IBE

- **Security poof via hybrid argument using a sequence of games:**




$$\left\{\begin{matrix} ct: & g^r & g^{r(xID^*+y)} & e(g,g)^{\alpha r}\cdot m_\beta \\ sk_i: & g^s\cdot R_3 & g^{\alpha+s(xID_i+y)}\cdot R_3' & \end{matrix}\right\}$$

$$\approx \left\{\begin{matrix} g^r\cdot g_2^{r'} & g^{r(xID^*+y)}\cdot g_2^{r'(xID^*+y)} & e(g,g)^{\alpha r}\cdot m_\beta \\ g^s\cdot R_3 & g^{\alpha+s(xID_i+y)}\cdot R_3' & \end{matrix}\right\}$$

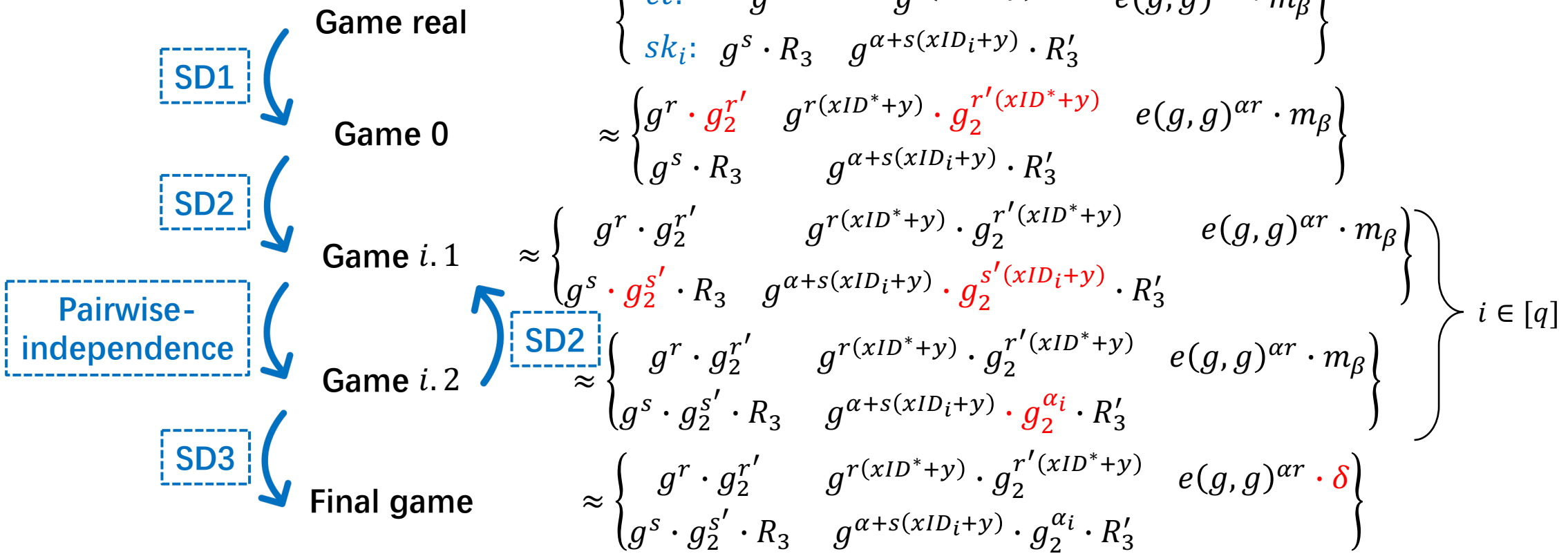
$$\approx \left\{\begin{matrix} g^r\cdot g_2^{r'} & g^{r(xID^*+y)}\cdot g_2^{r'(xID^*+y)} & e(g,g)^{\alpha r}\cdot m_\beta \\ g^s\cdot g_2^{s'}\cdot R_3 & g^{\alpha+s(xID_i+y)}\cdot g_2^{s'(xID_i+y)}\cdot R_3' & \end{matrix}\right\}$$

$$\approx \left\{\begin{matrix} g^r\cdot g_2^{r'} & g^{r(xID^*+y)}\cdot g_2^{r'(xID^*+y)} & e(g,g)^{\alpha r}\cdot m_\beta \\ g^s\cdot g_2^{s'}\cdot R_3 & g^{\alpha+s(xID_i+y)}\cdot g_2^{\alpha_i}\cdot R_3' & \end{matrix}\right\}$$

