Traitor Tracing with $N^{1/3}$-Size Ciphertexts and $O(1)$-Size Keys from k-Lin

Junqing Gong ✉

ECNU 上海期智研究院 SHANGHAI QI ZHI INSTITUTE

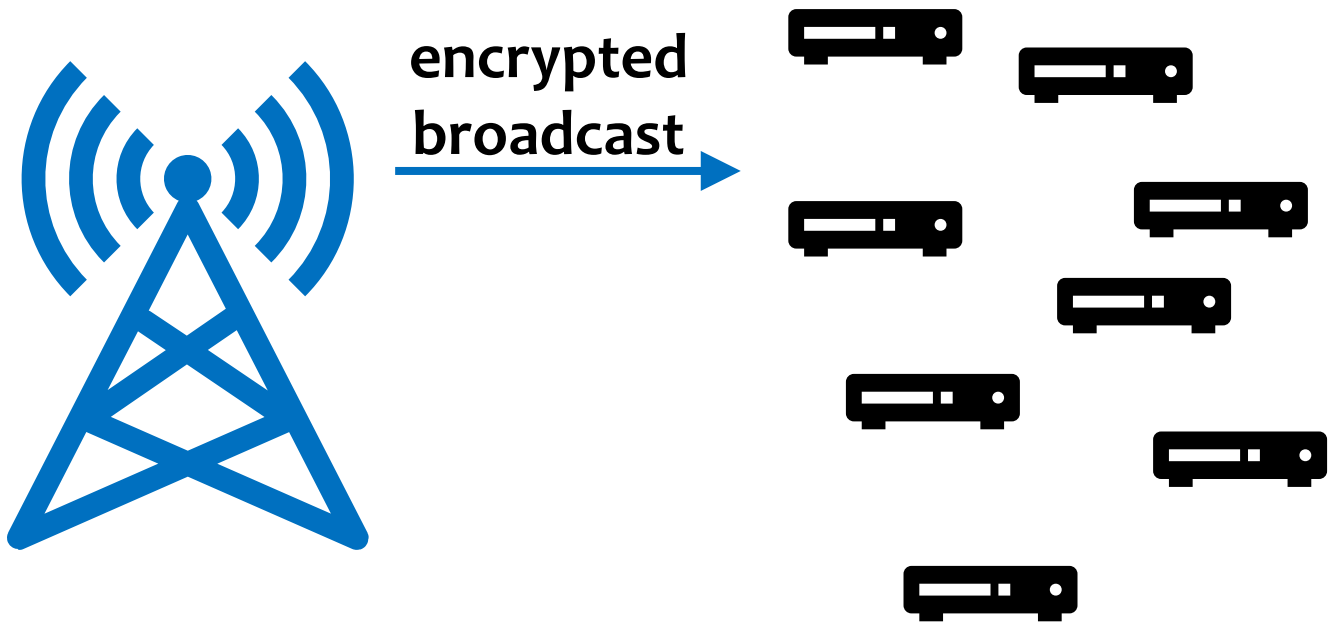
罗辑 (Ji Luo) ✉

UNIVERSITY of WASHINGTON

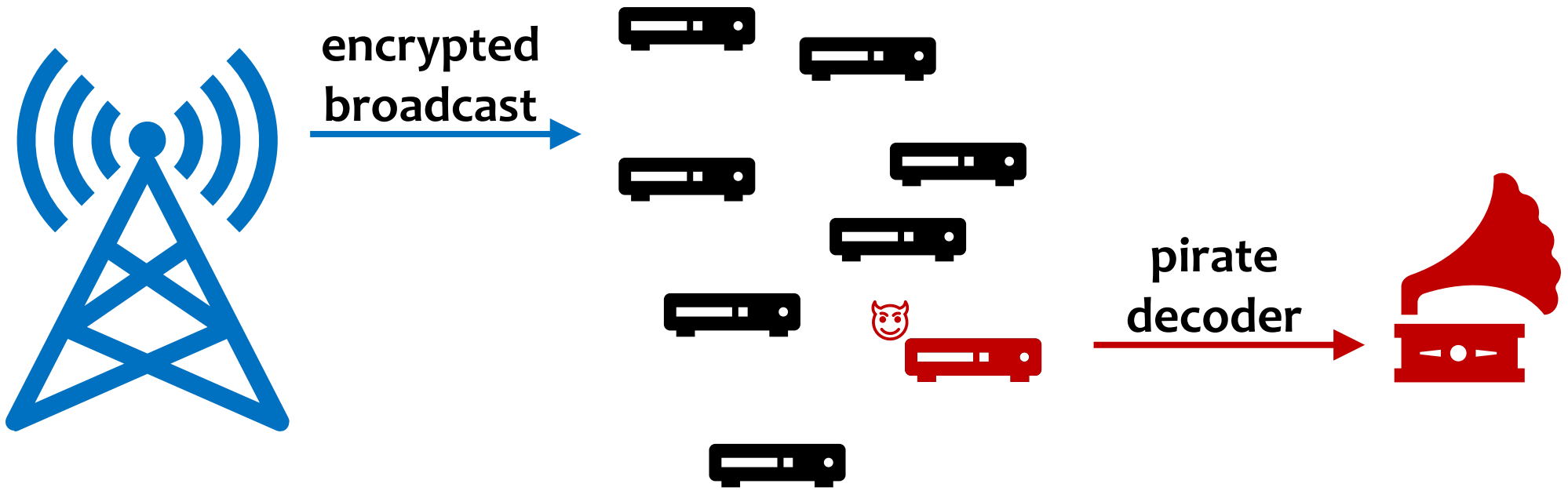
Hoeteck Wee ✉

NTTResearch

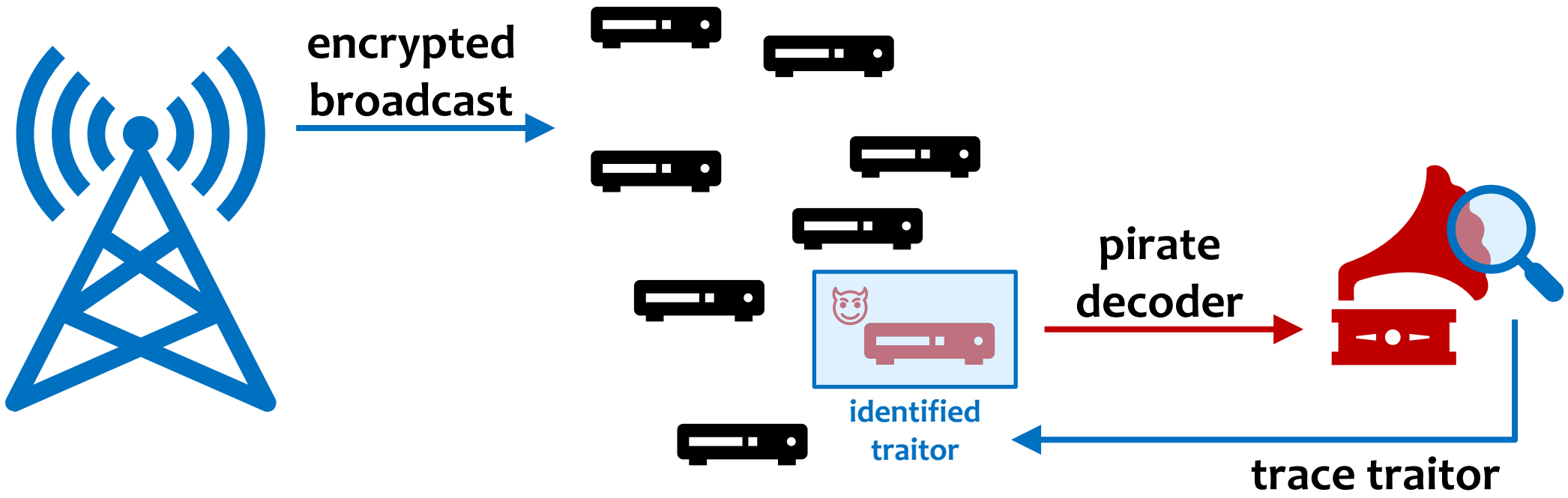
Traitor Tracing [CFN94]



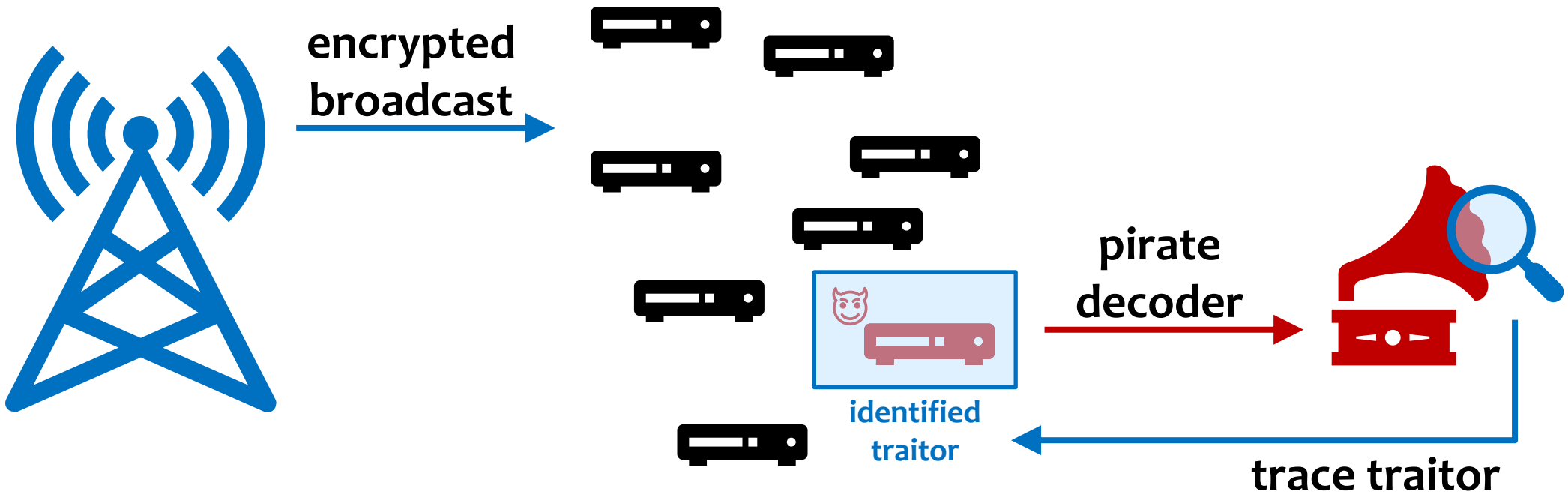
Traitor Tracing [CFN94]



Traitor Tracing [CFN94]

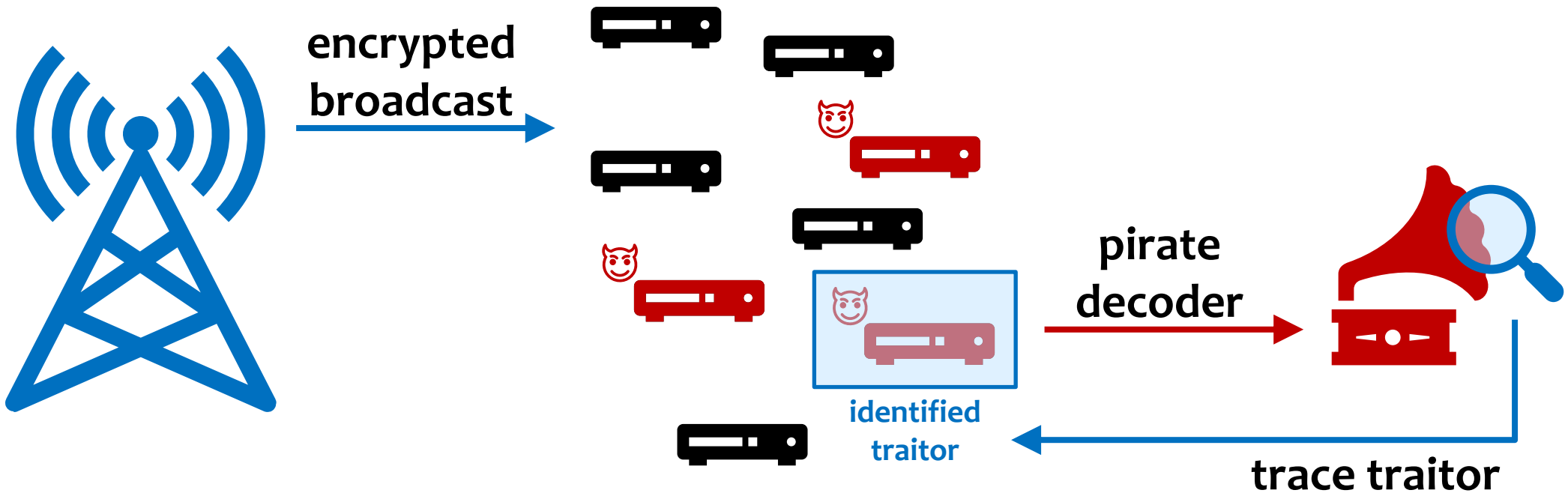


Traitor Tracing [CFN94]



- Can find **at least one traitor** as long as decoder breaks semantic security.
- **Never** accuses an **innocent** user.

Traitor Tracing [CFN94]

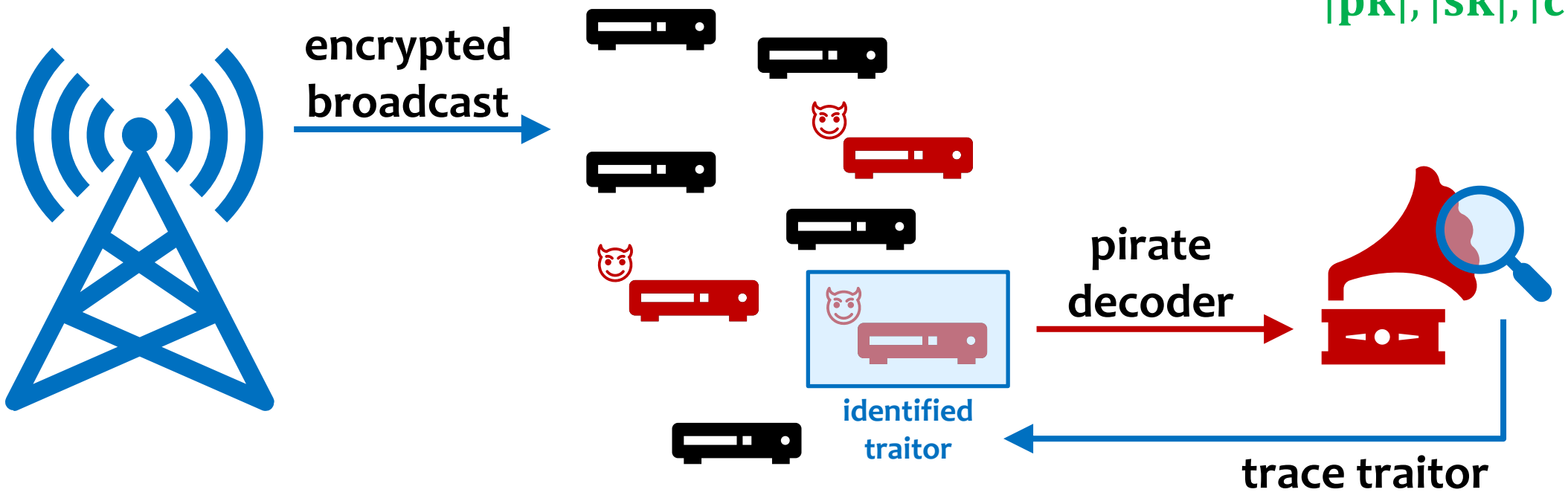


- Can find **at least one traitor** as long as decoder breaks semantic security.
- **Never** accuses an **innocent** user.
- Even if **arbitrarily** many users **collude**.

