ad hoc (decentralized) broadcast, trace, and revoke
自组型（去中心化）广播、追踪、撤销

罗辑

故事、大纲

No mathematical idea has ever been published ***in the way it was discovered***. Techniques have been developed and are used, if a problem has been solved, to turn the solution procedure ***upside down***, or if it is a larger complex of statements and theories, to turn definitions into propositions, and propositions into definitions, ***the hot invention into icy beauty***.

—— Hans Freudenthal [F]

故事、大纲

No mathematical idea has ever been published ***in the way it was discovered***. Techniques have been developed and are used, if a problem has been solved, to turn the solution procedure ***upside down***, or if it is a larger complex of statements and theories, to turn definitions into propositions, and propositions into definitions, ***the hot invention into icy beauty***.

—— Hans Freudenthal [F]

“数学家收起了**火热的思考**，留下了**冰冷的美丽**.”

——杨晶

故事、大纲

++启发式、自然思考式; --展示式（学术报告的常见模式）;

No mathematical idea has ever been published ***in the way it was discovered***. Techniques have been developed and are used, if a problem has been solved, to turn the solution procedure ***upside down***, or if it is a larger complex of statements and theories, to turn definitions into propositions, and propositions into definitions, ***the hot invention into icy beauty***.

—— Hans Freudenthal [F]

“数学家收起了**火热的思考**，留下了**冰冷的美丽**.”

——杨晶

故事、大纲

++启发式、自然思考式; --展示式（学术报告的常见模式）;

- 传统叛徒追踪
- 动机、问题

No mathematical idea has ever been published ***in the way it was discovered***. Techniques have been developed and are used, if a problem has been solved, to turn the solution procedure ***upside down***, or if it is a larger complex of statements and theories, to turn definitions into propositions, and propositions into definitions, ***the hot invention into icy beauty***.

—— Hans Freudenthal [F]

“数学家收起了**火热的思考**，留下了**冰冷的美丽**.”

——杨晶

故事、大纲

++启发式、自然思考式; --展示式（学术报告的常见模式）;

- 传统叛徒追踪
- 动机、问题

- 推演定义
- 两款构造
- 下界证明

No mathematical idea has ever been published ***in the way it was discovered***. Techniques have been developed and are used, if a problem has been solved, to turn the solution procedure ***upside down***, or if it is a larger complex of statements and theories, to turn definitions into propositions, and propositions into definitions, ***the hot invention into icy beauty***.

—— Hans Freudenthal [F]

“数学家收起了**火热的思考**，留下了**冰冷的美丽**.”

——杨晶

故事、大纲

++启发式、自然思考式; --展示式（学术报告的常见模式）;

- 传统叛徒追踪
- 动机、问题

- 推演定义
- 两款构造
- 下界证明

- 故事汇

No mathematical idea has ever been published ***in the way it was discovered***. Techniques have been developed and are used, if a problem has been solved, to turn the solution procedure ***upside down***, or if it is a larger complex of statements and theories, to turn definitions into propositions, and propositions into definitions, ***the hot invention into icy beauty***.

—— Hans Freudenthal [F]

“数学家收起了**火热的思考**，留下了**冰冷的美丽**.”

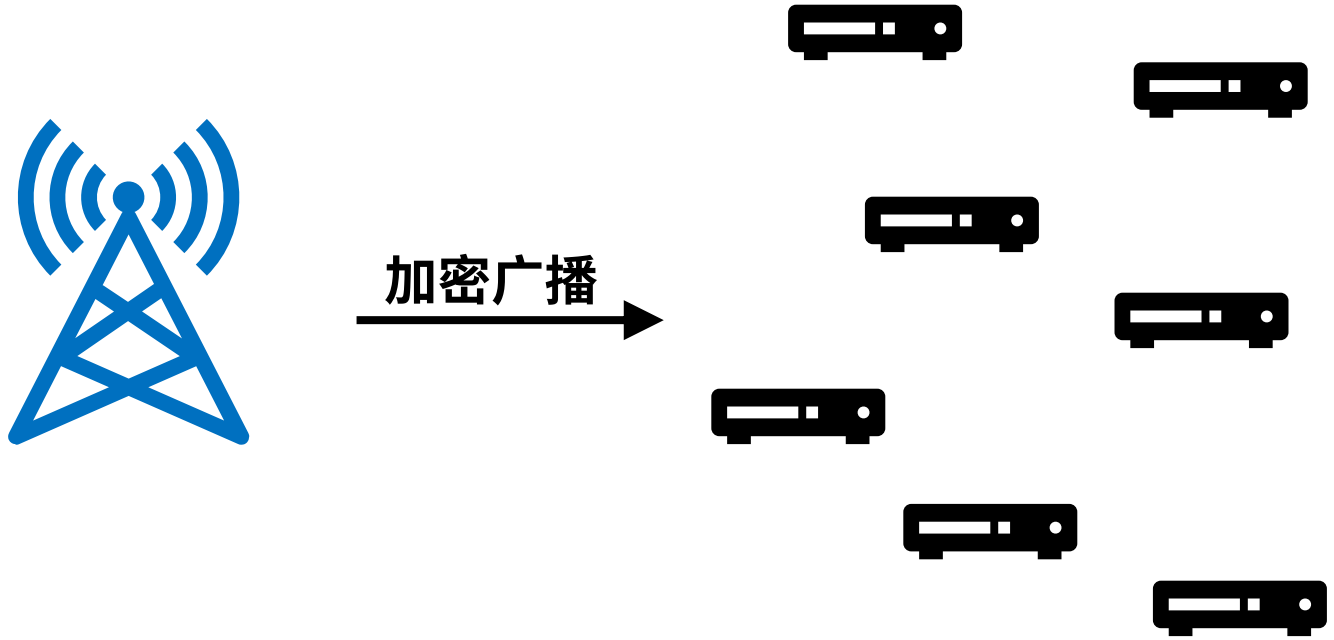
——杨晶

传统叛徒追踪 (TT) [CFN]

traitor tracing

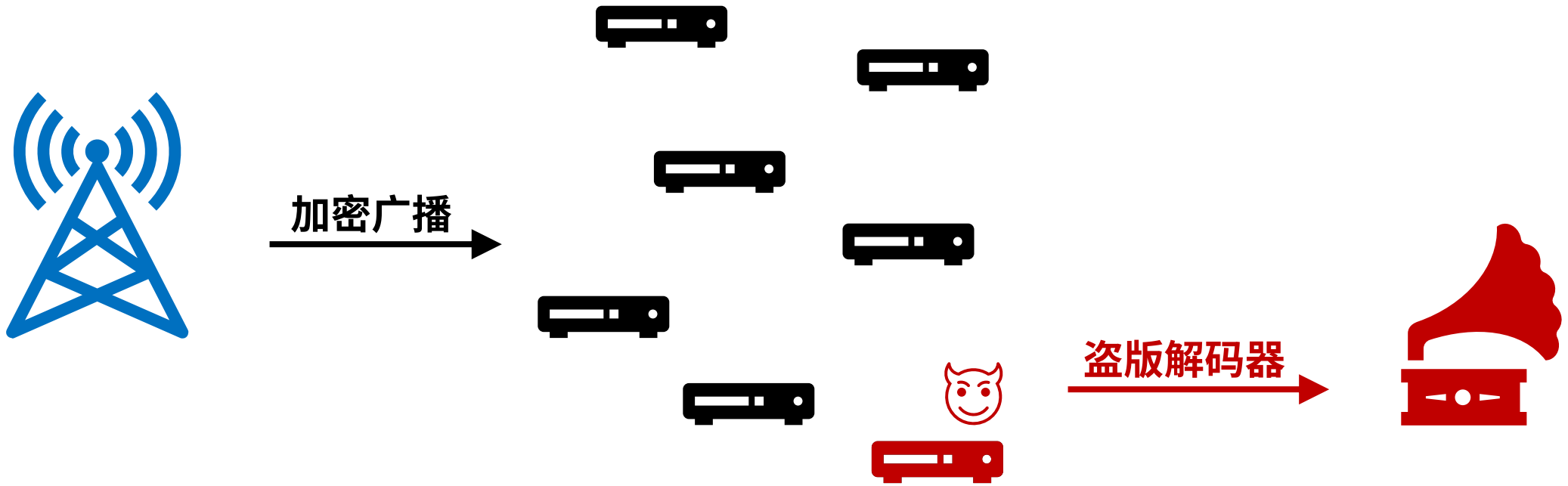
传统叛徒追踪 (TT) [CFN]

traitor tracing



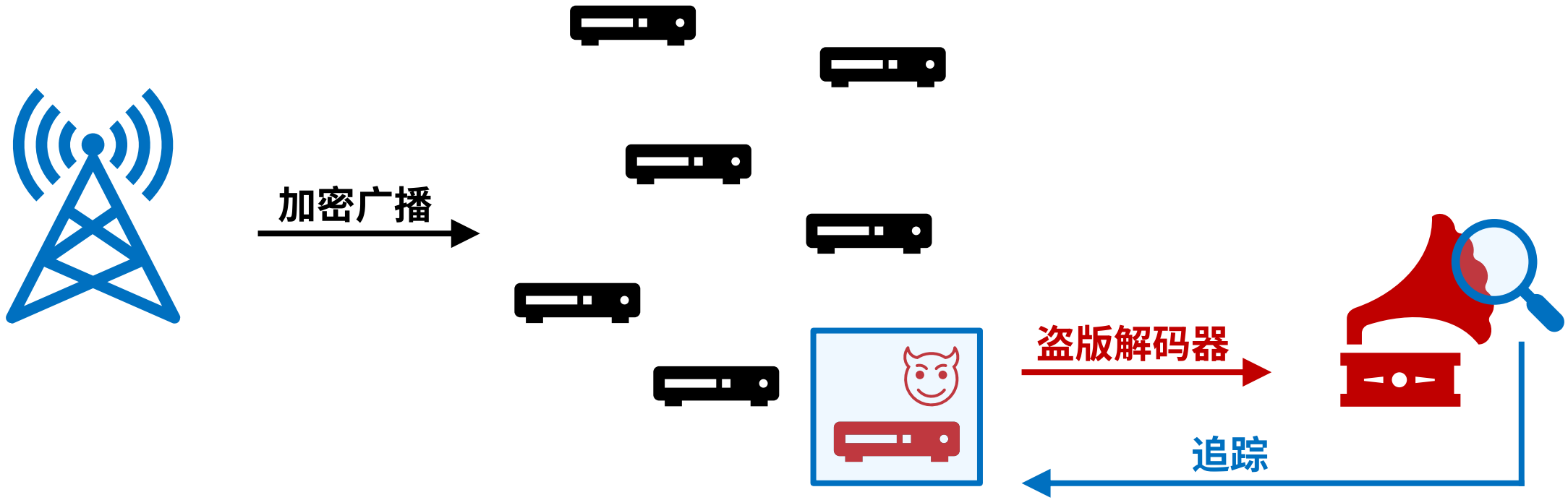
传统叛徒追踪 (TT) [CFN]