$i \in [q]$

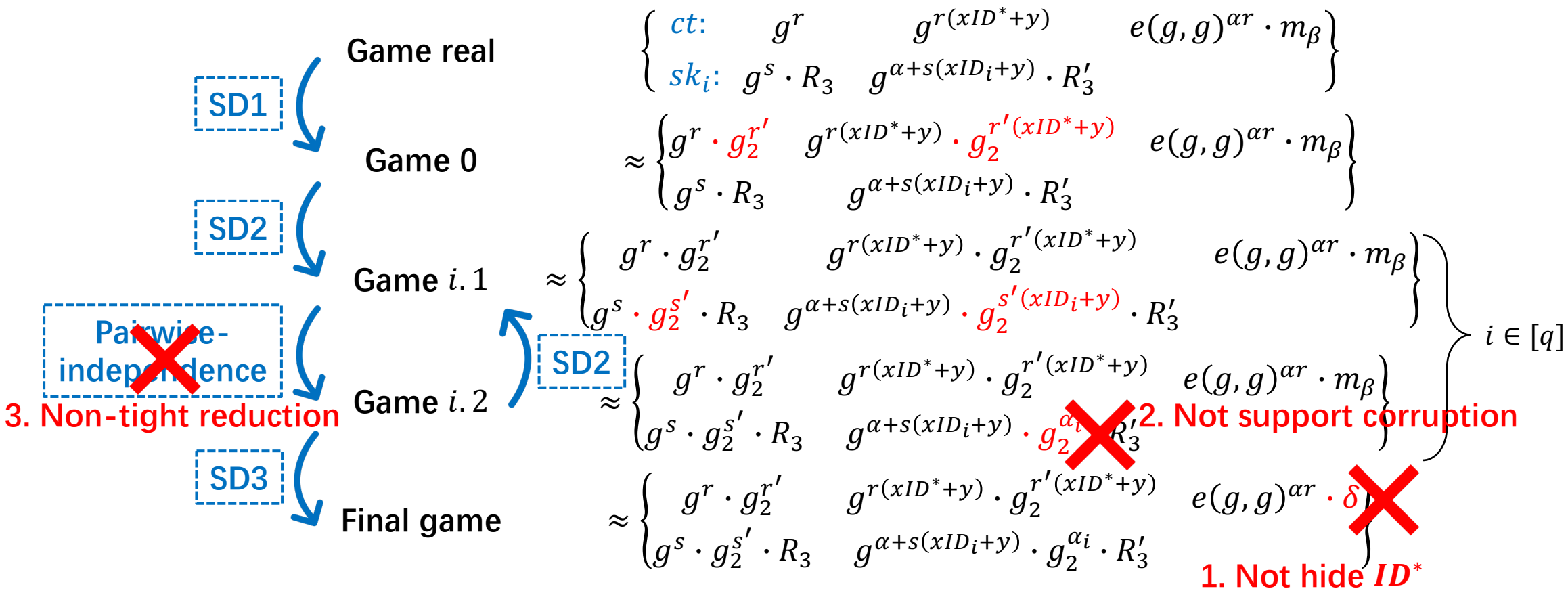
# Proof of LW IBE

- **Security poof via hybrid argument using a sequence of games:**



# Proof of LW IBE

- **Security poof via hybrid argument using a sequence of games:**



# Technical overview

- **Our first MU-PEKS scheme:**
  - the variant of Lewko-Waters IBE scheme (over asymmetric composite-order groups )

| | | | |
|---|---|---|---|
| $pk$: | $g^x$, | $g^y$, | $e(g, h^\alpha)$ |
| $sk$: | $x$, | $y$, | $\alpha$ |
| $ct$: | $g^r$, | $g^{r(xw+y)}$, | $e(g^r, h^\alpha) \cdot \delta, \delta$ |
| $td$: | $h^s$, | $h^{\alpha+s(xw+y)}$ | |

- **Intuition:**
  - **mask only keyword $w$ in ciphertext:**

    introduce $G_{p_2}$-components and entropy to $ct$; *no need* to introduce $H_{p_2}$-components to $td$
  - **address adaptive corruption:**