Traitor Tracing [CFN94]

minimize communication/storage overhead

$|pk|, |sk|, |ct|$



- Can find **at least one traitor** as long as decoder breaks semantic security.
- **Never** accuses an **innocent** user.
- Even if **arbitrarily** many users **collude**.

Traitor Tracing: Syntax

- $\mathrm{Gen}(1^N) \to \mathrm{pk}, \mathrm{sk}_1, \ldots, \mathrm{sk}_N, \mathrm{tk}$

Traitor Tracing: Syntax

- $\mathrm{Gen}(1^N) \to \mathrm{pk}, \mathrm{sk}_1, \ldots, \mathrm{sk}_N, \boxed{\mathrm{tk}}$ **private tracing**

Traitor Tracing: Syntax

- $\mathrm{Gen}(1^N) \to \mathrm{pk}, \mathrm{sk}_1, \ldots, \mathrm{sk}_N, \boxed{\mathrm{tk}}$ **private tracing**
- $\mathrm{Enc}(\mathrm{pk}) \to (\mathrm{ct}, \boxed{k})$ **KEM**

Traitor Tracing: Syntax

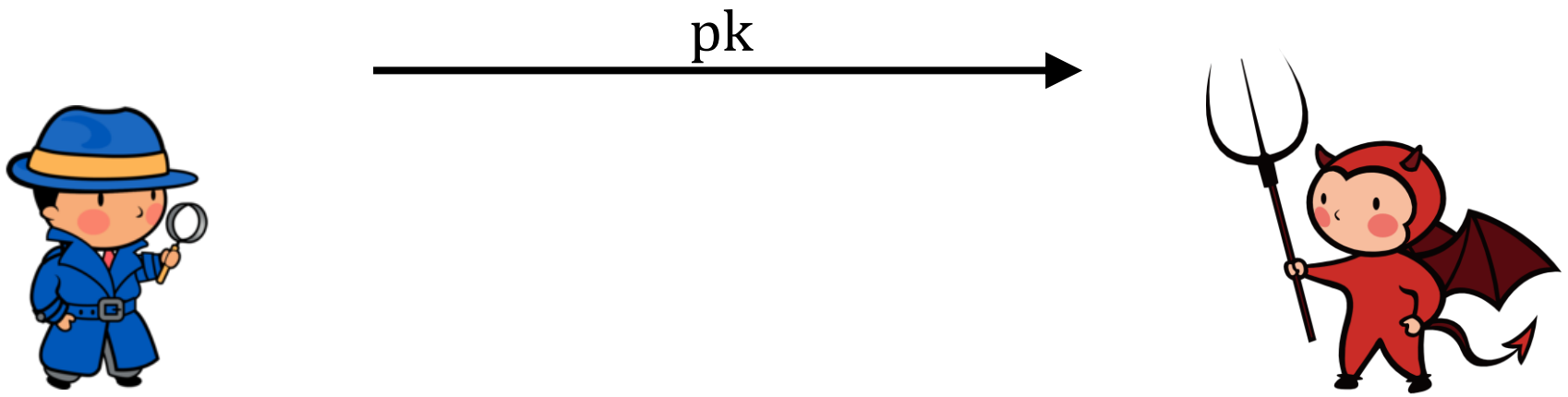
- $\mathrm{Gen}(1^N) \to \mathrm{pk}, \mathrm{sk}_1, \ldots, \mathrm{sk}_N, \boxed{\mathrm{tk}}$ **private tracing**
- $\mathrm{Enc}(\mathrm{pk}) \to (\mathrm{ct}, \boxed{k})$ **KEM**
- $\mathrm{Dec}(\boxed{\mathrm{pk}}, \mathrm{sk}_i, \mathrm{ct}) \to k$ **only count "truly secret" part in $|\mathrm{sk}|$ (minimize secret storage)**

Traitor Tracing: Syntax

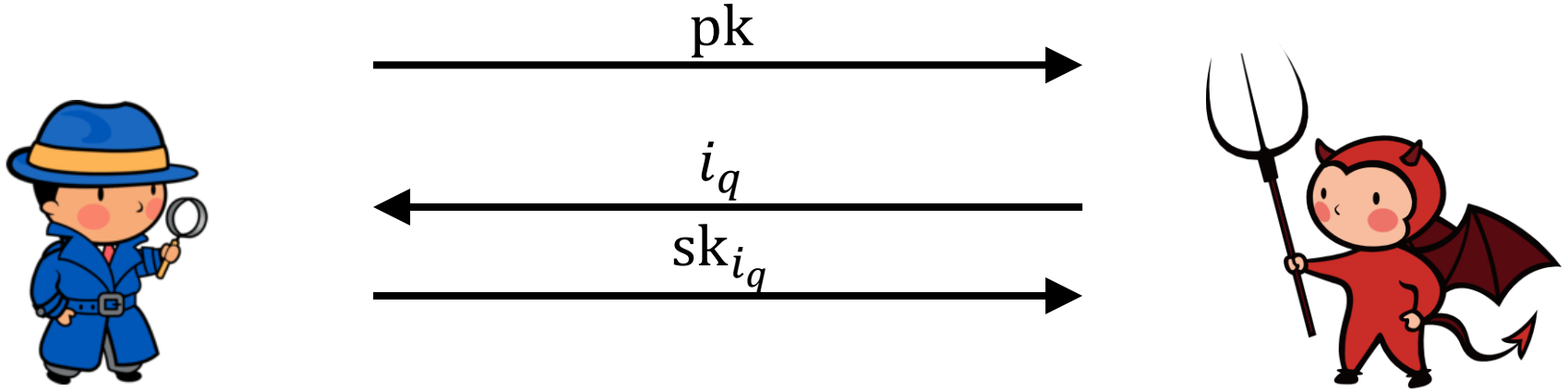
- $\mathrm{Gen}(1^N) \to \mathrm{pk}, \mathrm{sk}_1, \ldots, \mathrm{sk}_N, \boxed{\mathrm{tk}}$ **private tracing**
- $\mathrm{Enc}(\mathrm{pk}) \to (\mathrm{ct}, \boxed{k})$ **KEM**
- $\mathrm{Dec}(\boxed{\mathrm{pk}}, \mathrm{sk}_i, \mathrm{ct}) \to k$ **only count "truly secret" part in $|\mathrm{sk}|$ (minimize secret storage)**
- $\mathrm{Trace}^D(\mathrm{pk}, \mathrm{tk}, 1^{1/\varepsilon}) \to i^* \in [N] \cup \{\perp\}$

Traitor Tracing: Security

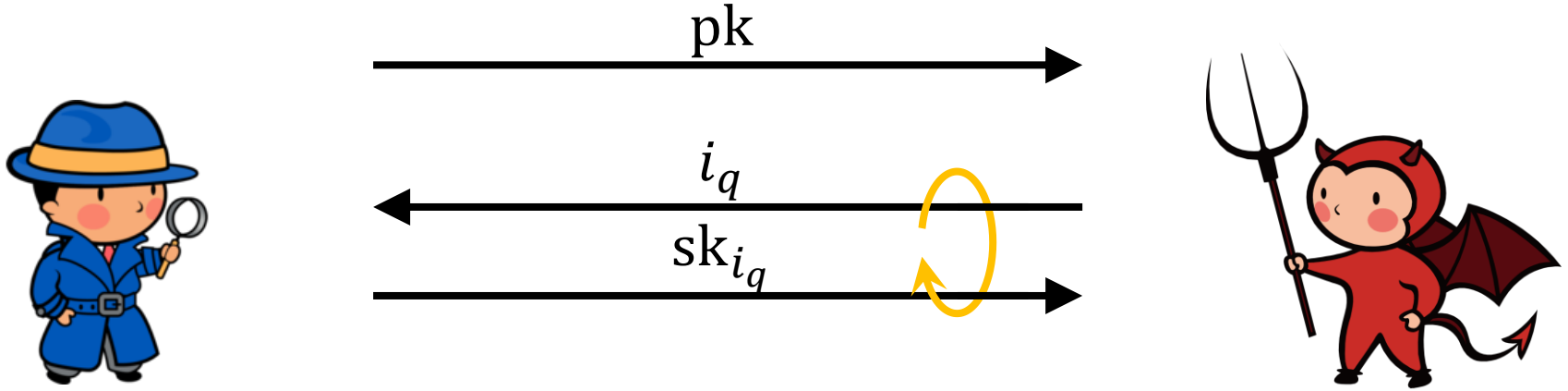
Traitor Tracing: Security



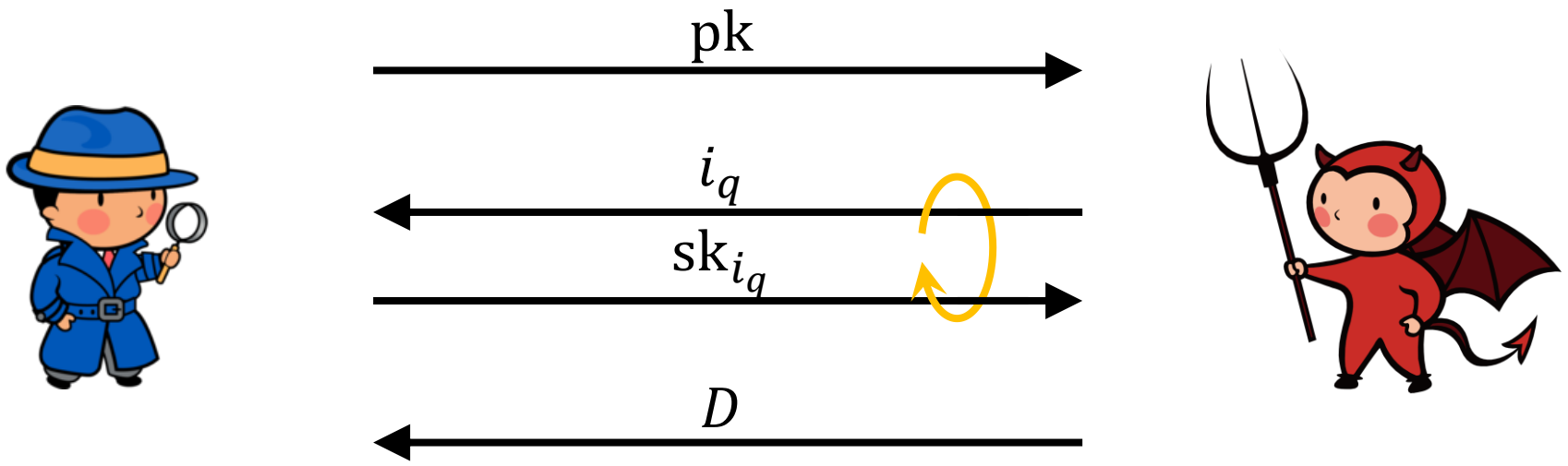
Traitor Tracing: Security



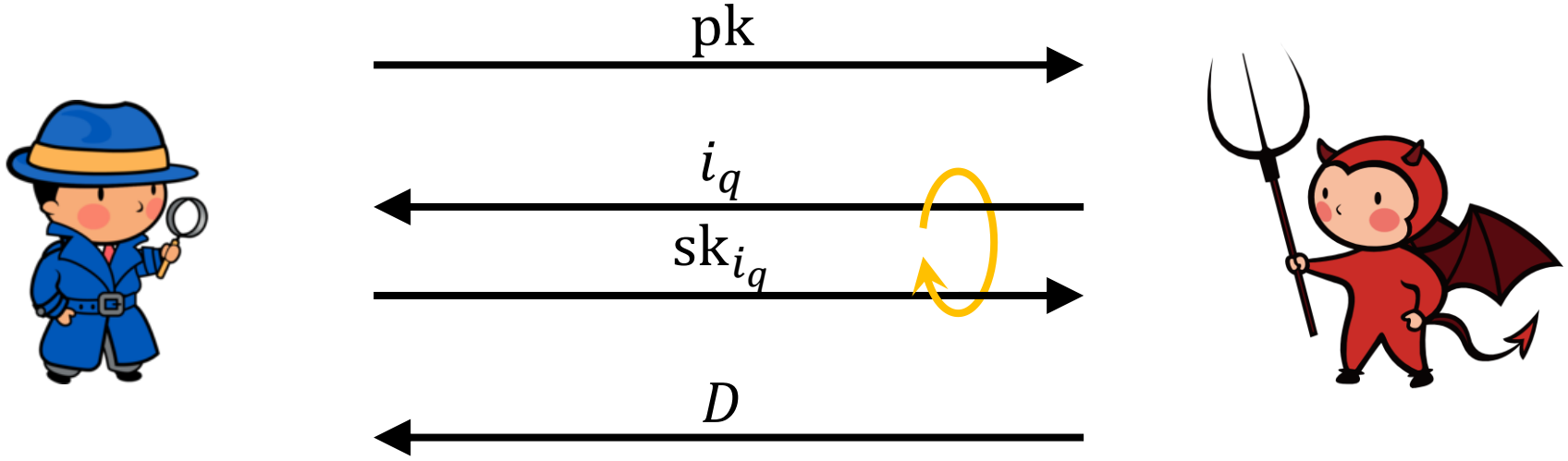
Traitor Tracing: Security



Traitor Tracing: Security



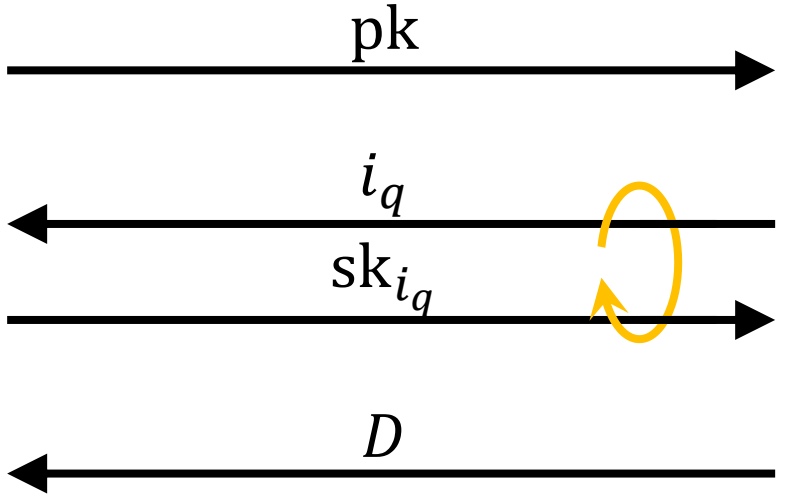
Traitor Tracing: Security



$$\varepsilon^* \stackrel{\text{def}}{=} \Pr\left[\begin{matrix} b, k_0 \leftarrow \$, \$ \\ (\mathrm{ct}, k_1) \leftarrow \mathrm{Enc}(\mathrm{pk}) \end{matrix} : D(\mathrm{ct}, k_b) = b\right] - \frac{1}{2}$$