traitor tracing



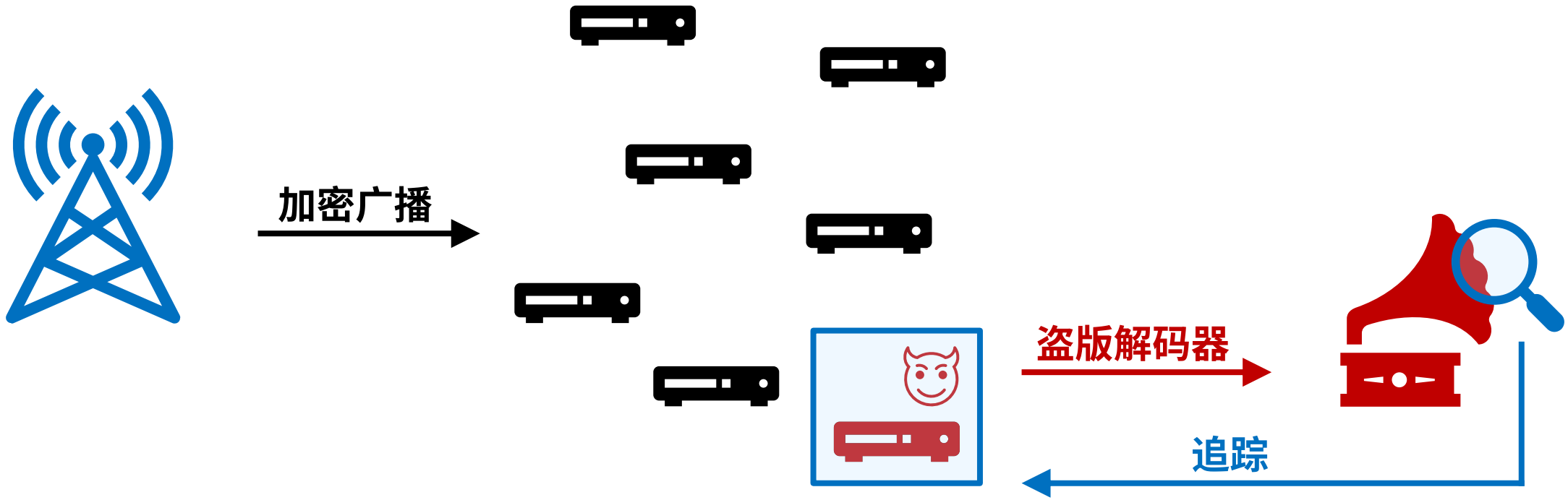
传统叛徒追踪 (TT) [CFN]

traitor tracing



传统叛徒追踪 (TT) [CFN]

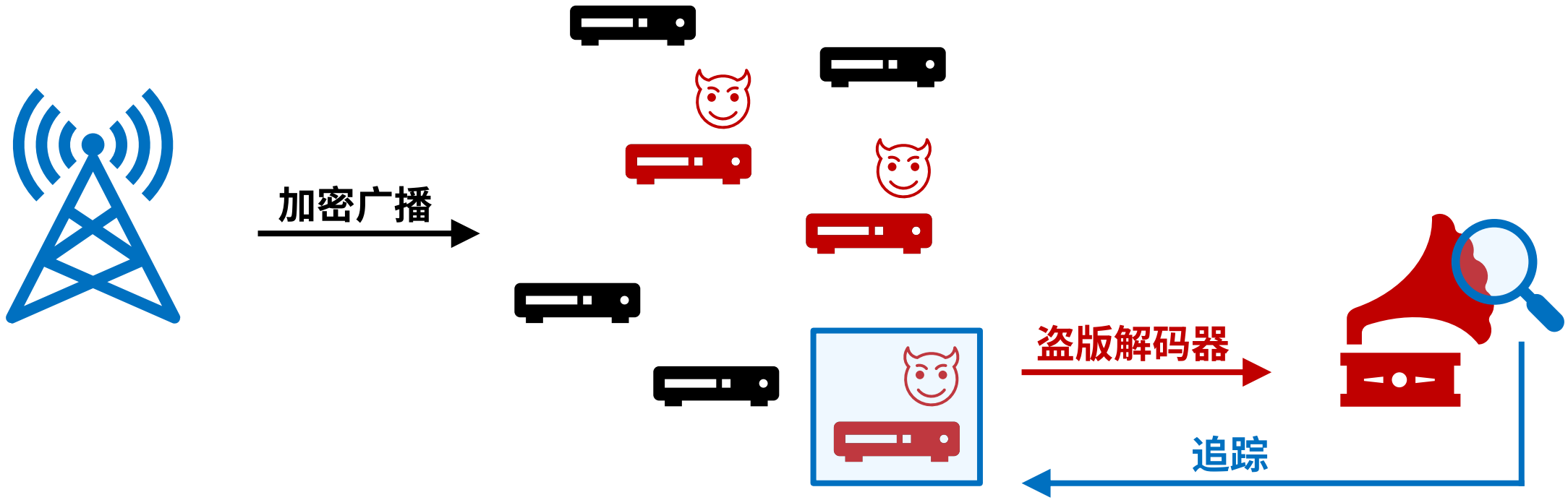
traitor tracing



- 只要盗版解码器**让加密不安全**，就能**找出**至少一个**叛徒**
- 永远**不指控无辜**订户

传统叛徒追踪 (TT) [CFN]

traitor tracing



- 只要盗版解码器**让加密不安全**，就能**找出**至少一个**叛徒**
- 永远**不指控无辜**订户
- 上述两条在任意多个叛徒**合谋**时也成立

传统叛徒追踪：定义

传统叛徒追踪：定义

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

传统叛徒追踪：定义

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

$$\mathrm{Enc}(\mathrm{pk}, \mu \in \{0,1\}^\lambda) \to \mathrm{ct}$$

传统叛徒追踪：定义

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

$$\mathrm{Enc}(\mathrm{pk}, \mu \in \{0,1\}^\lambda) \to \mathrm{ct}$$

$$\mathrm{Dec}(\mathrm{sk}_i, \mathrm{ct}) \to \mu$$

传统叛徒追踪：定义

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

$$\mathrm{Enc}(\mathrm{pk}, \mu \in \{0,1\}^\lambda) \to \mathrm{ct}$$

$$\mathrm{Dec}(\mathrm{sk}_i, \mathrm{ct}) \to \mu$$

$$\mathrm{Trace}^D(\mathrm{pk}, 1^{1/\varepsilon^*}) \to i^* \in [N] \cup \{\perp\}$$

传统叛徒追踪：定义

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

$$\mathrm{Enc}(\mathrm{pk}, \mu \in \{0,1\}^\lambda) \to \mathrm{ct}$$

$$\mathrm{Dec}(\mathrm{sk}_i, \mathrm{ct}) \to \mu$$

$$\mathrm{Trace}^D(\mathrm{pk}, 1^{1/\varepsilon^*}) \to i^* \in [N] \cup \{\perp\}$$

D 优势 $\geq \varepsilon^*$ 时，应识别出叛徒

传统叛徒追踪：定义

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

谁来运行 Gen?

$$\mathrm{Enc}(\mathrm{pk}, \mu \in \{0,1\}^\lambda) \to \mathrm{ct}$$

$$\mathrm{Dec}(\mathrm{sk}_i, \mathrm{ct}) \to \mu$$

$$\mathrm{Trace}^D(\mathrm{pk}, 1^{1/\varepsilon^*}) \to i^* \in [N] \cup \{\perp\}$$

D 优势 $\geq \varepsilon^*$ 时，应识别出叛徒

传统叛徒追踪：定义

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

谁来运行 Gen?

$$\mathrm{Enc}(\mathrm{pk}, \mu \in \{0,1\}^\lambda) \to \mathrm{ct}$$

$$\mathrm{Dec}(\mathrm{sk}_i, \mathrm{ct}) \to \mu$$

$$\mathrm{Trace}^D(\mathrm{pk}, 1^{1/\varepsilon^*}) \to i^* \in [N] \cup \{\perp\}$$

D 优势 $\geq \varepsilon^*$ 时，应识别出叛徒

叛徒追踪里有谁?

- 广播提供商
- 订户（使坏者）

传统叛徒追踪：定义

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

谁来运行 Gen?

$$\mathrm{Enc}(\mathrm{pk}, \mu \in \{0,1\}^\lambda) \to \mathrm{ct}$$

$$\mathrm{Dec}(\mathrm{sk}_i, \mathrm{ct}) \to \mu$$

$$\mathrm{Trace}^D(\mathrm{pk}, 1^{1/\varepsilon^*}) \to i^* \in [N] \cup \{\perp\}$$

D 优势 $\geq \varepsilon^*$ 时，应识别出叛徒

叛徒追踪里有谁?