    *never* introduce entropy to $td$; generate *all* secret keys
  - **obtain tight reduction:**

    introduce entropy via *computational hard problems*

# Technical overview

- **Proof idea:**

**Game 0 (real game)**

| | | | |
|---|---|---|---|
| $sk$: | $x$, | $y$, | $\alpha$ |
| $ct$: | $g^r$, | $g^{r(xw_\beta+y)}$, | $e(g^r, h^\alpha) \cdot \delta, \delta$ |
| $td$: | $h^s$, | $h^{\alpha+s(xw+y)}$ | |

Transition by SD: $g^r \approx g^r \cdot g_2^{r'}$
($q$ instances via self-reducibility)

**Game 1**

| | | | |
|---|---|---|---|
| $sk$: | $x$, | $y$, | $\alpha$ |
| $ct$: | $g^r \cdot g_2^{r'}$, | $g^{r(xw_\beta+y)} \cdot g_2^{r'(xw_\beta+y)}$, | $e(g^r, h^\alpha) \cdot \delta, \delta$ |
| $td$: | $h^s$, | $h^{\alpha+s(xw+y)}$ | |

# Technical overview

- **Proof idea:**

| | | | | |
|---|---|---|---|---|
| | $sk$: | $x$, | $y$, | $\alpha$ |
| **Game 1** | $ct$: | $g^r \cdot g_2^{r'}$, | $g^{r(xw_\beta+y)} \cdot g_2^{r'(xw_\beta+y)}$, | $e(g^r, h^\alpha) \cdot \delta, \delta$ |
| | $td$: | $h^s$, | $h^{\alpha+s(xw+y)}$ | |

Transition by DDH in $G_{p_2}$: $(g_2^{r'}, g_2^{r'y}) \approx (g_2^{r'}, g_2^{r'y} \cdot g_2^z)$
($q$ instances via the self-reducibility)

| | | | | |
|---|---|---|---|---|
| | $sk$: | $x$, | $y$, | $\alpha$ |
| **Game 2** | $ct$: | $g^r \cdot g_2^{r'}$, | $g^{r(xw_\beta+y)} \cdot g_2^{r'xw_\beta+r'y} \cdot g_2^z$, | $e(g^r, h^\alpha) \cdot \delta, \delta$ |
| | $td$: | $h^s$, | $h^{\alpha+s(xw+y)}$ | |

# Technical overview

- **Proof idea:**

**Game 3** $ct$: $g^r \cdot g_2^{r'}$, $g^{r(x\eta+y)} \cdot g_2^{r'x\eta+r'y} \cdot g_2^z$, $e(g^r, h^\alpha) \cdot \delta, \delta$

each $g_2^z$ is randomly distributed in $G_{p_2}$ and $p_1, p_2$ are all $\Theta(\lambda)$ bits

- **Our second MU-PEKS scheme:**

-the variant of Wee IBE scheme (over asymmetric composite-order groups )

$pk$: $g^x$, $e(g,h)^\alpha$

$ct$: $g^{r(x+w)}$, $e(g,h)^{\alpha r} \cdot \delta, \delta$

$td$: $h^{\frac{\alpha}{x+w}}$,

- similar proof idea

# Comparison

| Scheme | $\|pk\|$ | | $\|ct\|$ | | $\|td\|$ | Enc | | Trapdoor | Test | MUMC-C | Security loss | **Randomized $td$** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | $\|G_N\|$ | $\|G_T\|$ | $\|G_N\|$ | $\|G_T\|$ | $\|H_N\|$ | $E_{G_N}$ | $E_T$ | $E_{H_N}$ | $P$ | | | |
| The first | 2 | 1 | 2 | 2 | 2 | 3 | 1 | 2 | 2 | ✓ | $\mathcal{O}(1)$ | ✓ |
| The second | 1 | 1 | 1 | 2 | 1 | 1 | 1 | 1 | 1 | ✓ | $\mathcal{O}(1)$ | ✗ |

- **Note:** the randomized trapdoor is important to some extensions of PEKS
  - e.g. public key authenticated encryption with keyword search (requiring trapdoor privacy)

# Future work and open problem

- **Future work:**

  - more tightly secure encryption schemes in multi-user setting (e.g. proxy re-encryption)

- **Open problem:** transform our schemes to prime-order version

  - ineffective transformation techniques of dual system encryption ([CGW], [Att])

Thank you for your attention!

Email: yhlingyy@163.com