$$i^* \leftarrow \mathrm{Trace}^D(\mathrm{pk}, \mathrm{tk}, 1^{1/\varepsilon})$$

Traitor Tracing: Security



wins if

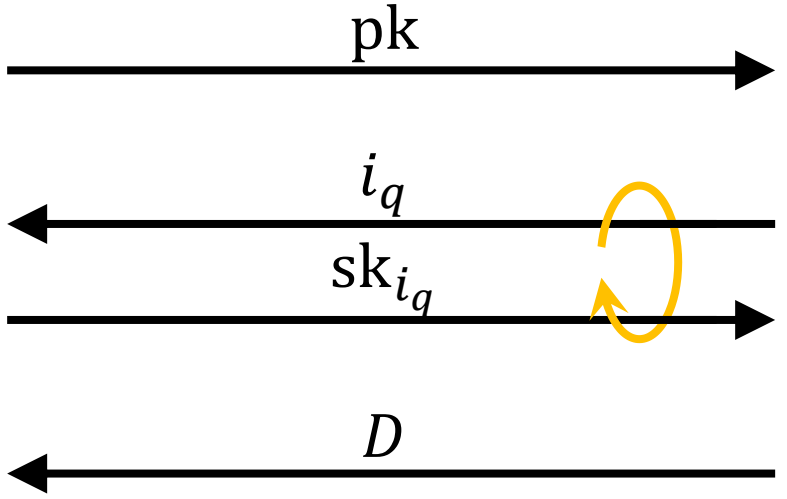
either $i^* \notin \{i_q\} \cup \{\perp\}$,

or $\varepsilon^* \geq \varepsilon$ and $i^* = \perp$.

$$\varepsilon^* \stackrel{\text{def}}{=} \Pr\left[\begin{matrix} b, k_0 \leftarrow \$, \$ \\ (\mathrm{ct}, k_1) \leftarrow \mathrm{Enc}(\mathrm{pk}) \end{matrix} : D(\mathrm{ct}, k_b) = b\right] - \frac{1}{2}$$

$$i^* \leftarrow \mathrm{Trace}^D(\mathrm{pk}, \mathrm{tk}, 1^{1/\varepsilon})$$

Traitor Tracing: Security



$$\varepsilon^* \stackrel{\text{def}}{=} \Pr\left[\begin{matrix} b, k_0 \leftarrow \$, \$ \\ (\mathrm{ct}, k_1) \leftarrow \mathrm{Enc}(\mathrm{pk}) \end{matrix} : D(\mathrm{ct}, k_b) = b\right] - \frac{1}{2}$$

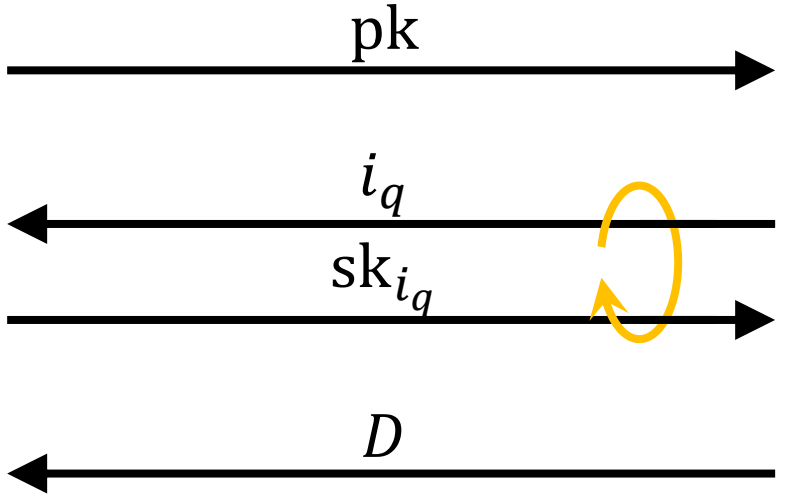
$$i^* \leftarrow \mathrm{Trace}^D(\mathrm{pk}, \mathrm{tk}, 1^{1/\varepsilon})$$

wins if

either $i^* \notin \{i_q\} \cup \{\perp\}$,
(honest user accused)

or $\varepsilon^* \geq \varepsilon$ and $i^* = \perp$.
(good decoder but no traitor found)

Traitor Tracing: Security



wins if

either $i^* \notin \{i_q\} \cup \{\perp\}$,

(honest user accused)

or $\varepsilon^* \geq \varepsilon$ and $i^* = \perp$.

(good decoder but no traitor found)

$$\varepsilon^* \stackrel{\text{def}}{=} \Pr\left[\begin{matrix} b, k_0 \leftarrow \$, \$ \\ (\mathrm{ct}, k_1) \leftarrow \mathrm{Enc}(\mathrm{pk}) \end{matrix} : D(\mathrm{ct}, k_b) = b\right] - \frac{1}{2}$$

$$i^* \leftarrow \mathrm{Trace}^D(\mathrm{pk}, \mathrm{tk}, 1^{1/\varepsilon})$$

Pr[ wins] ***negligible*** for all ***polynomial*** $N, 1/\varepsilon$

Traitor Tracing Schemes with Optimal Sizes

	$\|pk\|$	$\|sk\|$	$\|ct\|$	**tracing**	**assumption**
BZ14	$O(1)$			public	$i\mathcal{O}$
GKW18				private	LWE
CVWWW18				private	LWE

Traitor Tracing Schemes with Optimal Sizes

	$\|pk\|$	$\|sk\|$	$\|ct\|$	**tracing**	**assumption**
BZ14	$O(1)$			public	$i\mathcal{O}$
GKW18				private	LWE
CVWWW18				private	LWE

Traitor Tracing Schemes with Optimal Sizes

	$\|pk\|$	$\|sk\|$	$\|ct\|$	**tracing**	**assumption**
BZ14	$O(1)$			public	$i\mathcal{O}$
GKW18				private	LWE
CVWWW18				private	LWE

- **tracing from different assumptions**
- **exploration of techniques**

Traitor Tracing Schemes with Optimal Sizes

	$\|pk\|$	$\|sk\|$	$\|ct\|$	**tracing**	**assumption**
BZ14	$O(1)$			public	$i\mathcal{O}$
GKW18				private	LWE
CVWWW18				private	LWE

- **deployment-friendly**

pairing

- **tracing from different assumptions**
- **exploration of techniques**

Existing Traitor Tracing Schemes from Pairing

	$\lvert pk \rvert$	$\lvert sk \rvert$	$\lvert ct \rvert$	**tracing**	**assumption**
BSW06 + Z20	1	1	N	public	IBE
BN08/BP08 + Z20	1	N^2	1	private	IBE
BSW06	$\sqrt{N}$	1	$\sqrt{N}$	private	composite
BSW06 + W20	$\sqrt{N}$	1	$\sqrt{N}$	public	bi-k-Lin

Existing Traitor Tracing Schemes from Pairing

	$\lvert pk \rvert$	$\lvert sk \rvert$	$\lvert ct \rvert$	**tracing**	**assumption**
BSW06 + Z20	1	1	N	public	IBE
BN08/BP08 + Z20	1	N^2	1	private	IBE
BSW06	$\sqrt{N}$	1	$\sqrt{N}$	private	composite
BSW06 + W20	$\sqrt{N}$	1	$\sqrt{N}$	public	bi-k-Lin
Z20	$\sqrt[3]{N}$	$\sqrt[3]{N}$	$\sqrt[3]{N}$	private	GGM

+ more trade-offs

Existing Traitor Tracing Schemes from Pairing

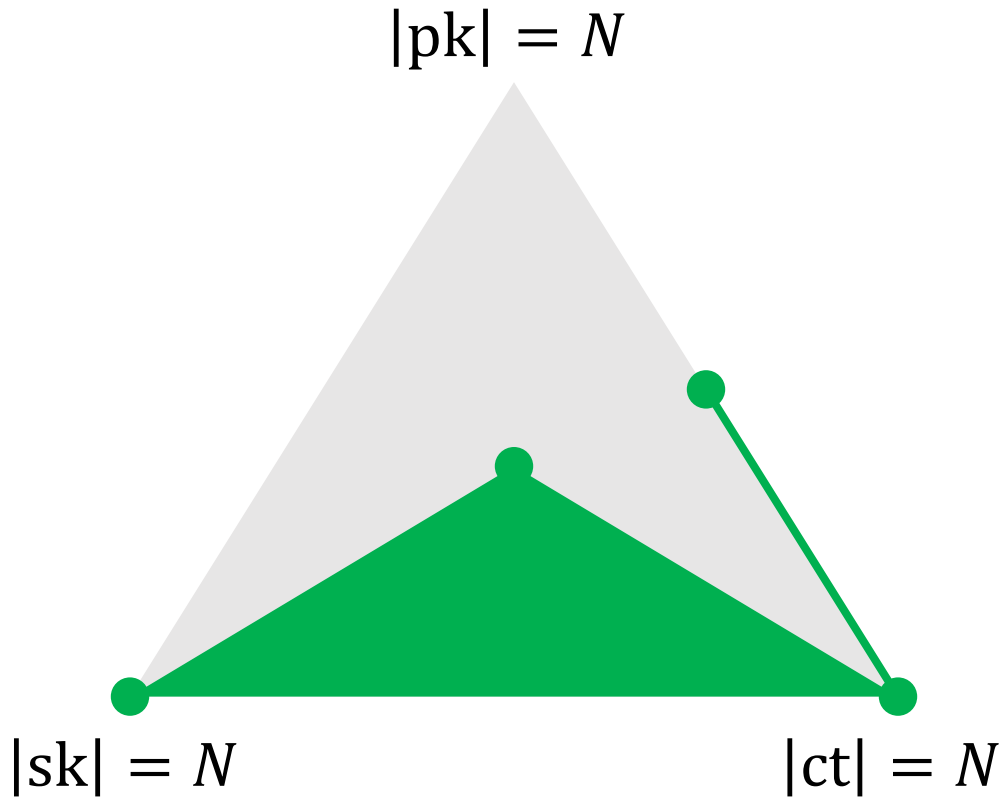
	$\lvert pk \rvert$	$\lvert sk \rvert$	$\lvert ct \rvert$	**tracing**	**assumption**
BSW06 + Z20	1	1	N	public	IBE
BN08/BP08 + Z20	1	N^2	1	private	IBE
BSW06	$\sqrt{N}$	1	$\sqrt{N}$	private	composite
BSW06 + W20	$\sqrt{N}$	1	$\sqrt{N}$	public	bi-k-Lin
Z20	$\sqrt[3]{N}$	$\sqrt[3]{N}$	$\sqrt[3]{N}$	private	GGM

+ more trade-offs

But $\lvert pk \rvert \times \lvert sk \rvert \times \lvert ct \rvert \geq N$ for all schemes so far!

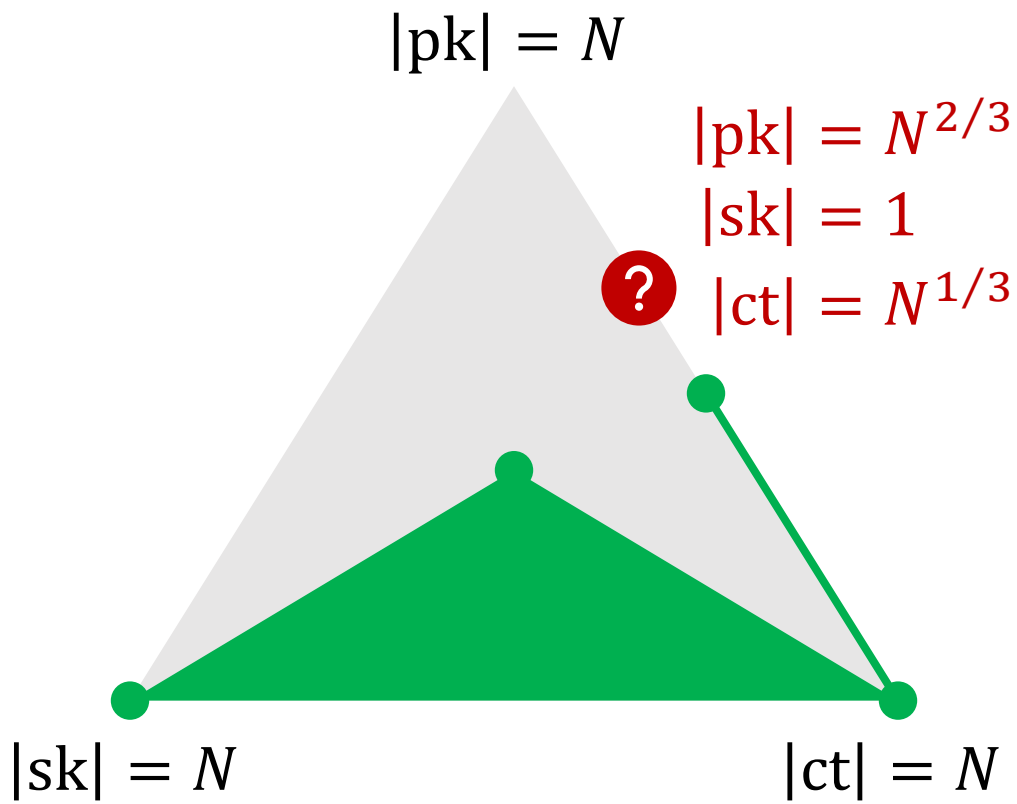
Traitor Tracing from Pairing: Trade-Off Simplices

$|\mathrm{pk}| \times |\mathrm{sk}| \times |\mathrm{ct}| = N$ **simplex** [Z20]