- 广播提供商
- 订户（使坏者）

它要保护谁的利益?

广播提供商.

传统叛徒追踪：定义

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

谁来运行 Gen?

$$\mathrm{Enc}(\mathrm{pk}, \mu \in \{0,1\}^\lambda) \to \mathrm{ct}$$

$$\mathrm{Dec}(\mathrm{sk}_i, \mathrm{ct}) \to \mu$$

$$\mathrm{Trace}^D(\mathrm{pk}, 1^{1/\varepsilon^*}) \to i^* \in [N] \cup \{\perp\}$$

D 优势 $\geq \varepsilon^*$ 时，应识别出叛徒

叛徒追踪里有谁?

- 广播提供商
- 订户（使坏者）

它要保护谁的利益?

广播提供商.

广播提供商运行 Gen.

新场景：传统定义无能为力

广播提供商运行 $\mathrm{Gen}(1^N) \to \mathrm{pk}, \mathrm{sk}_1, \ldots, \mathrm{sk}_N$

新场景：传统定义无能为力

广播提供商运行 $\mathrm{Gen}(1^N) \to \mathrm{pk}, \mathrm{sk}_1, \ldots, \mathrm{sk}_N$ **运行 Gen 的人掌握所有私钥**

新场景：传统定义无能为力

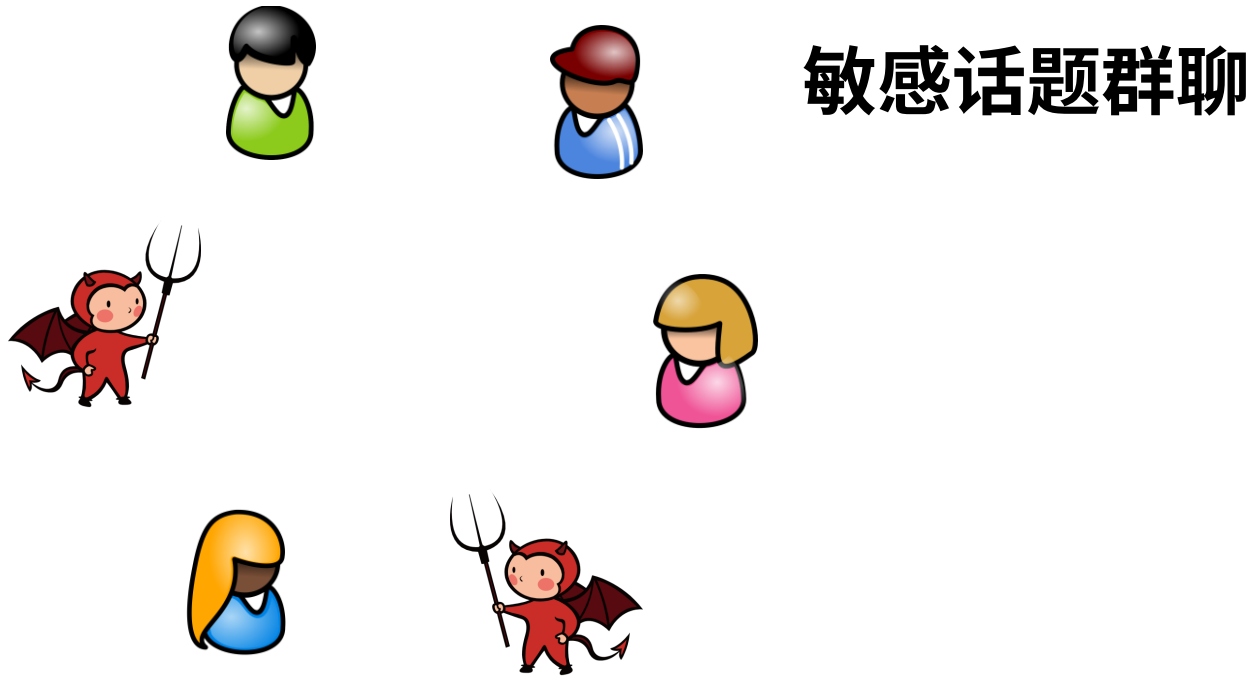
广播提供商运行 $\mathrm{Gen}(1^N) \to \mathrm{pk}, \mathrm{sk}_1, \ldots, \mathrm{sk}_N$ **运行 Gen 的人掌握所有私钥**

- 传统定义：仅为广播提供商设计、中心化
- 其他用法：不适宜

新场景：传统定义无能为力

广播提供商运行 $\mathrm{Gen}(1^N) \to \mathrm{pk}, \mathrm{sk}_1, \ldots, \mathrm{sk}_N$ **运行 Gen 的人掌握所有私钥**

- 传统定义：仅为广播提供商设计、中心化
- 其他用法：不适宜

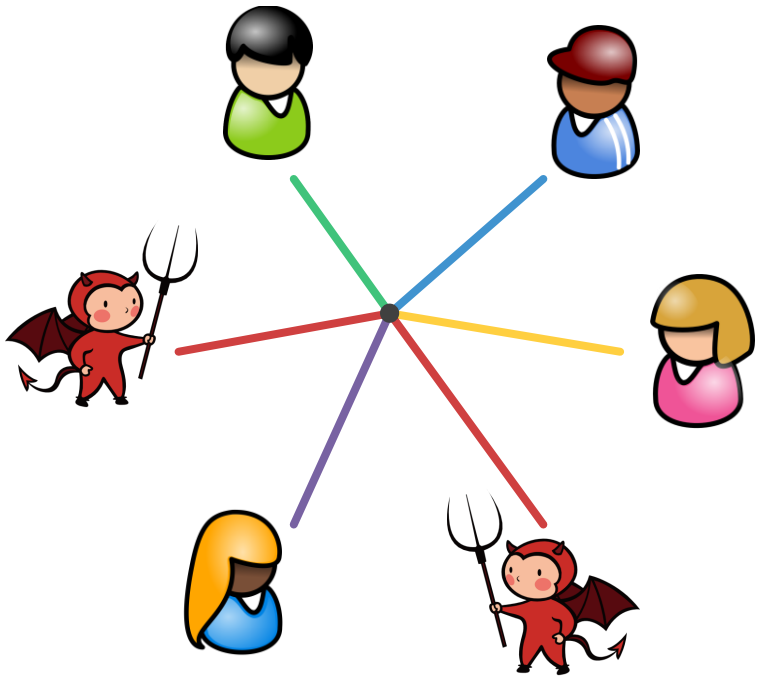


敏感话题群聊

新场景：传统定义无能为力

广播提供商运行 $\mathrm{Gen}(1^N) \to \mathrm{pk}, \boxed{\mathrm{sk}_1, \ldots, \mathrm{sk}_N}$ **运行 Gen 的人掌握所有私钥**

- 传统定义：仅为广播提供商设计、中心化
- 其他用法：不适宜

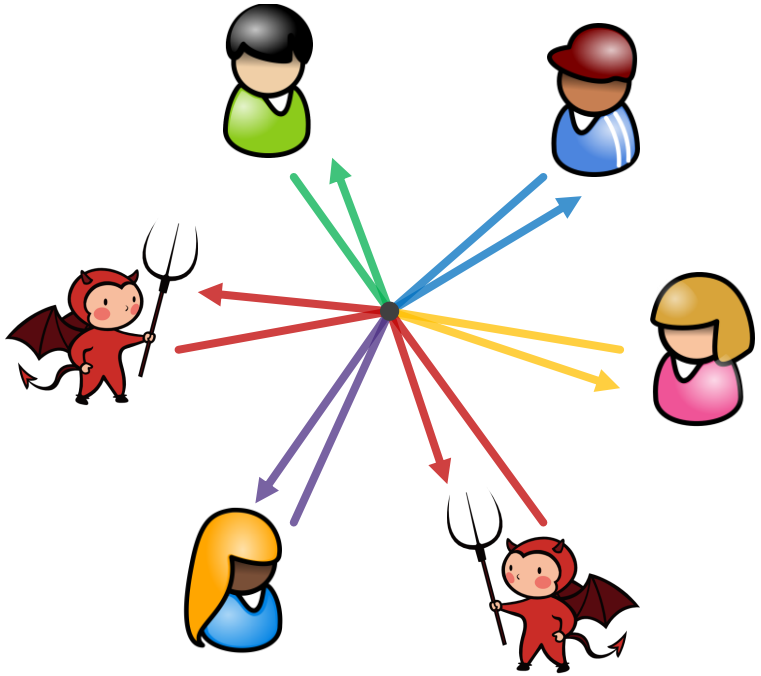


敏感话题群聊

新场景：传统定义无能为力

广播提供商运行 $\mathrm{Gen}(1^N) \to \mathrm{pk}, \boxed{\mathrm{sk}_1, \ldots, \mathrm{sk}_N}$ **运行 Gen 的人掌握所有私钥**