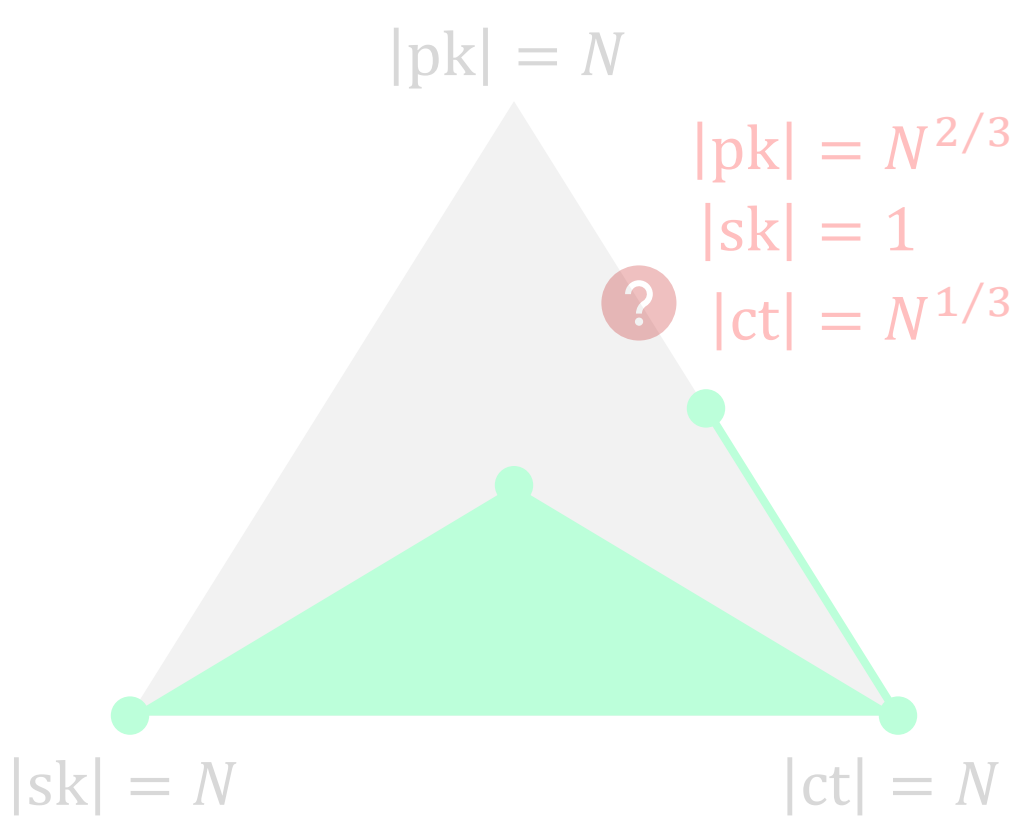
Traitor Tracing from Pairing: Trade-Off Simplices

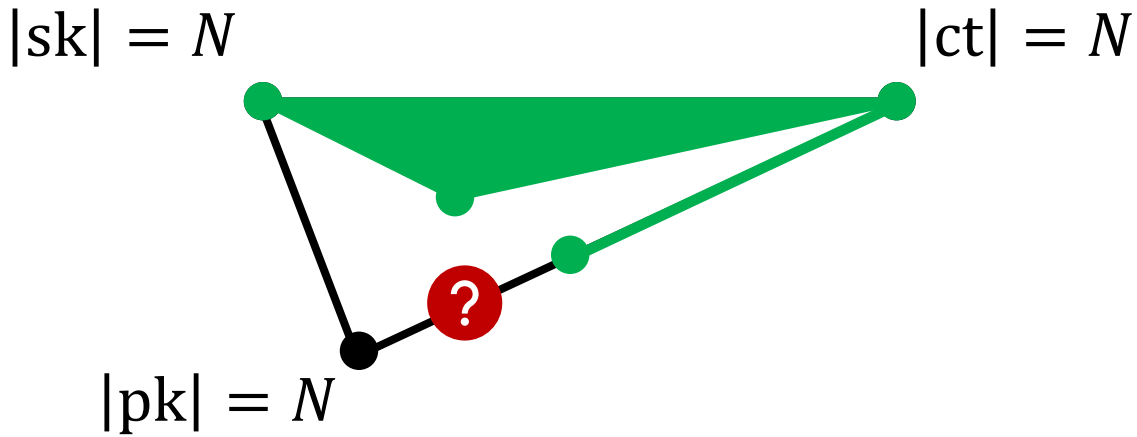
$|\mathrm{pk}| \times |\mathrm{sk}| \times |\mathrm{ct}| = N$ **simplex** [Z20]



Traitor Tracing from Pairing: Trade-Off Simplices

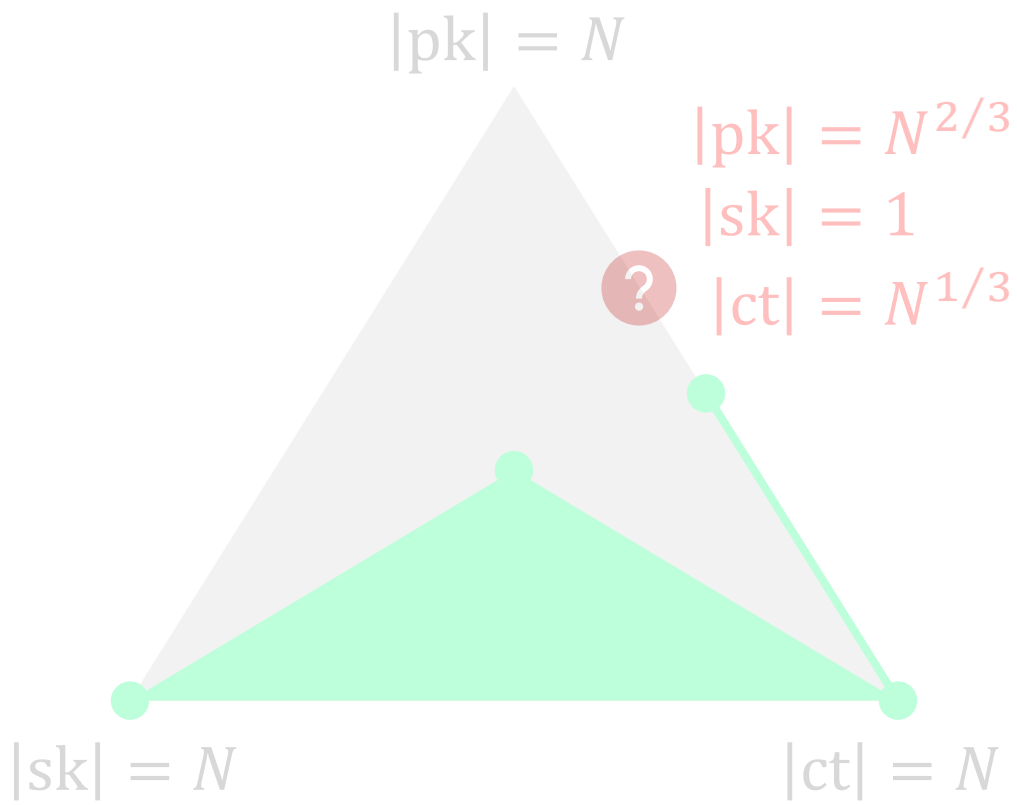
$|\mathrm{pk}| \times |\mathrm{sk}| \times |\mathrm{ct}| = N$ **simplex** [Z20]



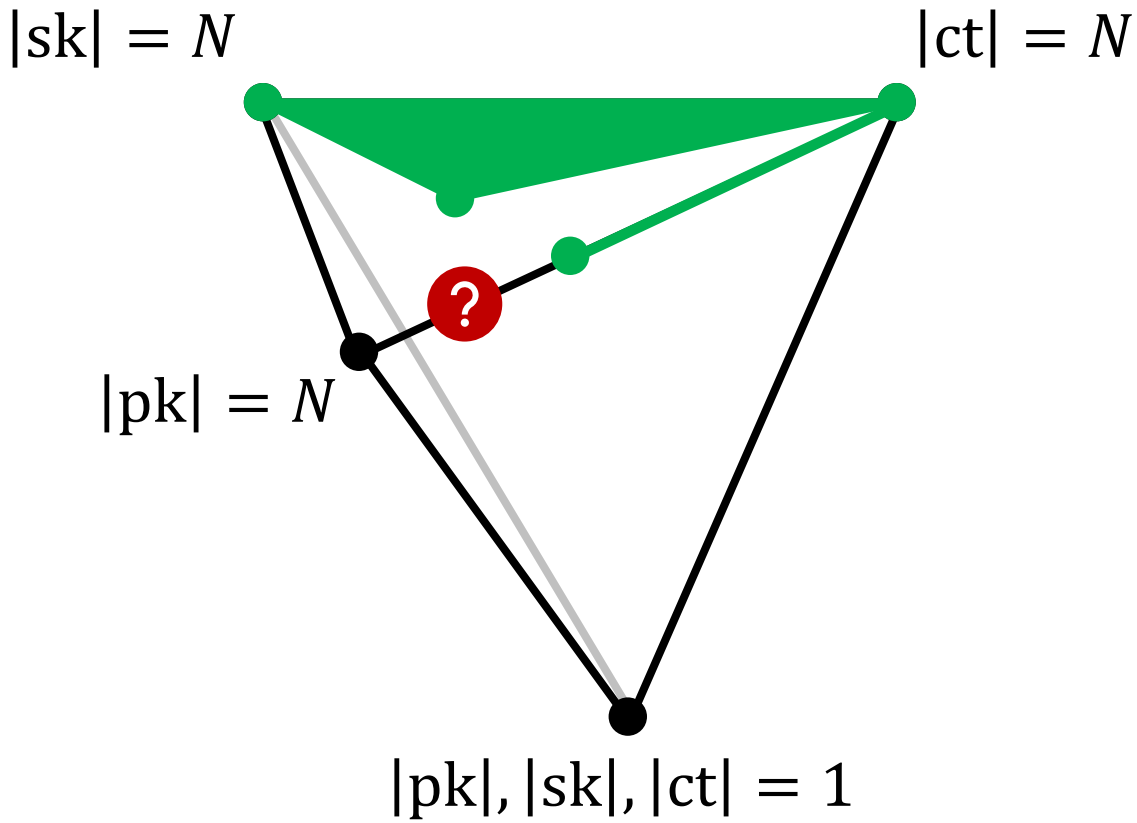


Traitor Tracing from Pairing: Trade-Off Simplices

$|\mathrm{pk}| \times |\mathrm{sk}| \times |\mathrm{ct}| = N$ **simplex** [Z20]

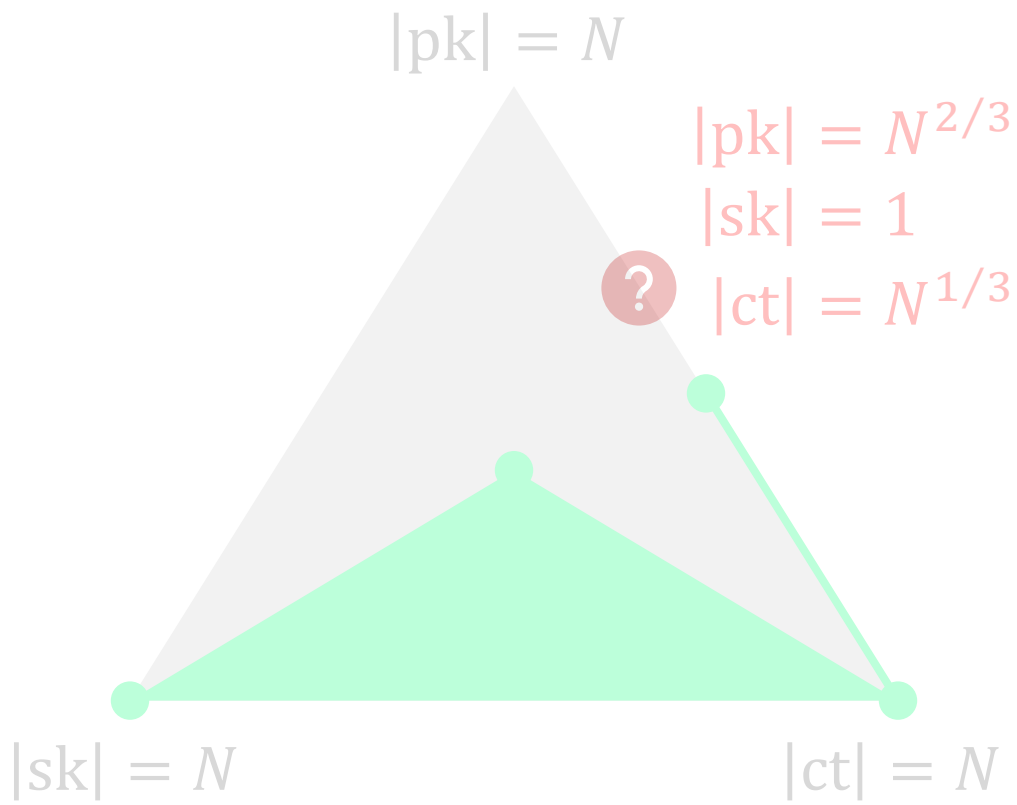


$1 \leq |\mathrm{pk}| \times |\mathrm{sk}| \times |\mathrm{ct}| \leq N$ **simplex**

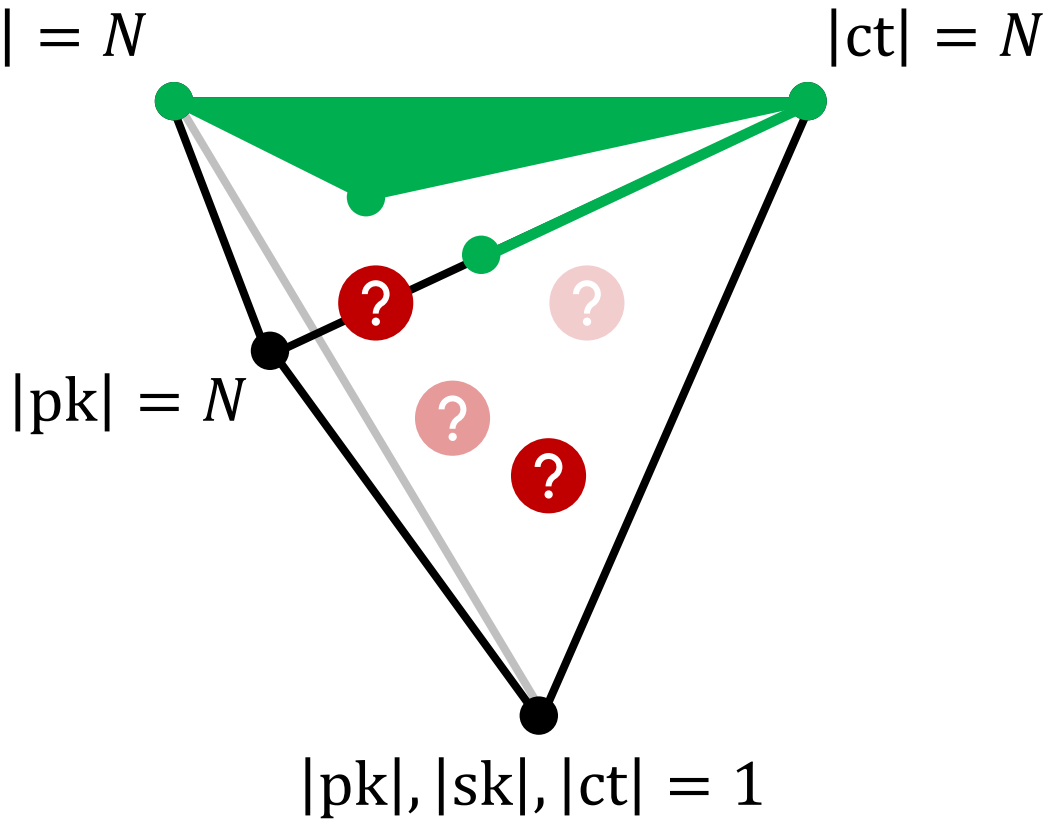


Traitor Tracing from Pairing: Trade-Off Simplices

$|\mathrm{pk}| \times |\mathrm{sk}| \times |\mathrm{ct}| = N$ **simplex** [Z20]

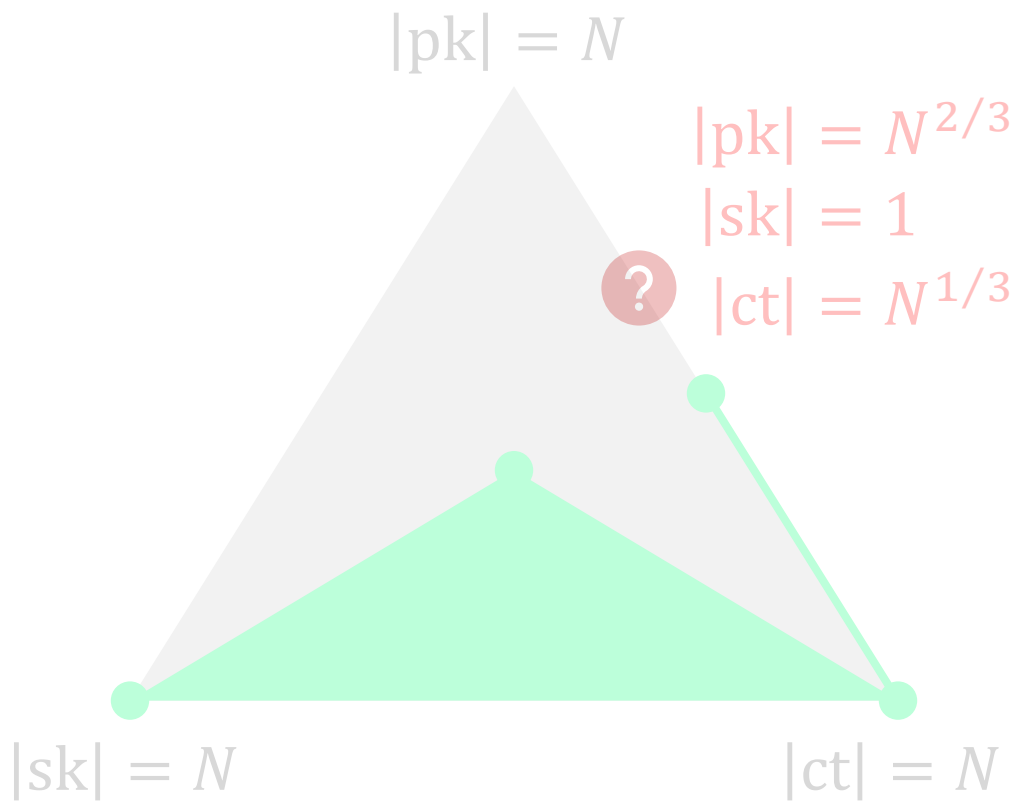


$1 \leq |\mathrm{pk}| \times |\mathrm{sk}| \times |\mathrm{ct}| \leq N$ **simplex**

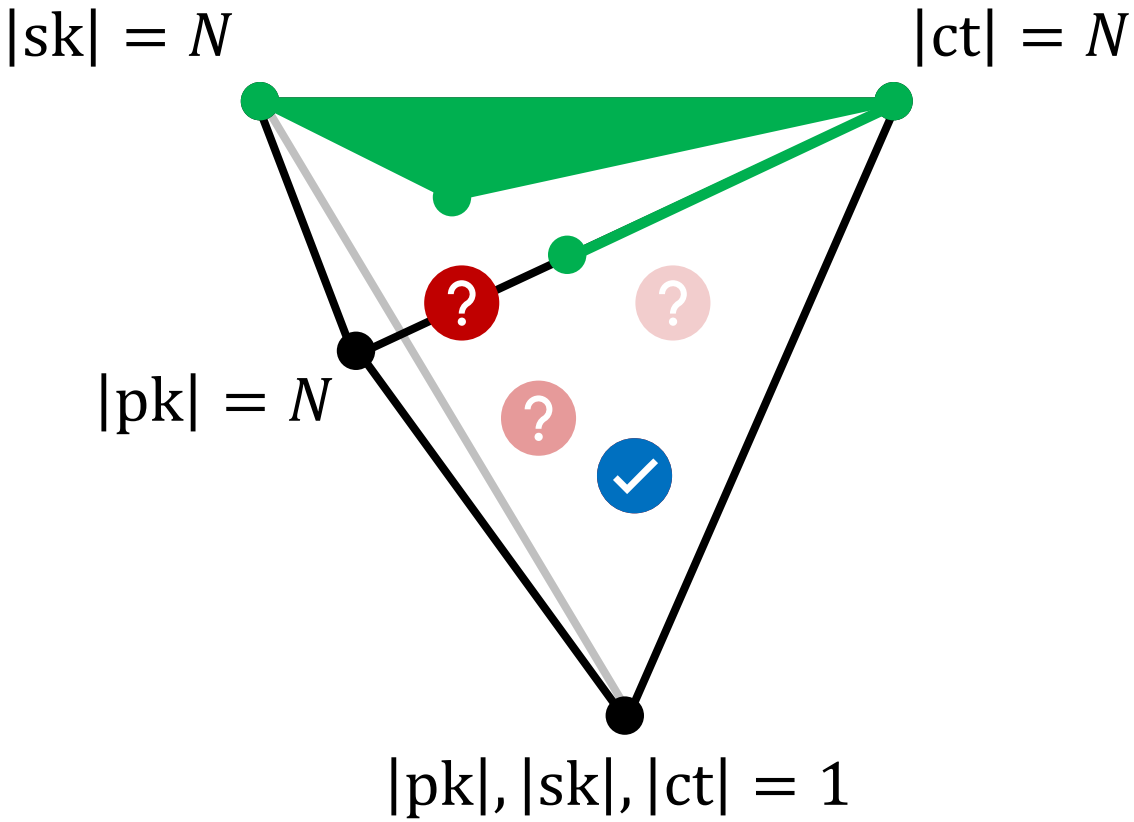


Traitor Tracing from Pairing: Trade-Off Simplices

$|\mathrm{pk}| \times |\mathrm{sk}| \times |\mathrm{ct}| = N$ **simplex** [Z20]



$1 \leq |\mathrm{pk}| \times |\mathrm{sk}| \times |\mathrm{ct}| \leq N$ **simplex**

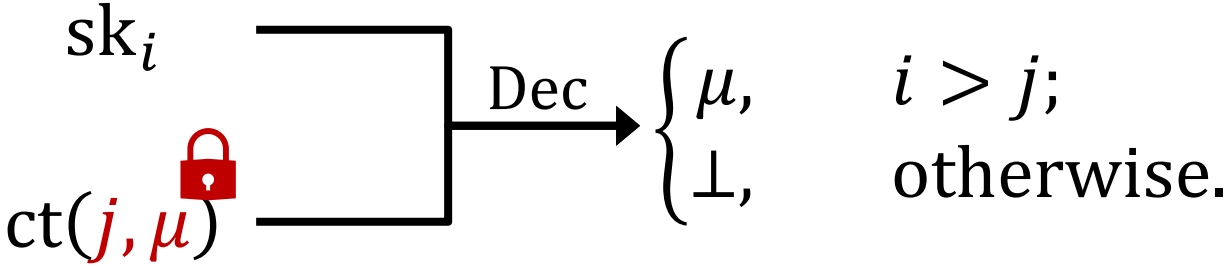


Our Results

	|pk|	|sk|	|ct|	**tracing**	**assumption**
this	$\sqrt[3]{N}$	**1**	$\sqrt[3]{N}$	**private**	**bi-k-Lin**
BSW06	$\sqrt{N}$	1	$\sqrt{N}$	private	composite
BSW06 + W20	$\sqrt{N}$	1	$\sqrt{N}$	public	bi-k-Lin
Z20	$\sqrt[3]{N}$	$\sqrt[3]{N}$	$\sqrt[3]{N}$	private	GGM

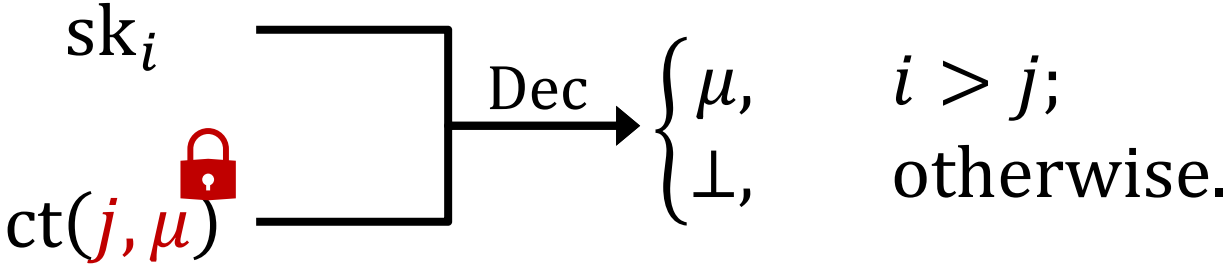
Quick Recap: Traitor Tracing from PLBE [BSW06]

Private Linear Broadcast Encryption



Quick Recap: Traitor Tracing from PLBE [BSW06]

Private Linear Broadcast Encryption



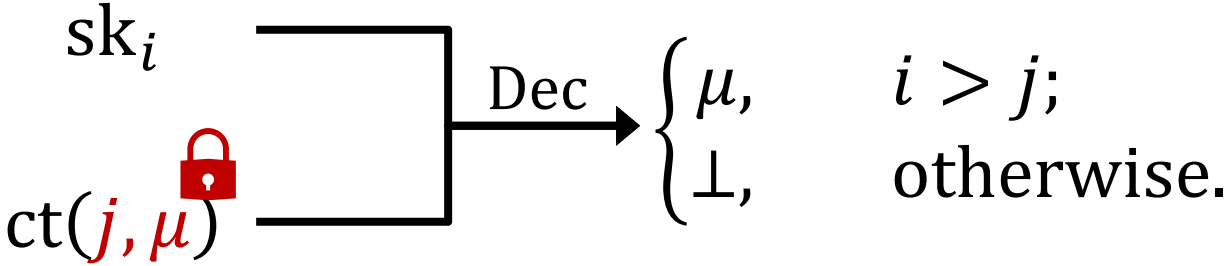
Traitor Tracing from PLBE

$$\mathrm{TTsk}_i = \mathrm{PLBEsk}_i$$

$$\mathrm{TTct}(\mu) = \mathrm{PLBEct}(0, \mu)$$

Quick Recap: Traitor Tracing from PLBE [BSW06]

Private Linear Broadcast Encryption



Traitor Tracing from PLBE

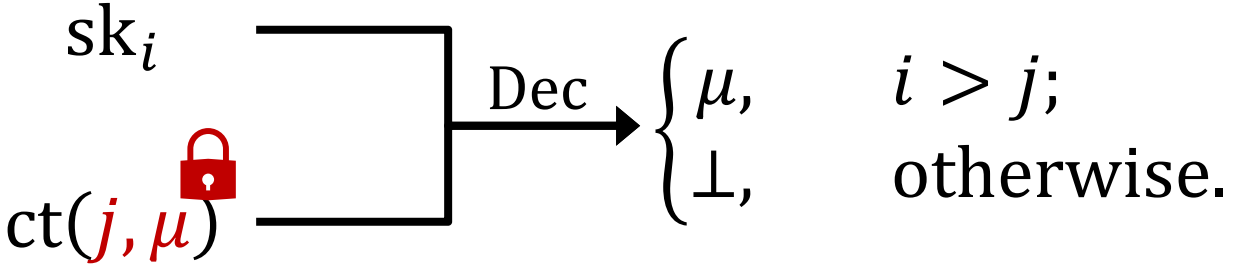
$$\mathrm{TTsk}_i = \mathrm{PLBEsk}_i$$

$$\mathrm{TTct}(\mu) = \mathrm{PLBEct}(0, \mu) \quad \cdots \quad \mathrm{PLBEct}(i-1, \mu) \quad \mathrm{PLBEct}(i, \mu) \quad \cdots \quad \mathrm{PLBEct}(N, \mu)$$

$$\geq \varepsilon$$

Quick Recap: Traitor Tracing from PLBE [BSW06]

Private Linear Broadcast Encryption



1

$$\mathrm{ct}(N, \mu) \approx \mathrm{ct}(N, 0) \text{ given } \mathrm{sk}_1, \ldots, \mathrm{sk}_N$$

Traitor Tracing from PLBE

$$\mathrm{TTsk}_i = \mathrm{PLBEsk}_i$$

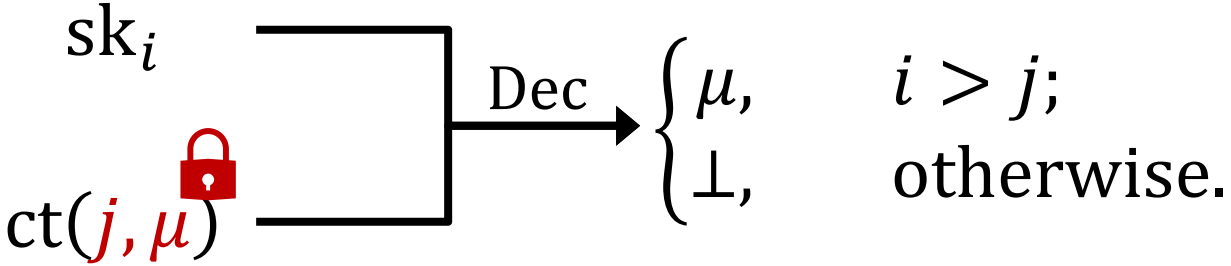
$$\mathrm{TTct}(\mu) = \mathrm{PLBEct}(0, \mu) \quad \cdots \quad \mathrm{PLBEct}(i-1, \mu) \quad \mathrm{PLBEct}(i, \mu) \quad \cdots \quad \mathrm{PLBEct}(N, \mu)$$

$$\geq \varepsilon$$

By (1), ≈ 0;
total gap of $\Omega(\varepsilon)$.