- 传统定义：仅为广播提供商设计、中心化
- 其他用法：不适宜

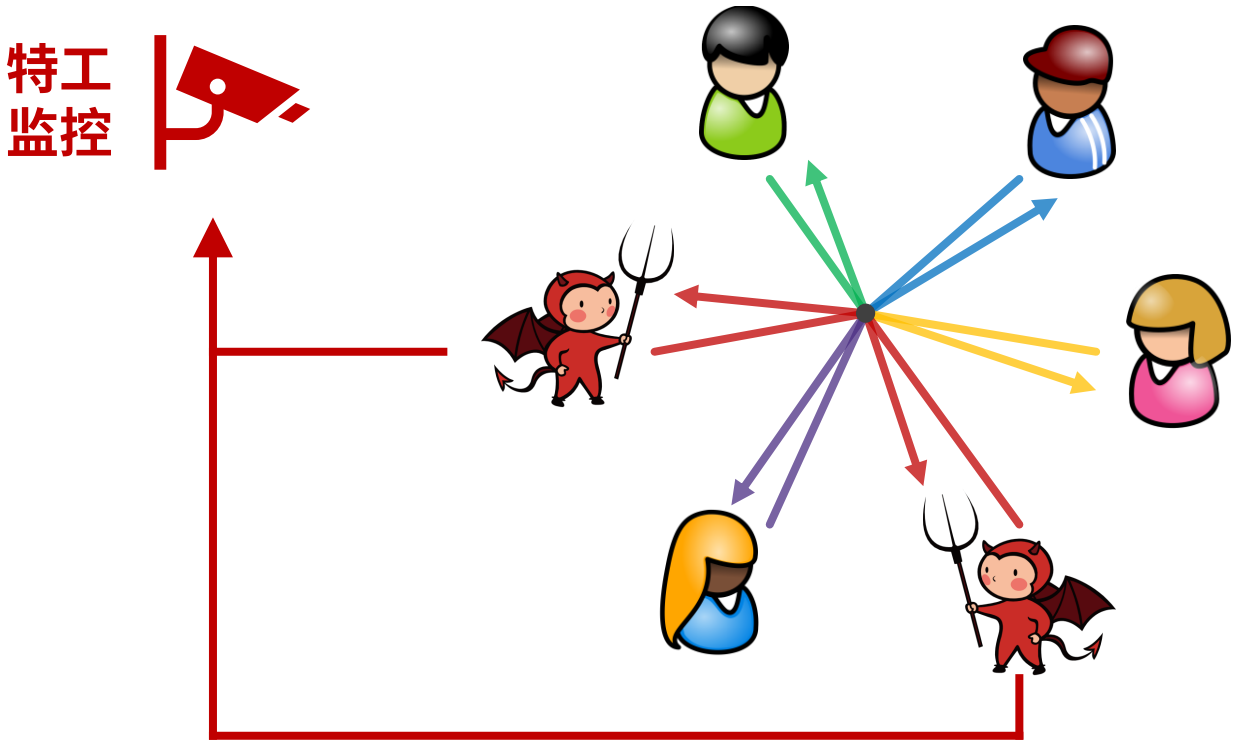


敏感话题群聊

新场景：传统定义无能为力

广播提供商运行 $\mathrm{Gen}(1^N) \to \mathrm{pk}, \mathrm{sk}_1, \ldots, \mathrm{sk}_N$ **运行 Gen 的人掌握所有私钥**

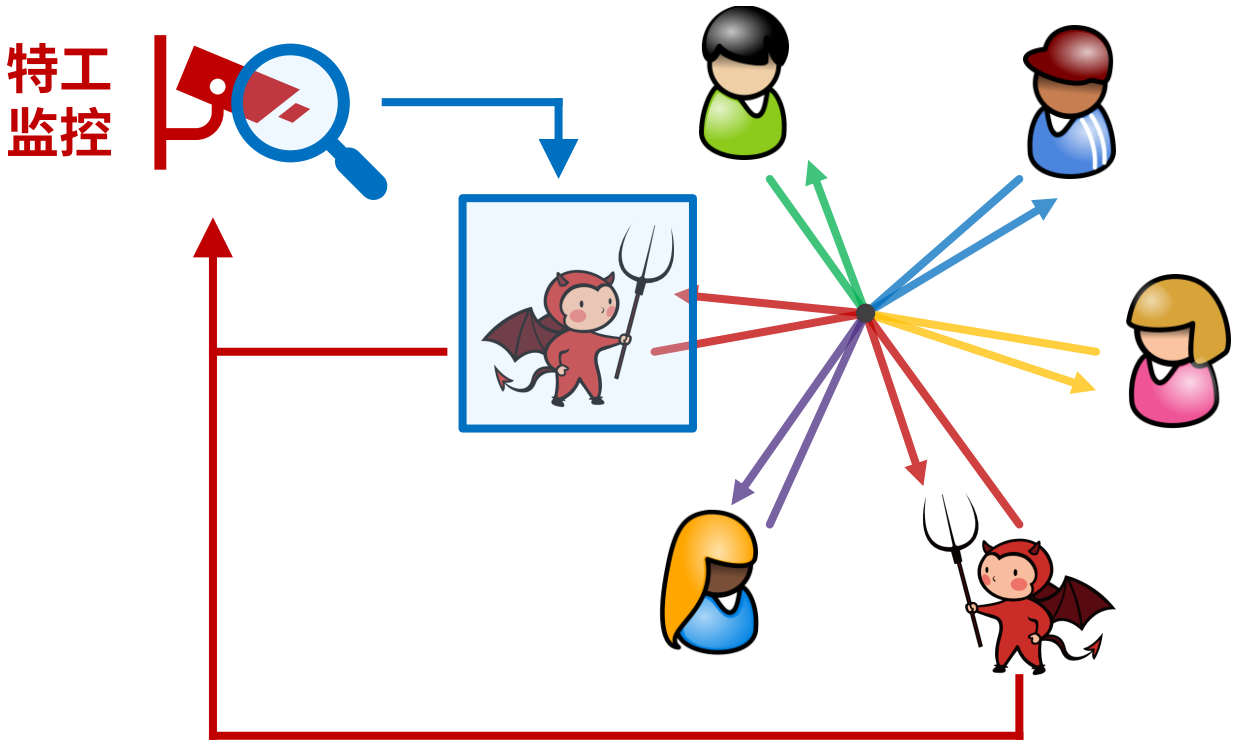
- 传统定义：仅为广播提供商设计、中心化
- 其他用法：不适宜



新场景：传统定义无能为力

广播提供商运行 $\mathrm{Gen}(1^N) \to \mathrm{pk}, \boxed{\mathrm{sk}_1, \ldots, \mathrm{sk}_N}$ **运行 Gen 的人掌握所有私钥**

- 传统定义：仅为广播提供商设计、中心化
- 其他用法：不适宜



敏感话题群聊

新场景：群聊的需求

- 可追踪叛徒

新场景：群聊的需求

- 可追踪叛徒
- 任何人都可能是使坏者 **adversary** 不应掌握他人的密钥

新场景：群聊的需求

- 可追踪叛徒
- 任何人都可能是使坏者 **adversary**
- 入群方便

不应掌握他人的密钥

最好无需交互

新场景：群聊的需求

- 可追踪叛徒
- 任何人都可能是使坏者 **adversary**
- 入群方便

不应掌握他人的密钥

最好无需交互

……

需要某种**去中心化**的叛徒追踪

新场景：群聊的需求

- 可追踪叛徒
- 任何人都可能是使坏者（adversary）　　不应掌握他人的密钥
- 入群方便　　最好无需交互

……

需要某种**去中心化**的叛徒追踪

ad hoc

称作“**自组型叛徒追踪**”

动机、问题

动机、问题

如何**恰当定义**自组型叛徒追踪?

动机、问题

如何**恰当定义**自组型叛徒追踪?

从**什么假设**可以构造它？**效率**如何?

动机、问题

如何**恰当定义**自组型叛徒追踪?

从**什么假设**可以构造它? **效率**如何?

它**效率的下界**是什么?

推演定义：从基本要求出发

目标是
叛徒追踪

推演定义：从基本要求出发

每个用户生成
自己的公私钥对

$$\mathrm{Gen}() \to \mathrm{pk}, \mathrm{sk}$$

目标是
叛徒追踪

推演定义：从基本要求出发

每个用户生成
自己的公私钥对

$$\mathrm{Gen}() \to \mathrm{pk}, \mathrm{sk}$$

目标是
叛徒追踪

$$\mathrm{Enc}(\{\mathrm{pk}_j\}_{j\in[N]}, \mu \in \{0,1\}^{\lambda}) \to \mathrm{ct}$$

推演定义：从基本要求出发

每个用户生成
自己的公私钥对

$$\mathrm{Gen}() \to \mathrm{pk}, \mathrm{sk}$$

目标是
叛徒追踪

$$\mathrm{Enc}(\{\mathrm{pk}_j\}_{j\in[N]}, \mu \in \{0,1\}^\lambda) \to \mathrm{ct}$$

加密之前
收件人列表无限制

推演定义：从基本要求出发

每个用户生成
自己的公私钥对

$$\mathrm{Gen}() \to \mathrm{pk}, \mathrm{sk}$$

~~目标是~~
~~叛徒追踪~~

$$\mathrm{Enc}(\{\mathrm{pk}_j\}_{j\in[N]}, \mu \in \{0,1\}^\lambda) \to \mathrm{ct}$$

加密之前
收件人列表无限制

自然具有
广播、撤销功能

推演定义：从基本要求出发

每个用户生成
自己的公私钥对

$$\mathrm{Gen}() \to \mathrm{pk}, \mathrm{sk}$$

~~目标是~~
~~叛徒追踪~~

$$\mathrm{Enc}(\{\mathrm{pk}_j\}_{j\in[N]}, \mu \in \{0,1\}^\lambda) \to \mathrm{ct}$$

加密之前
收件人列表无限制

自然具有
广播、撤销功能

$$\mathrm{Dec}^{\{\mathrm{pk}_j\}_{j\in[N]},\mathrm{ct}}(N, i, \mathrm{sk}_i) \to \mu$$

推演定义：从基本要求出发

每个用户生成
自己的公私钥对

$$\mathrm{Gen}() \to \mathrm{pk}, \mathrm{sk}$$

~~目标是~~
~~叛徒追踪~~

$$\mathrm{Enc}(\{\mathrm{pk}_j\}_{j\in[N]}, \mu \in \{0,1\}^\lambda) \to \mathrm{ct}$$