Quick Recap: Traitor Tracing from PLBE [BSW06]

Private Linear Broadcast Encryption



1. $\mathrm{ct}(N,\mu) \approx \mathrm{ct}(N,0)$ given $\mathrm{sk}_1, \ldots, \mathrm{sk}_N$

2. $\mathrm{ct}(i-1,\mu) \approx \mathrm{ct}(i,\mu)$ given $\mathrm{sk}_{\neq i}$'s

Traitor Tracing from PLBE

$$\mathrm{TTsk}_i = \mathrm{PLBEsk}_i$$

$$\mathrm{TTct}(\mu) = \mathrm{PLBEct}(0,\mu) \quad \cdots \quad \mathrm{PLBEct}(i-1,\mu) \quad \mathrm{PLBEct}(i,\mu) \quad \cdots \quad \mathrm{PLBEct}(N,\mu)$$

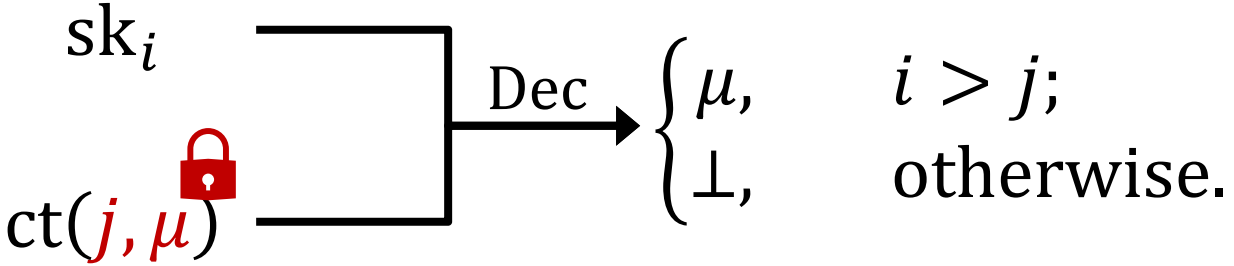
$\geq \varepsilon$

By (2), if user i is honest, then $\Delta\varepsilon_i \approx 0$;

By (1), ≈ 0;
total gap of $\Omega(\varepsilon)$.

Quick Recap: Traitor Tracing from PLBE [BSW06]

Private Linear Broadcast Encryption



1. $\mathrm{ct}(N,\mu) \approx \mathrm{ct}(N,0)$ given $\mathrm{sk}_1, \ldots, \mathrm{sk}_N$

2. $\mathrm{ct}(i-1,\mu) \approx \mathrm{ct}(i,\mu)$ given $\mathrm{sk}_{\neq i}$'s

Traitor Tracing from PLBE

$$\mathrm{TTsk}_i = \mathrm{PLBEsk}_i$$

$$\mathrm{TTct}(\mu) = \mathrm{PLBEct}(0,\mu) \quad \cdots \quad \mathrm{PLBEct}(i-1,\mu) \quad \mathrm{PLBEct}(i,\mu) \quad \cdots \quad \mathrm{PLBEct}(N,\mu)$$

$$\geq \varepsilon$$

By (2), if user i is honest, then $\Delta\varepsilon_i \approx 0$;
if $\Delta\varepsilon_i = \Omega(\varepsilon/N)$, then user i is a traitor.

By (1), ≈ 0;
total gap of $\Omega(\varepsilon)$.

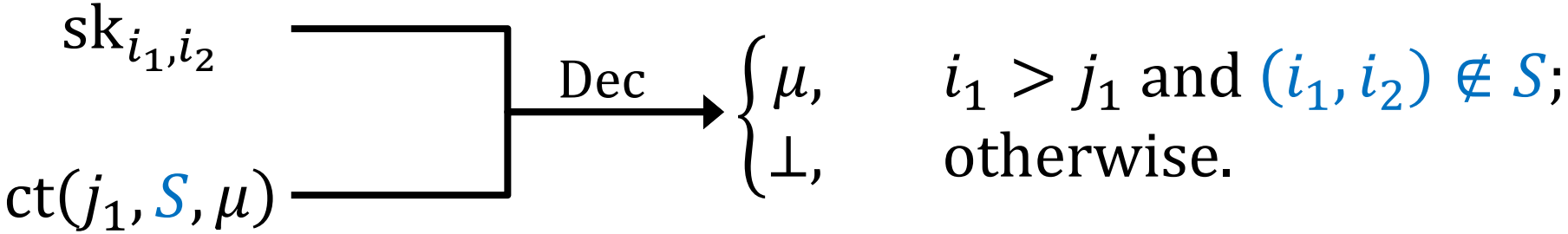
Revocable PLBE

Two Revocation Mechanisms: Index/Set Revocation

Revocable PLBE

Two Revocation Mechanisms: Index/Set Revocation

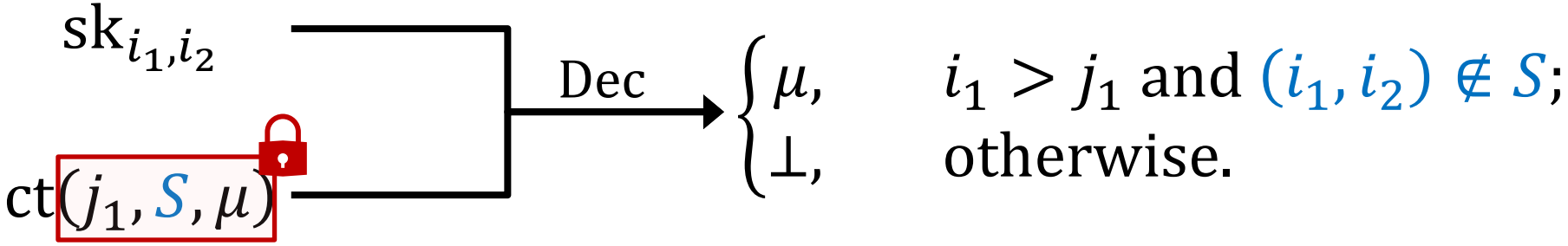
identity space $[N_1] \times [N_2]$



Revocable PLBE

Two Revocation Mechanisms: Index/Set Revocation

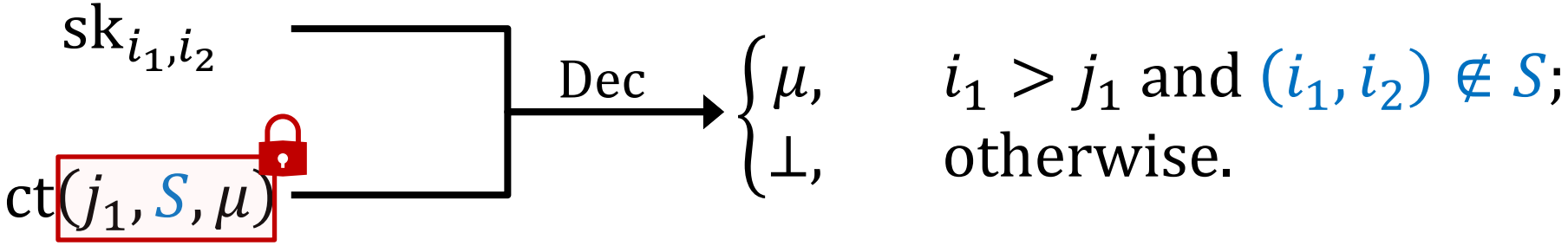
identity space $[N_1] \times [N_2]$



Revocable PLBE

Two Revocation Mechanisms: Index/Set Revocation

identity space $[N_1] \times [N_2]$



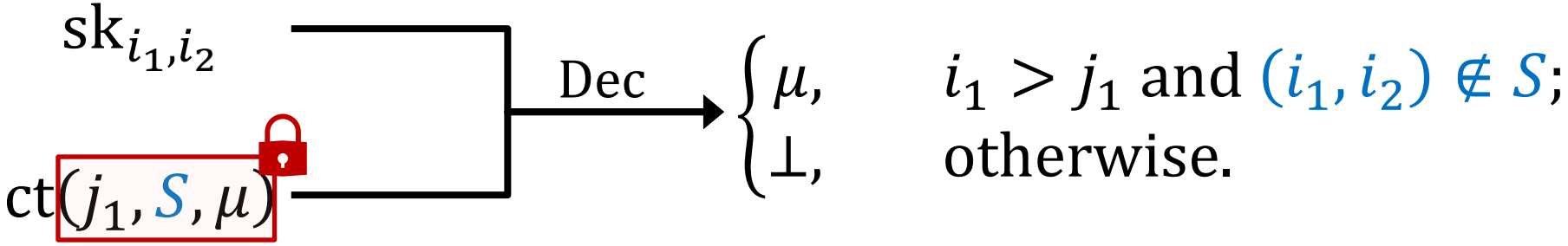
message-hiding

$\mathrm{ct}(N_1, \emptyset, \mu) \approx \mathrm{ct}(N_1, \emptyset, 0)$
given all sk's

Revocable PLBE

Two Revocation Mechanisms: Index/Set Revocation

identity space $[N_1] \times [N_2]$



message-hiding

$\mathrm{ct}(N_1, \emptyset, \mu) \approx \mathrm{ct}(N_1, \emptyset, 0)$
given all sk's

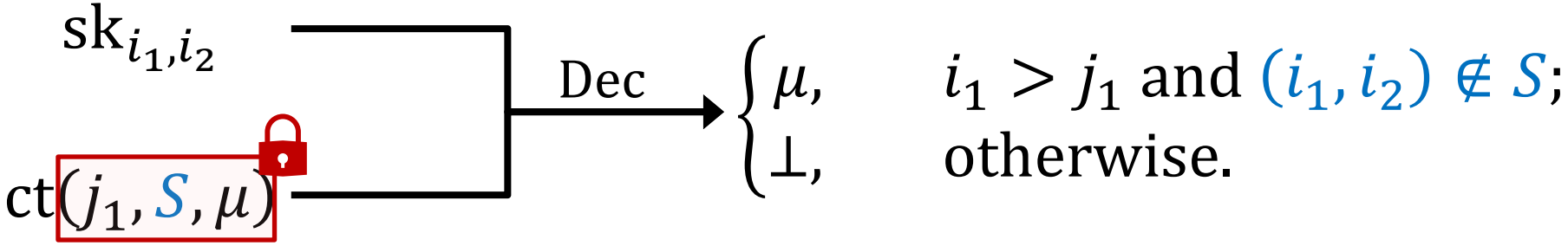
index-hiding

$\mathrm{ct}(i_1 - 1, S, \mu) \approx \mathrm{ct}(i_1, S, \mu)$
given $\mathrm{sk}_{\neq i_1,\star}$'s and $\mathrm{sk}_{\in S}$'s

Revocable PLBE

Two Revocation Mechanisms: Index/Set Revocation

identity space $[N_1] \times [N_2]$



message-hiding

$\mathrm{ct}(N_1, \emptyset, \mu) \approx \mathrm{ct}(N_1, \emptyset, 0)$
given all sk's

index-hiding

$\mathrm{ct}(i_1 - 1, S, \mu) \approx \mathrm{ct}(i_1, S, \mu)$
given $\mathrm{sk}_{\neq i_1, \star}$'s and $\mathrm{sk}_{\in S}$'s

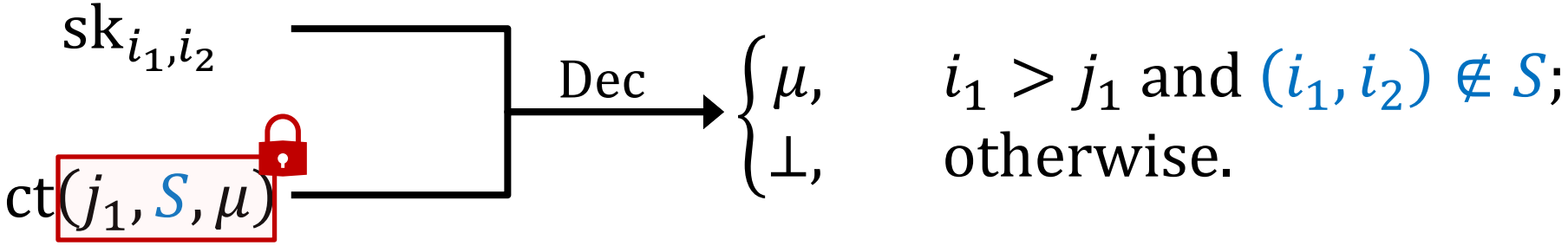
set-hiding

$\mathrm{ct}(i_1, S_0, \mu) \approx \mathrm{ct}(i_1, S_1, \mu)$
given $\mathrm{sk}_{\notin S_0 \oplus S_1}$'s

Revocable PLBE and Traitor Tracing

Two Revocation Mechanisms: Index/Set Revocation

identity space $[N_1] \times [N_2]$

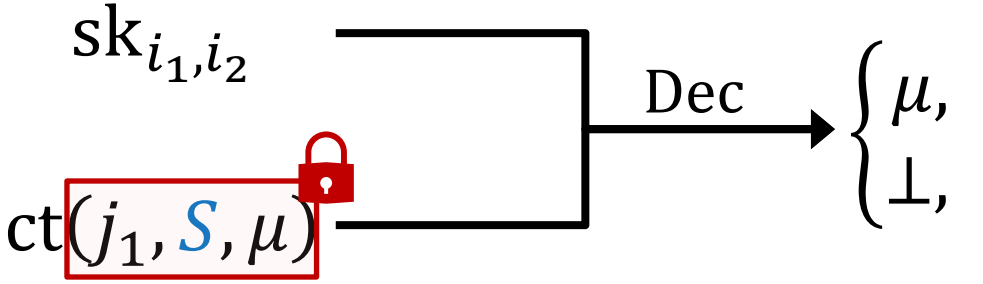


implies traitor tracing for $N = N_1 N_2$ users

Revocable PLBE and Traitor Tracing

Two Revocation Mechanisms: Index/Set Revocation

identity space $[N_1] \times [N_2]$



implies traitor tracing for $N = N_1 N_2$ users

tracing (similar to [Z20])

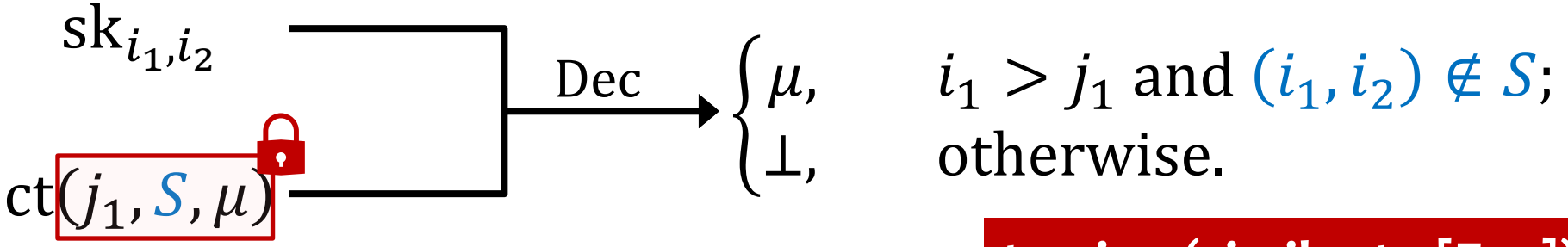
index-hiding $\Leftrightarrow$ finding i_1^*

set-hiding $\Leftrightarrow$ finding i_2^*

Revocable PLBE and Traitor Tracing

Two Revocation Mechanisms: Index/Set Revocation

identity space $[N_1] \times [N_2]$



tracing (similar to [Z20])

index-hiding $\Leftrightarrow$ finding i_1^*

set-hiding $\Leftrightarrow$ finding i_2^*

implies traitor tracing for $N = N_1 N_2$ users

Ours. $|\mathrm{pk}|, |\mathrm{ct}| = \sqrt{N_1} + N_2, \quad |\mathrm{sk}| = O(1)$.