加密之前
收件人列表无限制

自然具有
广播、撤销功能

$$\mathrm{Dec}^{\{\mathrm{pk}_j\}_{j\in[N]},\mathrm{ct}}(N, i, \mathrm{sk}_i) \to \mu$$

random-access
可随机访问的输入
Dec 不一定全读，刻画效率

推演定义：从基本要求出发

每个用户生成
自己的公私钥对

$$\mathrm{Gen}() \to \mathrm{pk}, \mathrm{sk}$$

~~目标是~~
~~叛徒追踪~~

$$\mathrm{Enc}(\{\mathrm{pk}_j\}_{j\in[N]}, \mu \in \{0,1\}^\lambda) \to \mathrm{ct}$$

加密之前
收件人列表无限制

自然具有
广播、撤销功能

$$\mathrm{Dec}^{\{\mathrm{pk}_j\}_{j\in[N]},\mathrm{ct}}(N, i, \mathrm{sk}_i) \to \mu$$

random-access
可随机访问的输入
Dec 不一定全读，刻画效率

$$\mathrm{Trace}^{D}(\{\mathrm{pk}_j^*\}_{j\in[N]}, 1^{1/\varepsilon^*}) \to i^* \in [N] \cup \{\perp\}$$

推演定义：从基本要求出发

每个用户生成
自己的公私钥对

$$\mathrm{Gen}() \to \mathrm{pk}, \mathrm{sk}$$

~~目标是~~
~~叛徒追踪~~

$$\mathrm{Enc}(\{\mathrm{pk}_j\}_{j\in[N]}, \mu \in \{0,1\}^\lambda) \to \mathrm{ct}$$

加密之前
收件人列表无限制

自然具有
广播、撤销功能

$$\mathrm{Dec}^{\{\mathrm{pk}_j\}_{j\in[N]},\mathrm{ct}}(N, i, \mathrm{sk}_i) \to \mu$$

random-access
可随机访问的输入
Dec 不一定全读，刻画效率

$$\mathrm{Trace}^{D}(\{\mathrm{pk}_j^*\}_{j\in[N]}, 1^{1/\varepsilon^*}) \to i^* \in [N] \cup \{\perp\}$$

D 让以 $\{\mathbf{pk}_j^*\}_{j\in[N]}$ 为收件人列表的密文不安全 $\Rightarrow$ 能追踪到叛徒

推演定义：从基本要求出发

ad hoc broadcast, trace, and revoke
自组型广播、追踪、撤销 (AH-BTR)

每个用户生成
自己的公私钥对

$$\mathrm{Gen}() \to \mathrm{pk}, \mathrm{sk}$$

~~目标是~~
~~叛徒追踪~~

$$\mathrm{Enc}(\{\mathrm{pk}_j\}_{j\in[N]}, \mu \in \{0,1\}^\lambda) \to \mathrm{ct}$$

加密之前
收件人列表无限制

自然具有
广播、撤销功能

$$\mathrm{Dec}^{\{\mathrm{pk}_j\}_{j\in[N]},\mathrm{ct}}(N, i, \mathrm{sk}_i) \to \mu$$

random-access
可随机访问的输入
Dec 不一定全读，刻画效率

$$\mathrm{Trace}^{D}(\{\mathrm{pk}_j^*\}_{j\in[N]}, 1^{1/\varepsilon^*}) \to i^* \in [N] \cup \{\perp\}$$

D 让以 $\{\mathrm{pk}_j^*\}_{j\in[N]}$ 为收件人列表的密文不安全 $\Rightarrow$ 能追踪到叛徒

推演定义：正确性

通常定义．$\forall N, \mu, i,$

$$\Pr\left[\begin{array}{c}(\mathrm{pk}_j, \mathrm{sk}_j) \xleftarrow{\$} \mathrm{Gen}() \quad \forall j \\ \mathrm{ct} \xleftarrow{\$} \mathrm{Enc}(\{\mathrm{pk}_j\}_{j\in[N]}, \mu) \\ : \ \mathrm{Dec}^{\{\mathrm{pk}_j\}_{j\in[N]},\mathrm{ct}}(N, i, \mathrm{sk}_i) = \mu\end{array}\right] = 1.$$

推演定义：正确性

通常定义．$\forall N, \mu, i,$

$$\Pr\left[\begin{array}{c} \boxed{(\mathrm{pk}_j, \mathrm{sk}_j) \xleftarrow{\$} \mathrm{Gen}() \quad \forall j} \\ \mathrm{ct} \xleftarrow{\$} \mathrm{Enc}(\{\mathrm{pk}_j\}_{j\in[N]}, \mu) \\ : \ \mathrm{Dec}^{\{\mathrm{pk}_j\}_{j\in[N]},\mathrm{ct}}(N, i, \mathrm{sk}_i) = \mu \end{array}\right] = 1.$$

所有密钥都**正常**

推演定义：正确性

通常定义．$\forall N, \mu, i,$

$$\Pr\left[\begin{array}{c}(\mathrm{pk}_j, \mathrm{sk}_j) \xleftarrow{\$} \mathrm{Gen}() \quad \forall j \\ \mathrm{ct} \xleftarrow{\$} \mathrm{Enc}(\{\mathrm{pk}_j\}_{j\in[N]}, \mu) \\ : \ \mathrm{Dec}^{\{\mathrm{pk}_j\}_{j\in[N]},\mathrm{ct}}(N, i, \mathrm{sk}_i) = \mu\end{array}\right] = 1.$$

所有密钥都**正常**

adversarial malformed denial-of-service

担忧．收件人列表有**别有用心**的**异常**公钥，导致**拒绝服务**攻击，
即正常公钥对应的也无法解密

推演定义：正确性

通常定义．$\forall N, \mu, i,$

$$\Pr\left[\begin{array}{c}\boxed{(\mathrm{pk}_j, \mathrm{sk}_j) \xleftarrow{\$} \mathrm{Gen}() \quad \forall j} \\ \mathrm{ct} \xleftarrow{\$} \mathrm{Enc}(\{\mathrm{pk}_j\}_{j\in[N]}, \mu) \\ : \ \mathrm{Dec}^{\{\mathrm{pk}_j\}_{j\in[N]},\mathrm{ct}}(N, i, \mathrm{sk}_i) = \mu\end{array}\right] = 1.$$

所有密钥都**正常**

adversarial malformed denial-of-service

担忧．收件人列表有**别有用心**的**异常**公钥，导致**拒绝服务**攻击，
即正常公钥对应的也无法解密

robust correctness

定义**牢靠正确性**排除这种攻击

推演定义：牢靠正确性
robust

推演定义：牢靠正确性

robust

设正常公钥的长度是 ℓ_{pk}，即 $\Pr\left[(\mathrm{pk},\mathrm{sk}) \xleftarrow{\$} \mathrm{Gen}() \ : \ |\mathrm{pk}| = \ell_{\mathrm{pk}}\right] = 1.$

推演定义：牢靠正确性

robust

设正常公钥的长度是 ℓ_{pk}，即 $\Pr\left[(\mathrm{pk},\mathrm{sk}) \xleftarrow{\$} \mathrm{Gen}() \ : \ |\mathrm{pk}| = \ell_{\mathrm{pk}}\right] = 1.$

$\forall N \qquad \forall i \qquad \forall \{\mathrm{pk}_j\}_{j\in[N]\setminus\{i\}}$ s.t. $\forall j: |\mathrm{pk}_j| = \ell_{\mathrm{pk}} \qquad \forall \mu$

推演定义：牢靠正确性
robust

设正常公钥的长度是 ℓ_{pk}，即 $\Pr\left[(\mathrm{pk},\mathrm{sk}) \xleftarrow{\$} \mathrm{Gen}() \ : \ |\mathrm{pk}| = \ell_{\mathrm{pk}}\right] = 1.$

$\forall N \qquad \forall i \qquad \forall \{\mathrm{pk}_j\}_{j\in[N]\setminus\{i\}} \text{ s.t. } \forall j: |\mathrm{pk}_j| = \ell_{\mathrm{pk}} \qquad \forall \mu$

$$\Pr\left[\begin{array}{l}(\mathrm{pk}_i,\mathrm{sk}_i) \xleftarrow{\$} \mathrm{Gen}() \\ \qquad \mathrm{ct} \xleftarrow{\$} \mathrm{Enc}(\{\mathrm{pk}_j\}_{j\in[N]},\mu) \\ \qquad : \ \mathrm{Dec}^{\{\mathrm{pk}_j\}_{j\in[N]},\mathrm{ct}}(N,i,\mathrm{sk}_i) = \mu\end{array}\right] = 1.$$

推演定义：牢靠正确性

robust

设正常公钥的长度是 ℓ_{pk}，即 $\Pr\left[(\mathrm{pk},\mathrm{sk}) \xleftarrow{\$} \mathrm{Gen}() \ : \ |\mathrm{pk}| = \ell_{\mathrm{pk}}\right] = 1.$

$\forall N \qquad \forall i \qquad \forall \{\mathrm{pk}_j\}_{j\in[N]\setminus\{i\}} \text{ s.t. } \forall j: |\mathrm{pk}_j| = \ell_{\mathrm{pk}} \qquad \forall \mu$

$$\Pr\left[\begin{array}{c}(\mathrm{pk}_i,\mathrm{sk}_i) \xleftarrow{\$} \mathrm{Gen}() \\ \mathrm{ct} \xleftarrow{\$} \mathrm{Enc}(\{\mathrm{pk}_j\}_{j\in[N]},\mu) \\ : \ \mathrm{Dec}^{\{\mathrm{pk}_j\}_{j\in[N]},\mathrm{ct}}(N,i,\mathrm{sk}_i) = \mu\end{array}\right] = 1.$$

异常 pk 不影响正常 sk 解密

推演定义：牢靠正确性

robust

设正常公钥的长度是 ℓ_{pk}，即 $\Pr\left[(\mathrm{pk},\mathrm{sk}) \xleftarrow{\$} \mathrm{Gen}() \ : \ |\mathrm{pk}| = \ell_{\mathrm{pk}}\right] = 1.$