Optimal Balancing. $N_1 = N^{2/3}, \quad N_2 = N^{1/3}$.

Relaxation and Threshold Broadcast PLBE

Relaxation and Threshold Broadcast PLBE

Relaxation 1.

- Encrypting to $S = \emptyset$ only uses mpk.
- Encrypting to $S \neq \emptyset$ uses msk.

Relaxation and Threshold Broadcast PLBE

Relaxation 1.

- Encrypting to $S = \emptyset$ only uses mpk.
- Encrypting to $S \neq \emptyset$ uses msk.

Relaxation 2.

- Encryption to S is adversary-dependent.

Relaxation and Threshold Broadcast PLBE

Relaxation 1.

- Encrypting to $S = \emptyset$ only uses mpk.
- Encrypting to $S \neq \emptyset$ uses msk.

Relaxation 2.

- Encryption to S is adversary-dependent.

Implementation. Combine PLBE and Threshold Broadcast [Z20].

$$\mathrm{Dec}\left(\mathrm{sk}_{i_1,i_2,u_{i_1,i_2}}, \mathrm{ct}_{r_1,\ldots,r_{N_2}}(j_1,\mu)\right)$$

$$= \begin{cases} \mu, & i_1 > j_1 \text{ and } \mathrm{HammingWeight}\left(r_{i_2} \oplus u_{i_1,i_2}\right) \geq 2\lambda/5 \\ \perp, & \text{otherwise.} \end{cases};$$

Relaxation and Threshold Broadcast PLBE

Relaxation 1.

- Encrypting to $S = \emptyset$ only uses mpk.
- Encrypting to $S \neq \emptyset$ uses msk.

Relaxation 2.

- Encryption to S is adversary-dependent.

Implementation. Combine PLBE and Threshold Broadcast [Z20].

$$\mathrm{Dec}\left(\mathrm{sk}_{i_1,i_2,u_{i_1,i_2}}, \mathrm{ct}_{r_1,\ldots,r_{N_2}}(j_1,\mu)\right)$$

$$= \begin{cases} \mu, & i_1 > j_1 \text{ and } \mathrm{HammingWeight}\left(r_{i_2} \oplus u_{i_1,i_2}\right) \geq 2\lambda/5 \\ \perp, & \text{otherwise.} \end{cases}$$

no need to hide r's in ct

Attribute-Based Functional Encryption

$$\mathrm{Dec}\left(\mathrm{sk}_{f,P}, \mathrm{ct}_{x}(z)\right) = \begin{cases} f(z), & P(x) = 1; \\ \perp, & P(x) = 0. \end{cases}$$

Attribute-Based Functional Encryption

$$\mathrm{Dec}\left(\mathrm{sk}_{f,P}, \mathrm{ct}_{x}(z)\right) = \begin{cases} f(z), & P(x) = 1; \\ \perp, & P(x) = 0. \end{cases}$$

Combine pairing-based FE/ABE techniques.

Ours. FE for quadratic functions + "dual-system ABE" (here, for read-once MSP)

(PLBE, $\sqrt{N_1}$-size pk/ct and $\mathrm{O}(1)$-size sk) (Threshold Broadcast, N_2-size pk/ct and $\mathrm{O}(1)$-size sk)

Attribute-Based Functional Encryption

$$\mathrm{Dec}\left(\mathrm{sk}_{f,P}, \mathrm{ct}_x(z)\right) = \begin{cases} f(z), & P(x) = 1; \\ \perp, & P(x) = 0. \end{cases}$$

Combine pairing-based FE/ABE techniques.

Ours. FE for quadratic functions + "dual-system ABE" (here, for read-once MSP)

(PLBE, $\sqrt{N_1}$-size pk/ct and $O(1)$-size sk) (Threshold Broadcast, N_2-size pk/ct and $O(1)$-size sk)

$$|\mathrm{pk}|, |\mathrm{ct}| = \sqrt{N_1} + N_2 \qquad |\mathrm{sk}| = 1 + 1$$

AB-FE: **Functional Encryption** Part

$$\mathrm{Dec}\left(\mathrm{sk}_{f,P}, \mathrm{ct}_{x}(z)\right) = \begin{cases} f(z), & P(x) = 1; \\ \perp, & P(x) = 0. \end{cases}$$

Combine pairing-based FE/ABE techniques.

Ours. FE for quadratic functions + "dual-system ABE" (here, for read-once MSP)

(PLBE, $\sqrt{N_1}$-size pk/ct and $O(1)$-size sk) (Threshold Broadcast, N_2-size pk/ct and $O(1)$-size sk)

$$|\mathrm{pk}|, |\mathrm{ct}| = \sqrt{N_1} + N_2 \qquad |\mathrm{sk}| = 1 + 1$$

AB-FE: **Functional Encryption** Part

$$\mathrm{Dec}\left(\mathrm{sk}_{f,P}, \mathrm{ct}_{x}(z)\right) = \begin{cases} f(z), & P(x) = 1; \\ \perp, & P(x) = 0. \end{cases}$$

Combine pairing-based FE/ABE techniques.

Ours. FE for quadratic functions + "dual-system ABE" (here, for read-once MSP)

(PLBE, $\sqrt{N_1}$-size pk/ct and $O(1)$-size sk) (Threshold Broadcast, N_2-size pk/ct and $O(1)$-size sk)

?

$$|\mathrm{pk}|, |\mathrm{ct}| = \sqrt{N_1} + N_2 \qquad |\mathrm{sk}| = 1 + 1$$

W20 FE for quadratic functions (QFE):

$$f(\boldsymbol{z}_1, \boldsymbol{z}_2) = \boldsymbol{f}^{\top}(\boldsymbol{z}_1 \otimes \boldsymbol{z}_2), \quad \boldsymbol{z}_1, \boldsymbol{z}_2 \in \mathbb{Z}_p^n, \quad \boldsymbol{f} \in \mathbb{Z}_p^{n^2}, \qquad |\mathrm{pk}|, |\mathrm{ct}| = O(n), \quad |\mathrm{sk}| = O(1).$$

AB-FE: **Functional Encryption** Part

$$\mathrm{Dec}\left(\mathrm{sk}_{f,P}, \mathrm{ct}_{x}(z)\right) = \begin{cases} f(z), & P(x) = 1; \\ \perp, & P(x) = 0. \end{cases}$$

Combine pairing-based FE/ABE techniques.

Ours. FE for quadratic functions + "dual-system ABE" (here, for read-once MSP)

(PLBE, $\sqrt{N_1}$-size pk/ct and $O(1)$-size sk) (Threshold Broadcast, N_2-size pk/ct and $O(1)$-size sk)

?

$$|\mathrm{pk}|, |\mathrm{ct}| = \sqrt{N_1} + N_2 \qquad |\mathrm{sk}| = 1 + 1$$

W20 FE for quadratic functions (QFE):

$$f(\boldsymbol{z}_1, \boldsymbol{z}_2) = \boldsymbol{f}^{\top}(\boldsymbol{z}_1 \otimes \boldsymbol{z}_2), \quad \boldsymbol{z}_1, \boldsymbol{z}_2 \in \mathbb{Z}_p^n, \quad \boldsymbol{f} \in \mathbb{Z}_p^{n^2}, \qquad |\mathrm{pk}|, |\mathrm{ct}| = O(n), \quad |\mathrm{sk}| = O(1).$$

BCFG17 PLBE from QFE. $[N_1] \Leftrightarrow [n] \times [n]$ and use one-hot encoding.

AB-FE: **Attribute-Based Encryption** Part

$$\mathrm{Dec}\left(\mathrm{sk}_{f,P}, \mathrm{ct}_{x}(z)\right) = \begin{cases} f(z), & P(x) = 1; \\ \perp, & P(x) = 0. \end{cases}$$

Combine pairing-based FE/ABE techniques.

Ours. FE for quadratic functions + "dual-system ABE" (here, for read-once MSP)

(PLBE, $\sqrt{N_1}$-size pk/ct and $O(1)$-size sk) (Threshold Broadcast, N_2-size pk/ct and $O(1)$-size sk)

$$|\mathrm{pk}|, |\mathrm{ct}| = \sqrt{N_1} + N_2 \qquad |\mathrm{sk}| = 1 + 1$$

?

AB-FE: **Attribute-Based Encryption** Part

$$\mathrm{Dec}\left(\mathrm{sk}_{f,P}, \mathrm{ct}_x(z)\right) = \begin{cases} f(z), & P(x) = 1; \\ \perp, & P(x) = 0. \end{cases}$$

Combine pairing-based FE/ABE techniques.

Ours. FE for quadratic functions + "dual-system ABE" (here, for read-once MSP)

(PLBE, $\sqrt{N_1}$-size pk/ct and $O(1)$-size sk) (Threshold Broadcast, N_2-size pk/ct and $O(1)$-size sk)

$$|\mathrm{pk}|, |\mathrm{ct}| = \sqrt{N_1} + N_2 \qquad |\mathrm{sk}| = 1 + 1$$

?

roMSP = linear secret sharing s.t. each party has at most one share

local roMSP = roMSP s.t. only **a few** (locality many of) parties have **a** share

AB-FE: **Attribute-Based Encryption** Part

$$\mathrm{Dec}\left(\mathrm{sk}_{f,P}, \mathrm{ct}_x(z)\right) = \begin{cases} f(z), & P(x) = 1; \\ \perp, & P(x) = 0. \end{cases}$$

Combine pairing-based FE/ABE techniques.

Ours. FE for quadratic functions + "dual-system ABE" (here, for read-once MSP)

(PLBE, $\sqrt{N_1}$-size pk/ct and $O(1)$-size sk) (Threshold Broadcast, N_2-size pk/ct and $O(1)$-size sk)

$$|\mathrm{pk}|, |\mathrm{ct}| = \sqrt{N_1} + N_2 \qquad |\mathrm{sk}| = 1 + 1$$

?

roMSP = linear secret sharing s.t. each party has at most one share

local roMSP = roMSP s.t. only **a few** (locality many of) parties have **a** share

ABE sk is roughly "encryptions" of the possible shares.

$$|\mathrm{sk}| \propto \#[\text{possible shares}] = \text{locality}$$

AB-FE: **Attribute-Based Encryption** Part

$$\mathrm{Dec}\left(\mathrm{sk}_{f,P}, \mathrm{ct}_x(z)\right) = \begin{cases} f(z), & P(x) = 1; \\ \perp, & P(x) = 0. \end{cases}$$

Combine pairing-based FE/ABE techniques.

roMSP for TB is λ-local

Ours. FE for quadratic functions + "dual-system ABE" (here, for read-once MSP)

(PLBE, $\sqrt{N_1}$-size pk/ct and $O(1)$-size sk) (Threshold Broadcast, N_2-size pk/ct and $O(1)$-size sk)

$$|\mathrm{pk}|, |\mathrm{ct}| = \sqrt{N_1} + N_2 \qquad |\mathrm{sk}| = 1 + 1$$

?

roMSP = linear secret sharing s.t. each party has at most one share

local roMSP = roMSP s.t. only **a few** (locality many of) parties have **a** share

ABE sk is roughly "encryptions" of the possible shares.

$$|\mathrm{sk}| \propto \#[\text{possible shares}] = \text{locality}$$

One More Thing: Adaptive Security

$$\mathrm{Dec}\left(\mathrm{sk}_{f,P}, \mathrm{ct}_{x}(z)\right) = \begin{cases} f(z), & P(x) = 1; \\ \perp, & P(x) = 0. \end{cases}$$

z-selective and **x-adaptive** by carefully implementing hybrids.

One More Thing: Adaptive Security

$$\mathrm{Dec}\left(\mathrm{sk}_{f,P}, \mathrm{ct}_{x}(z)\right) = \begin{cases} f(z), & P(x) = 1; \\ \perp, & P(x) = 0. \end{cases}$$

z-selective and **x-adaptive** by carefully implementing hybrids.

Challenge. cannot predict $P(x)$ – if $P(x) = 1$,
hybrid move for hiding $f(z)$ in typical proof is invalid
("switch to semi-functional key")

One More Thing: Adaptive Security

$$\mathrm{Dec}\left(\mathrm{sk}_{f,P}, \mathrm{ct}_x(z)\right) = \begin{cases} f(z), & P(x) = 1; \\ \perp, & P(x) = 0. \end{cases}$$

z-selective and **x-adaptive** by carefully implementing hybrids.

Challenge. cannot predict $P(x)$ – if $P(x) = 1$,
hybrid move for hiding $f(z)$ in typical proof is invalid
("switch to semi-functional key")

Solution. if $f(z_0) = f(z_1)$, no move is needed;
if $f(z_0) \neq f(z_1)$, deduce $P(x) = 0$ and perform the move.

Open Questions

Is the product “the correct measure”?
Can we **“rebalance”** among $\mathrm{pk}, \mathrm{sk}, \mathrm{ct}$
to achieve $O(N^{2/9})$-size components?

Open Questions

Is the product "the correct measure"?
Can we **"rebalance"** among $\mathrm{pk}, \mathrm{sk}, \mathrm{ct}$
to achieve $\mathrm{O}(N^{2/9})$-size components?

How far can pairings go?
Can we achieve $|\mathrm{pk}|, |\mathrm{ct}| = \mathrm{O}\left(N^{1/3-\varepsilon}\right)$, $|\mathrm{sk}| = \mathrm{O}(1)$?

Open Questions

Is the product "the correct measure"?
Can we **"rebalance"** among $\mathrm{pk}, \mathrm{sk}, \mathrm{ct}$
to achieve $O(N^{2/9})$-size components?

How far can pairings go?
Can we achieve $|\mathrm{pk}|, |\mathrm{ct}| = O\left(N^{1/3-\varepsilon}\right)$, $|\mathrm{sk}| = O(1)$?

Can we achieve such parameter sizes
for **broadcast-and-trace** / **public tracing**?