$\forall N \qquad \forall i \qquad \forall \{\mathrm{pk}_j\}_{j\in[N]\setminus\{i\}} \text{ s.t. } \forall j: |\mathrm{pk}_j| = \ell_{\mathrm{pk}} \qquad \forall \mu$

$$\Pr\left[\begin{array}{c}(\mathrm{pk}_i,\mathrm{sk}_i) \xleftarrow{\$} \mathrm{Gen}() \\ \mathrm{ct} \xleftarrow{\$} \mathrm{Enc}(\{\mathrm{pk}_j\}_{j\in[N]},\mu) \\ : \ \mathrm{Dec}^{\{\mathrm{pk}_j\}_{j\in[N]},\mathrm{ct}}(N,i,\mathrm{sk}_i) = \mu\end{array}\right] = 1.$$

异常 pk 不影响正常 sk 解密

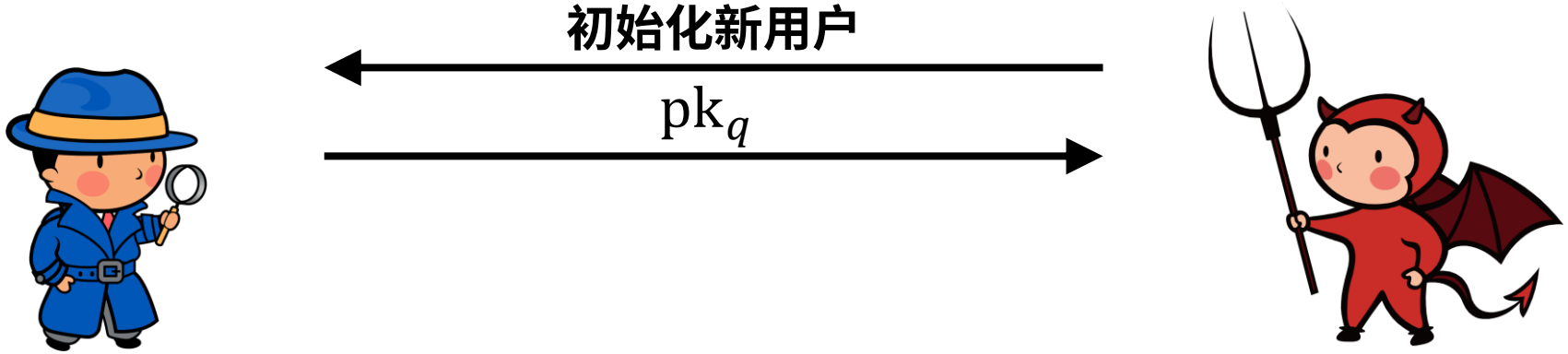
blatantly

不考虑明目张胆异常（长度错误）的 pk

——效率考量

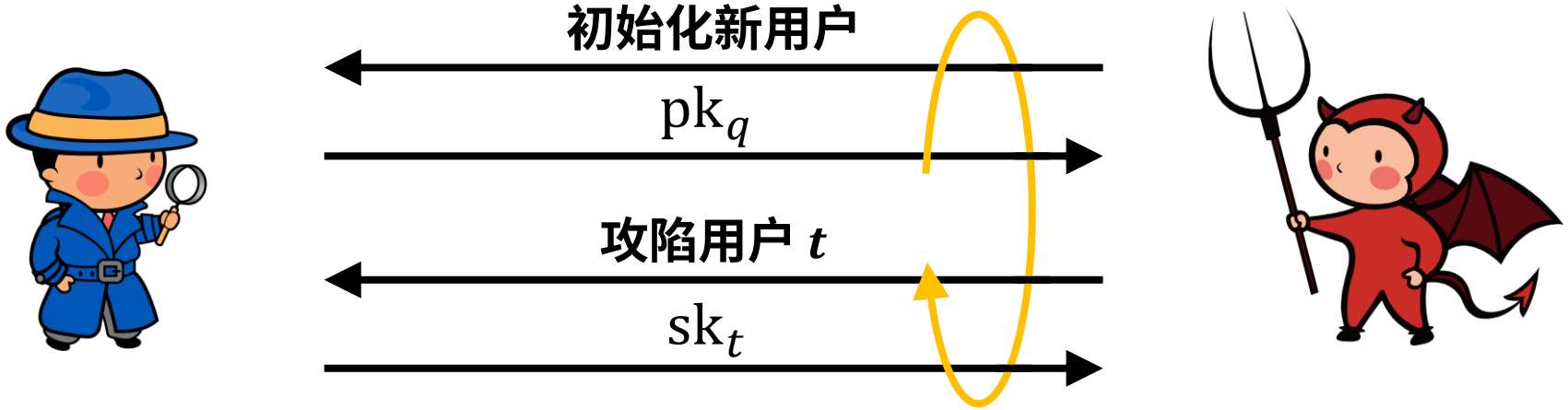
安全定义：可追踪性

安全定义：可追踪性

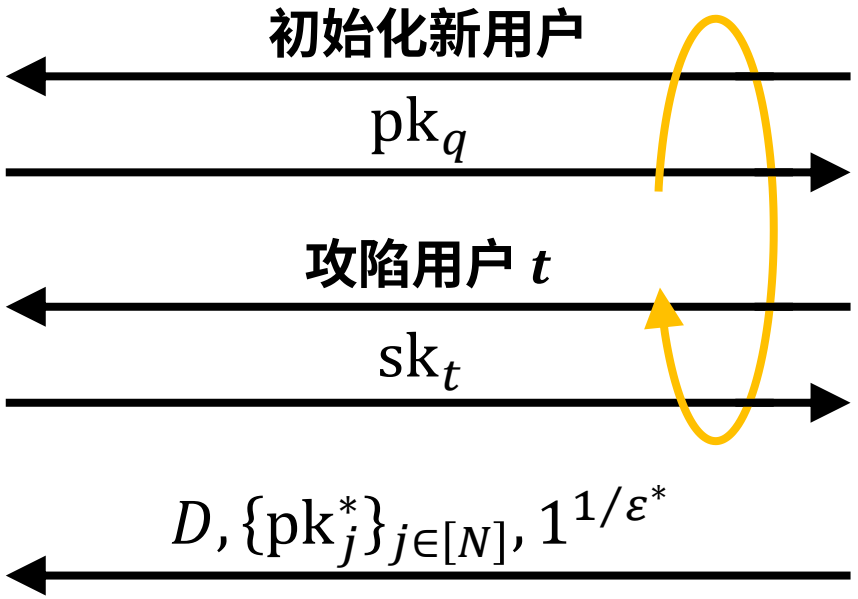


安全定义：可追踪性

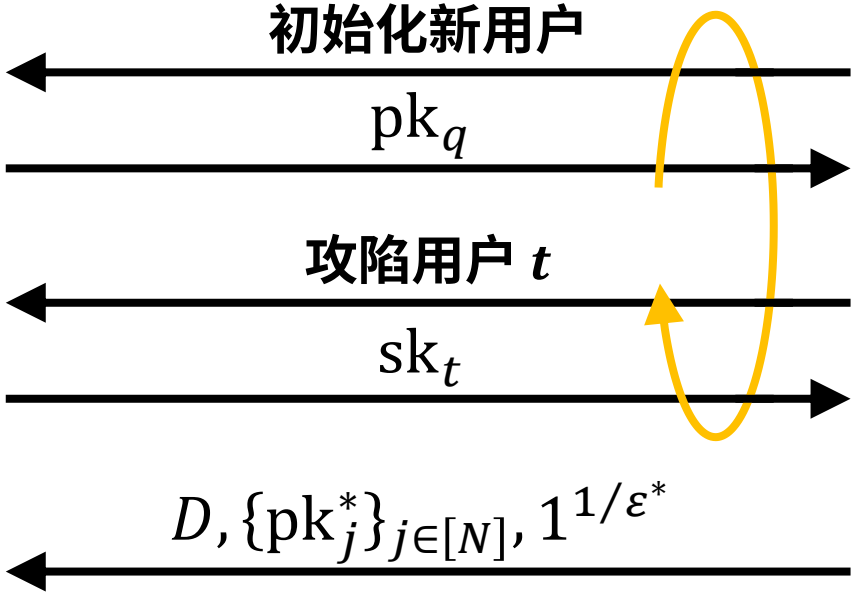
安全定义：可追踪性



安全定义：可追踪性


初始化新用户
pk_q
攻陷用户 t
sk_t
$D, \{\mathrm{pk}_j^*\}_{j\in[N]}, 1^{1/\varepsilon^*}$

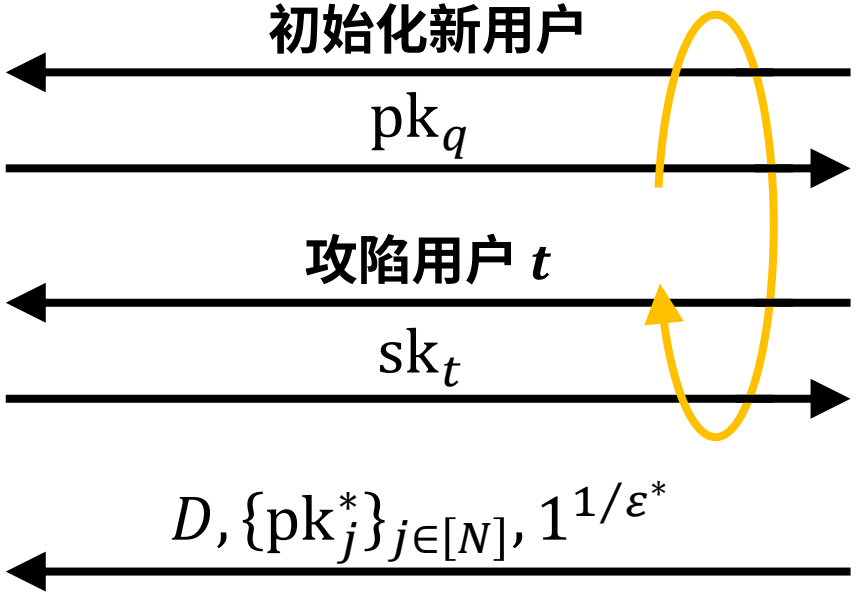
安全定义：可追踪性



$\varepsilon \leftarrow D$ 的区分优势

$i^* \xleftarrow{\$} \mathrm{Trace}^D(\{\mathrm{pk}_j^*\}_{j\in[N]}, 1^{1/\varepsilon^*})$