Thanks!

ePrint 2023/256

Stock Question: Technical Comparison with [Z20]

this: rPLBE / traitor tracing with $|\mathrm{pk}|, |\mathrm{ct}| = O(N_1^{1/2} + N_2)$, $|\mathrm{sk}| = O(1)$.

Stock Question: Technical Comparison with [Z20]

this: rPLBE / traitor tracing with $|\mathrm{pk}|, |\mathrm{ct}| = \mathrm{O}(N_1^{1/2} + N_2)$, $|\mathrm{sk}| = \mathrm{O}(1)$.

Z20: (can be interpreted as)
rPLBE / traitor tracing with $|\mathrm{pk}|, |\mathrm{ct}| = \mathrm{O}(N_2)$, $|\mathrm{sk}| = \mathrm{O}(N_1 + N_2)$, *

* proof requires GGM & amplified from "risky" traitor tracing.

Stock Question: Technical Comparison with [Z20]

this: rPLBE / traitor tracing with $|\mathrm{pk}|, |\mathrm{ct}| = \mathrm{O}(N_1^{1/2} + N_2)$, $|\mathrm{sk}| = \mathrm{O}(1)$.

Z20: (can be interpreted as)
rPLBE / traitor tracing with $|\mathrm{pk}|, |\mathrm{ct}| = \mathrm{O}(N_2)$, $|\mathrm{sk}| = \mathrm{O}(N_1 + N_2)$, *
amplifying that scheme to (for $N_1 N_2 N_3$ users)
$|\mathrm{pk}| = \mathrm{O}(N_2)$, $|\mathrm{sk}| = \mathrm{O}(N_1 + N_2)$, $|\mathrm{ct}| = \mathrm{O}(N_2 + N_3)$,

* proof requires GGM & amplified from "risky" traitor tracing.

Stock Question: Technical Comparison with [Z20]

this: rPLBE / traitor tracing with $|\mathrm{pk}|, |\mathrm{ct}| = \mathrm{O}(N_1^{1/2} + N_2)$, $|\mathrm{sk}| = \mathrm{O}(1)$.

Z20: (can be interpreted as)

rPLBE / traitor tracing with $|\mathrm{pk}|, |\mathrm{ct}| = \mathrm{O}(N_2)$, $|\mathrm{sk}| = \mathrm{O}(N_1 + N_2)$, *

amplifying that scheme to (for $N_1 N_2 N_3$ users)

$$|\mathrm{pk}| = \mathrm{O}(N_2), \quad |\mathrm{sk}| = \mathrm{O}(N_1 + N_2), \quad |\mathrm{ct}| = \mathrm{O}(N_2 + N_3),$$

optimal balancing by $N_1 = N_2 = N_3 = N^{1/3}$.

* proof requires GGM & amplified from "risky" traitor tracing.

Stock Question: Traitor Tracing from rPLBE: Identifying i_1

$$\mathrm{TTsk}_i = \mathrm{rPLBsk}_i$$

$$\mathrm{TTct}(\mu) = \mathrm{rPLBct}(0, \emptyset, \mu)$$

Stock Question: Traitor Tracing from rPLBE: Identifying i_1

$$\mathrm{TTsk}_i = \mathrm{rPLBsk}_i$$

$$\mathrm{TTct}(\mu) = \mathrm{rPLBct}(0, \emptyset, \mu) \quad \cdots \quad \mathrm{rPLBct}(i_1 - 1, \emptyset, \mu) \quad \mathrm{rPLBct}(i_1, \emptyset, \mu) \quad \cdots \quad \mathrm{rPLBct}(N_1, \emptyset, \mu)$$

$$\geq \varepsilon$$

Stock Question: Traitor Tracing from rPLBE: Identifying i_1

$$\mathrm{TTsk}_i = \mathrm{rPLBsk}_i$$

$$\mathrm{TTct}(\mu) = \mathrm{rPLBct}(0, \emptyset, \mu) \quad \cdots \quad \mathrm{rPLBct}(i_1 - 1, \emptyset, \mu) \quad \mathrm{rPLBct}(i_1, \emptyset, \mu) \quad \cdots \quad \mathrm{rPLBct}(N_1, \emptyset, \mu)$$

$$\geq \varepsilon$$

By message-hiding, ≈ 0;
total gap of $\Omega(\varepsilon)$.

Stock Question: Traitor Tracing from rPLBE: Identifying i_1

$$\mathrm{TTsk}_i = \mathrm{rPLBsk}_i$$

$$\mathrm{TTct}(\mu) =$$

$$\mathrm{rPLBct}(0, \emptyset, \mu) \quad \cdots \quad \mathrm{rPLBct}(i_1 - 1, \emptyset, \mu) \quad \mathrm{rPLBct}(i_1, \emptyset, \mu) \quad \cdots \quad \mathrm{rPLBct}(N_1, \emptyset, \mu)$$

$$\geq \varepsilon$$

By message-hiding, ≈ 0; total gap of $\Omega(\varepsilon)$.

By index-hiding, if all $i_1, \star$ are honest, then $\Delta\varepsilon_{i_1} \approx 0$;

Stock Question: Traitor Tracing from rPLBE: Identifying i_1

$$\mathrm{TTsk}_i = \mathrm{rPLBsk}_i$$

$$\mathrm{TTct}(\mu) =$$

$$\mathrm{rPLBct}(0, \emptyset, \mu) \quad \cdots \quad \mathrm{rPLBct}(i_1 - 1, \emptyset, \mu) \quad \mathrm{rPLBct}(i_1, \emptyset, \mu) \quad \cdots \quad \mathrm{rPLBct}(N_1, \emptyset, \mu)$$

$$\geq \varepsilon$$

By message-hiding, ≈ 0; total gap of $\Omega(\varepsilon)$.

By index-hiding, if all $i_1,\star$ are honest, then $\Delta\varepsilon_{i_1} \approx 0$;

index-hiding

$\mathrm{ct}(i_1 - 1, \emptyset, \mu) \approx \mathrm{ct}(i_1, \emptyset, \mu)$
given $\mathrm{sk}_{\neq i_1,\star}$'s ~~and $\mathrm{sk}_{\in\emptyset}$'s~~

Stock Question: Traitor Tracing from rPLBE: Identifying i_1

$$\mathrm{TTsk}_i = \mathrm{rPLBsk}_i$$

$$\mathrm{TTct}(\mu) =$$

$$\mathrm{rPLBct}(0, \emptyset, \mu) \quad \cdots \quad \mathrm{rPLBct}(i_1 - 1, \emptyset, \mu) \quad \mathrm{rPLBct}(i_1, \emptyset, \mu) \quad \cdots \quad \mathrm{rPLBct}(N_1, \emptyset, \mu)$$

$$\geq \varepsilon$$

By message-hiding, ≈ 0; total gap of $\Omega(\varepsilon)$.

By index-hiding, if all $i_1,\star$ are honest, then $\Delta\varepsilon_{i_1} \approx 0$; if $\Delta\varepsilon_{i_1} = \Omega(\varepsilon/N_1)$, then some $i_1,\star$ is a traitor.

index-hiding

$\mathrm{ct}(i_1 - 1, \emptyset, \mu) \approx \mathrm{ct}(i_1, \emptyset, \mu)$ given $\mathrm{sk}_{\neq i_1,\star}$'s ~~and $\mathrm{sk}_{\in\emptyset}$'s~~

Stock Question: Traitor Tracing from rPLBE: Identifying i_2

$$\mathrm{TTsk}_i = \mathrm{rPLBsk}_i$$

$$\mathrm{TTct}(\mu) = \mathrm{rPLBct}(0, \emptyset, \mu) \quad \cdots \quad \mathrm{rPLBct}(i_1 - 1, \emptyset, \mu) \quad \mathrm{rPLBct}(i_1, \emptyset, \mu) \quad \cdots \quad \mathrm{rPLBct}(N_1, \emptyset, \mu)$$

$$\Delta\varepsilon_{i_1} = \Omega(\varepsilon / N_1)$$

Stock Question: Traitor Tracing from rPLBE: Identifying i_2

$$\mathrm{TTsk}_i = \mathrm{rPLBsk}_i$$

$$\mathrm{TTct}(\mu) = \mathrm{rPLBct}(0, \emptyset, \mu) \quad \cdots \quad \mathrm{rPLBct}(N_1, \emptyset, \mu)$$

$$\Delta\varepsilon_{i_1} = \Omega(\varepsilon / N_1)$$

$$S_{i_2} = \{(i_1, \leq i_2)\}$$

$$\begin{array}{cc}
\mathrm{rPLBct}(i_1 - 1, \emptyset, \mu) & \mathrm{rPLBct}(i_1, \emptyset, \mu) \\
\mathrm{rPLBct}(i_1 - 1, S_1, \mu) & \mathrm{rPLBct}(i_1, S_1, \mu) \\
\vdots & \vdots \\
\mathrm{rPLBct}(i_1 - 1, S_{i_2 - 1}, \mu) & \mathrm{rPLBct}(i_1, S_{i_2 - 1}, \mu) \\
\mathrm{rPLBct}(i_1 - 1, S_{i_2}, \mu) & \mathrm{rPLBct}(i_1, S_{i_2}, \mu) \\
\vdots & \vdots \\
\mathrm{rPLBct}(i_1 - 1, S_{N_2}, \mu) & \mathrm{rPLBct}(i_1, S_{N_2}, \mu)
\end{array}$$

Stock Question: Traitor Tracing from rPLBE: Identifying i_2

$\mathrm{TTsk}_i = \mathrm{rPLBsk}_i$

$\mathrm{TTct}(\mu) = \mathrm{rPLBct}(0, \emptyset, \mu) \quad \cdots \quad \mathrm{rPLBct}(N_1, \emptyset, \mu)$

$S_{i_2} = \{(i_1, \leq i_2)\}$

$$\Delta\varepsilon_{i_1} = \Omega(\varepsilon / N_1)$$

$$\begin{array}{cc}
\mathrm{rPLBct}(i_1 - 1, \emptyset, \mu) & \mathrm{rPLBct}(i_1, \emptyset, \mu) \\
\mathrm{rPLBct}(i_1 - 1, S_1, \mu) & \mathrm{rPLBct}(i_1, S_1, \mu) \\
\vdots & \vdots \\
\mathrm{rPLBct}(i_1 - 1, S_{i_2 - 1}, \mu) & \mathrm{rPLBct}(i_1, S_{i_2 - 1}, \mu) \\
\mathrm{rPLBct}(i_1 - 1, S_{i_2}, \mu) & \mathrm{rPLBct}(i_1, S_{i_2}, \mu) \\
\vdots & \vdots \\
\mathrm{rPLBct}(i_1 - 1, S_{N_2}, \mu) & \mathrm{rPLBct}(i_1, S_{N_2}, \mu)
\end{array}$$

$\Delta\varepsilon \approx 0$ by **index-hiding**

$\mathrm{ct}(i_1 - 1, S_{N_2}, \mu) \approx \mathrm{ct}(i_1, S_{N_2}, \mu)$
given $\mathrm{sk}_{\neq i_1, \star}$'s and $\mathrm{sk}_{i_1, \star}$'s

Stock Question: Traitor Tracing from rPLBE: Identifying i_2

$\mathrm{TTsk}_i = \mathrm{rPLBsk}_i$

$\mathrm{TTct}(\mu) = \mathrm{rPLBct}(0, \emptyset, \mu)$ $\cdots$ $\mathrm{rPLBct}(i_1 - 1, \emptyset, \mu)$ $\mathrm{rPLBct}(i_1, \emptyset, \mu)$ $\cdots$ $\mathrm{rPLBct}(N_1, \emptyset, \mu)$

$\mathrm{rPLBct}(i_1 - 1, S_1, \mu)$ $\mathrm{rPLBct}(i_1, S_1, \mu)$

$\mathrm{rPLBct}(i_1 - 1, S_{i_2-1}, \mu)$ $\mathrm{rPLBct}(i_1, S_{i_2-1}, \mu)$

$\mathrm{rPLBct}(i_1 - 1, S_{i_2}, \mu)$ $\mathrm{rPLBct}(i_1, S_{i_2}, \mu)$

$\mathrm{rPLBct}(i_1 - 1, S_{N_2}, \mu)$ $\mathrm{rPLBct}(i_1, S_{N_2}, \mu)$

$$\Delta\varepsilon_{i_1} = \Omega(\varepsilon/N_1)$$

$$S_{i_2} = \{(i_1, \leq i_2)\}$$

By **set-hiding**,
if (i_1, i_2) is honest,
then $\Delta\Delta\varepsilon \approx 0$;

$\Delta\varepsilon \approx 0$ by **index-hiding**

$\mathrm{ct}(i_1 - 1, S_{N_2}, \mu) \approx \mathrm{ct}(i_1, S_{N_2}, \mu)$
given $\mathrm{sk}_{\neq i_1,\star}$'s and $\mathrm{sk}_{i_1,\star}$'s

Stock Question: Traitor Tracing from rPLBE: Identifying i_2

$\mathrm{TTsk}_i = \mathrm{rPLBsk}_i$

$\mathrm{TTct}(\mu) =$

$\mathrm{rPLBct}(0, \emptyset, \mu) \quad \cdots \quad \mathrm{rPLBct}(i_1 - 1, \emptyset, \mu) \quad \mathrm{rPLBct}(i_1, \emptyset, \mu) \quad \cdots \quad \mathrm{rPLBct}(N_1, \emptyset, \mu)$

$\mathrm{rPLBct}(i_1 - 1, S_1, \mu) \quad \mathrm{rPLBct}(i_1, S_1, \mu)$

$\vdots \qquad \vdots$

$\mathrm{rPLBct}(i_1 - 1, S_{i_2-1}, \mu) \quad \mathrm{rPLBct}(i_1, S_{i_2-1}, \mu)$

$\mathrm{rPLBct}(i_1 - 1, S_{i_2}, \mu) \quad \mathrm{rPLBct}(i_1, S_{i_2}, \mu)$

$\vdots \qquad \vdots$

$\mathrm{rPLBct}(i_1 - 1, S_{N_2}, \mu) \quad \mathrm{rPLBct}(i_1, S_{N_2}, \mu)$

$$\Delta\varepsilon_{i_1} = \Omega(\varepsilon/N_1)$$

$$S_{i_2} = \{(i_1, \leq i_2)\}$$

By **set-hiding**,
if (i_1, i_2) is honest,
then $\Delta\Delta\varepsilon \approx 0$;
so
if $\Delta\Delta\varepsilon = \Omega(\varepsilon/N_1N_2)$,
then (i_1, i_2) is a traitor.

$\Delta\varepsilon \approx 0$ by **index-hiding**

$\mathrm{ct}(i_1 - 1, S_{N_2}, \mu) \approx \mathrm{ct}(i_1, S_{N_2}, \mu)$
given $\mathrm{sk}_{\neq i_1,\star}$'s and $\mathrm{sk}_{i_1,\star}$'s