安全定义：可追踪性



$\varepsilon \leftarrow D$ 的区分优势

$i^* \xleftarrow{\$} \mathrm{Trace}^D(\{\mathrm{pk}_j^*\}_{j\in[N]}, 1^{1/\varepsilon^*})$

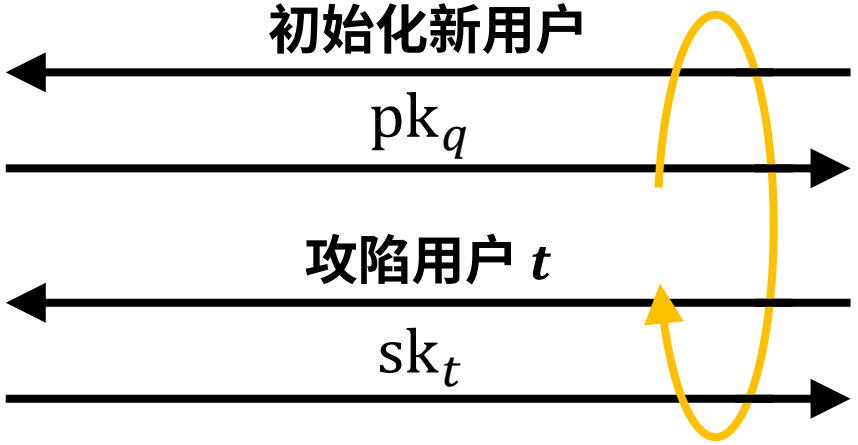
胜利条件.

$i^* \in [N]$ 且 $\mathrm{pk}_{i^*}^*$ 是某个**未被攻陷用户**的公钥

或

$|\varepsilon| \geq \varepsilon^*$ 且 $i^* = \perp$

安全定义：可追踪性



$\varepsilon \leftarrow D$ 的区分优势

$i^* \xleftarrow{\$} \mathrm{Trace}^D(\{\mathrm{pk}_j^*\}_{j\in[N]}, 1^{1/\varepsilon^*})$

胜利条件.

$i^* \in [N]$ 且 $\mathrm{pk}_{i^*}^*$ 是某个**未被攻陷用户**的公钥

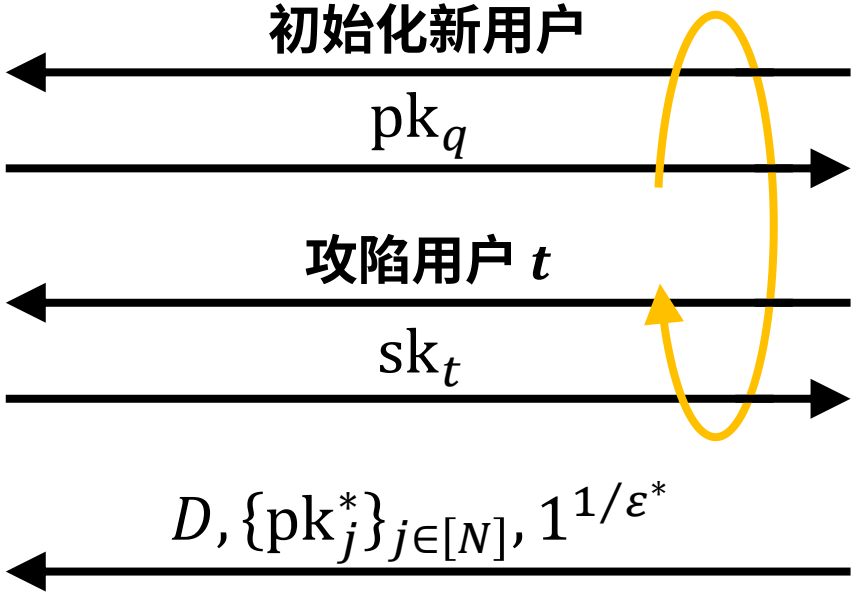
指控了无辜用户

或

$|\varepsilon| \geq \varepsilon^*$ 且 $i^* = \perp$

解码器让加密不安全，但没识别出叛徒

安全定义：可追踪性



$\varepsilon \leftarrow D$ 的区分优势

$i^* \xleftarrow{\$} \mathrm{Trace}^D(\{\mathrm{pk}_j^*\}_{j\in[N]}, 1^{1/\varepsilon^*})$

胜利条件.

$i^* \in [N]$ 且 $\mathrm{pk}_{i^*}^*$ 是某个**未被攻陷用户**的公钥

指控了无辜用户

或

$|\varepsilon| \geq \varepsilon^*$ 且 $i^* = \perp$

解码器让加密不安全，但没识别出叛徒

$\Pr[\text{  } \text{胜利}] \in \mathrm{negl}(\lambda)$

安全定义：可追踪性

初始化新用户

pk_q

攻陷用户 t

sk_t

$\varepsilon \leftarrow D$ 的区分优势

$i^* \xleftarrow{\$} \mathrm{Trace}^D(\{\mathrm{pk}_j^*\}_{j\in[N]}, 1^{1/\varepsilon^*})$

$D, \{\mathrm{pk}_j^*\}_{j\in[N]}, 1^{1/\varepsilon^*}$

胜利条件.

$i^* \in [N]$ 且 $\mathrm{pk}_{i^*}^*$ 是某个**未被攻陷用户**的公钥

指控了无辜用户

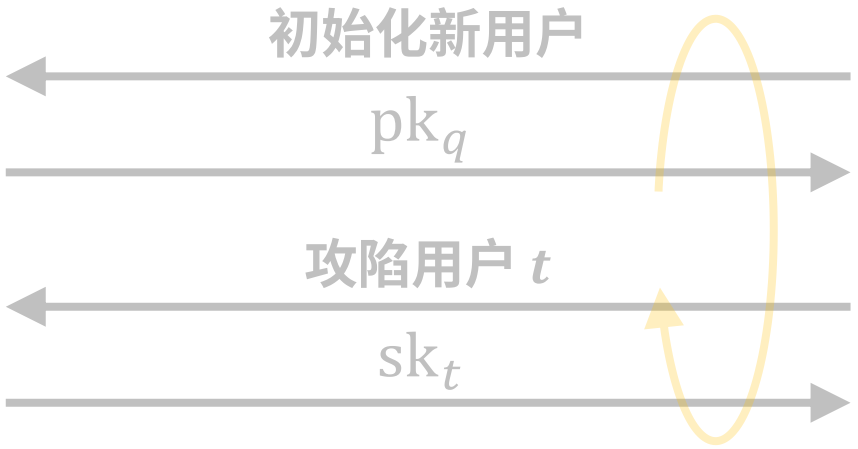
或

$|\varepsilon| \geq \varepsilon^*$ 且 $i^* = \perp$

解码器让加密不安全，但没识别出叛徒

$\Pr[$  胜利$] \in \mathrm{negl}(\lambda)$

安全定义：可追踪性



$\varepsilon \leftarrow D$ 的区分优势

$i^* \xleftarrow{\$} \mathrm{Trace}^D(\{\mathrm{pk}_j^*\}_{j\in[N]}, 1^{1/\varepsilon^*})$

$D, \{\mathrm{pk}_j^*\}_{j\in[N]}, 1^{1/\varepsilon^*}$

pk_j^* 不需要来自挑战者

（Trace 可以指控使坏者自己生成的 pk）

胜利条件.

$i^* \in [N]$ 且 $\mathrm{pk}_{i^*}^*$ 是某个**未被攻陷用户**的公钥

指控了无辜用户

或

$|\varepsilon| \geq \varepsilon^*$ 且 $i^* = \perp$

解码器让加密不安全，但没识别出叛徒

$\Pr[\text{胜利}] \in \mathrm{negl}(\lambda)$

安全定义：可追踪性

初始化新用户

pk_q

攻陷用户 t

sk_t

$\varepsilon \leftarrow D$ 的区分优势

$i^* \xleftarrow{\$} \mathrm{Trace}^D(\{\mathrm{pk}_j^*\}_{j\in[N]}, 1^{1/\varepsilon^*})$

$D, \{\mathrm{pk}_j^*\}_{j\in[N]}, 1^{1/\varepsilon^*}$

pk_j^* 不需要来自挑战者

（Trace 可以指控使坏者自己生成的 pk）

胜利条件.

$i^* \in [N]$ 且 $\mathrm{pk}_{i^*}^*$ 是某个**未被攻陷用户**的公钥

指控了无辜用户

或

$|\varepsilon| \geq \varepsilon^*$ 且 $i^* = \perp$

解码器让加密不安全，
但没识别出叛徒

$\Pr[$  胜利$] \in \mathrm{negl}(\lambda)$

安全定义：可追踪性

初始化新用户

pk_q

攻陷用户 t

sk_t

$\varepsilon \leftarrow D$ 的区分优势

$i^* \xleftarrow{\$} \mathrm{Trace}^D(\{\mathrm{pk}_j^*\}_{j\in[N]}, 1^{1/\varepsilon^*})$

$D, \{\mathrm{pk}_j^*\}_{j\in[N]}, 1^{1/\varepsilon^*}$

pk_j^* 不需要来自挑战者

（Trace 可以指控使坏者自己生成的 pk）

胜利条件：

必须是挑战者初始化的

$i^* \in [N]$ 且 $\mathrm{pk}_{i^*}^*$ 是某个**未被攻陷用户**的公钥

指控了无辜用户

或

$|\varepsilon| \geq \varepsilon^*$ 且 $i^* = \perp$

解码器让加密不安全，
但没识别出叛徒

$\Pr[$  胜利$] \in \mathrm{negl}(\lambda)$

安全定义：可追踪性

初始化新用户

pk_q

攻陷用户 t

sk_t

$\varepsilon \leftarrow D$ 的区分优势

$i^* \xleftarrow{\$} \mathrm{Trace}^D(\{\mathrm{pk}_j^*\}_{j\in[N]}, 1^{1/\varepsilon^*})$

$D, \{\mathrm{pk}_j^*\}_{j\in[N]}, 1^{1/\varepsilon^*}$

pk_j^* 不需要来自挑战者

（Trace 可以指控使坏者自己生成的 pk）

胜利条件：

$i^* \in [N]$ 且 $\mathrm{pk}_{i^*}^*$ 是某个**未被攻陷用户**的公钥

必须是挑战者初始化的

指控了无辜用户

若 $\mathrm{pk}_1 = \mathrm{pk}_2$ 且查询了 sk_2，则 $\mathrm{pk}_1, \mathrm{pk}_2$ 都未被攻陷

排除公钥碰撞

或

$|\varepsilon| \geq \varepsilon^*$ 且 $i^* = \perp$

解码器让加密不安全，但没识别出叛徒

$\Pr[$  胜利$] \in \mathrm{negl}(\lambda)$

安全定义：可追踪性

[Z] 可追踪 ⇒ 语义安全

初始化新用户

pk_q

攻陷用户 t

sk_t

$\varepsilon \leftarrow D$ 的区分优势

$i^* \xleftarrow{\$} \mathrm{Trace}^D(\{\mathrm{pk}_j^*\}_{j\in[N]}, 1^{1/\varepsilon^*})$

$D, \{\mathrm{pk}_j^*\}_{j\in[N]}, 1^{1/\varepsilon^*}$

pk_j^* 不需要来自挑战者

（Trace 可以指控使坏者自己生成的 pk）

胜利条件.

$i^* \in [N]$ 且 $\mathrm{pk}_{i^*}^*$ 是某个**未被攻陷用户**的公钥

必须是挑战者初始化的

指控了无辜用户

或

$|\varepsilon| \geq \varepsilon^*$ 且 $i^* = \perp$

解码器让加密不安全，

但没识别出叛徒

若 $\mathrm{pk}_1 = \mathrm{pk}_2$ 且查询了 sk_2，

则 $\mathrm{pk}_1, \mathrm{pk}_2$ 都未被攻陷

排除公钥碰撞

$\Pr[$  胜利$] \in \mathrm{negl}(\lambda)$

安全定义：可追踪性

[Z] 可追踪 ⟹ 语义安全

初始化新用户

pk_q

攻陷用户 t

sk_t

$\varepsilon \leftarrow D$ 的区分优势

$i^* \xleftarrow{\$} \mathrm{Trace}^D(\{\mathrm{pk}_j^*\}_{j\in[N]}, 1^{1/\varepsilon^*})$

$D, \{\mathrm{pk}_j^*\}_{j\in[N]}, 1^{1/\varepsilon^*}$

pk_j^* 不需要来自挑战者

（Trace 可以指控使坏者自己生成的 pk）

胜利条件.

$i^* \in [N]$ 且 $\mathrm{pk}_{i^*}^*$ 是某个**未被攻陷用户**的公钥

必须是挑战者初始化的

指控了无辜用户

或

$|\varepsilon| \geq \varepsilon^*$ 且 $i^* = \perp$

解码器让加密不安全，

但没识别出叛徒

若 $\mathrm{pk}_1 = \mathrm{pk}_2$ 且查询了 sk_2，

则 $\mathrm{pk}_1, \mathrm{pk}_2$ 都未被攻陷

排除公钥碰撞

$\Pr[$  胜利$] \in \mathrm{negl}(\lambda)$

简化安全定义：完备性与可靠性

completeness soundness

完备性

$D, \{\mathrm{pk}_j^*\}_{j\in[N]}, 1^{1/\varepsilon^*}$

$\varepsilon \leftarrow D$ 的区分优势

$i^* \xleftarrow{\$} \mathrm{Trace}^D(\{\mathrm{pk}_j^*\}_{j\in[N]}, 1^{1/\varepsilon^*})$

胜利条件。 $|\varepsilon| \geq \varepsilon^*$ 且 $i^* = \perp$

简化安全定义：完备性与可靠性

completeness soundness

完备性

$D, \{\mathrm{pk}_j^*\}_{j\in[N]}, 1^{1/\varepsilon^*}$

$\varepsilon \leftarrow D$ 的区分优势

$i^* \xleftarrow{\$} \mathrm{Trace}^D(\{\mathrm{pk}_j^*\}_{j\in[N]}, 1^{1/\varepsilon^*})$

胜利条件．$|\varepsilon| \geq \varepsilon^*$ 且 $i^* = \perp$

可靠性

pk

$D, N, i_\perp^*, \{\mathrm{pk}_j^*\}_{j\in[N]\setminus\{i_\perp^*\}}, 1^{1/\varepsilon^*}$

$\mathrm{pk}_{i_\perp^*}^* \leftarrow \mathrm{pk}$

$i^* \xleftarrow{\$} \mathrm{Trace}^D(\{\mathrm{pk}_j^*\}_{j\in[N]}, 1^{1/\varepsilon^*})$

胜利条件．$i^* = i_\perp^*$

简化安全定义：完备性与可靠性

completeness soundness

简

完备性

$D, \{\mathrm{pk}_j^*\}_{j\in[N]}, 1^{1/\varepsilon^*}$

$\varepsilon \leftarrow D$ 的区分优势

$i^* \xleftarrow{\$} \mathrm{Trace}^D(\{\mathrm{pk}_j^*\}_{j\in[N]}, 1^{1/\varepsilon^*})$

胜利条件．$|\varepsilon| \geq \varepsilon^*$ 且 $i^* = \perp$

定理．AH-BTR 可追踪 ⇔ 完备且可靠

可靠性

pk

$D, N, i_\perp^*, \{\mathrm{pk}_j^*\}_{j\in[N]\setminus\{i_\perp^*\}}, 1^{1/\varepsilon^*}$

$\mathrm{pk}_{i_\perp^*}^* \leftarrow \mathrm{pk}$

$i^* \xleftarrow{\$} \mathrm{Trace}^D(\{\mathrm{pk}_j^*\}_{j\in[N]}, 1^{1/\varepsilon^*})$

胜利条件．$i^* = i_\perp^*$

叛徒追踪与隐私区间广播加密 (PLBE) [BSW]

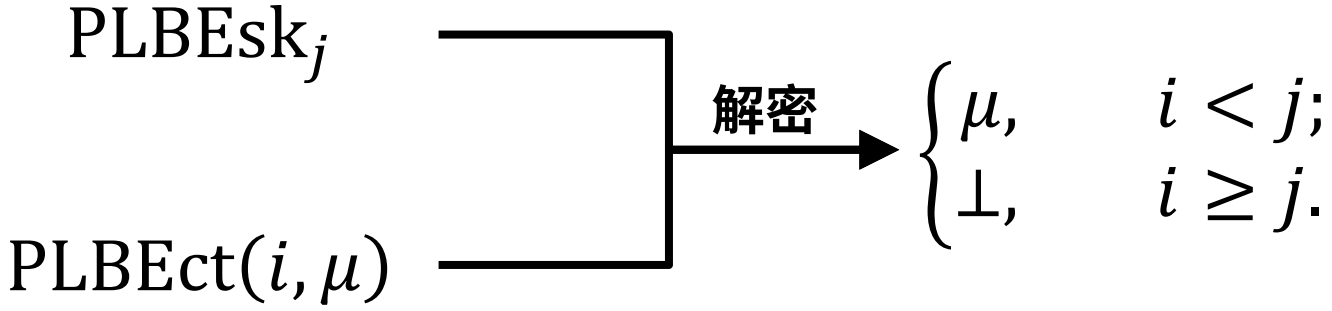
private linear broadcast encryption

PLBEsk_j

$\mathrm{PLBEct}(i, \mu)$

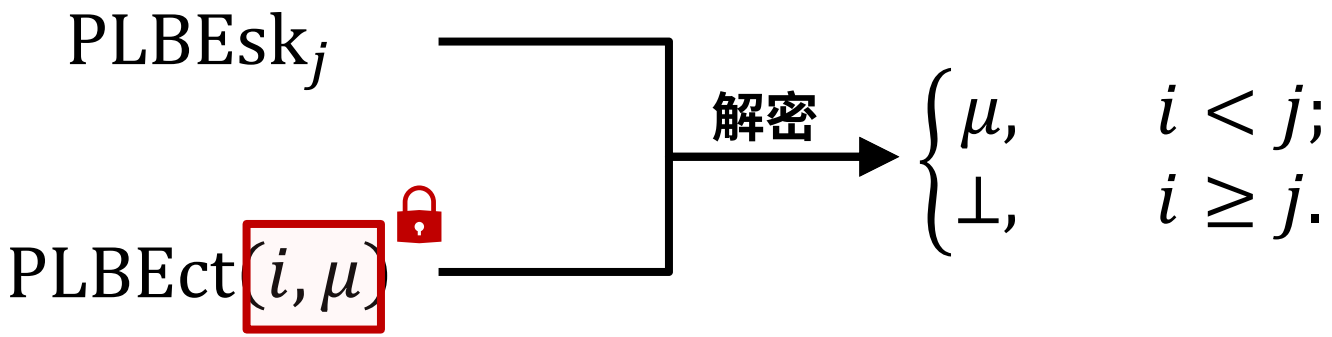
叛徒追踪与隐私区间广播加密 (PLBE) [BSW]

private linear broadcast encryption



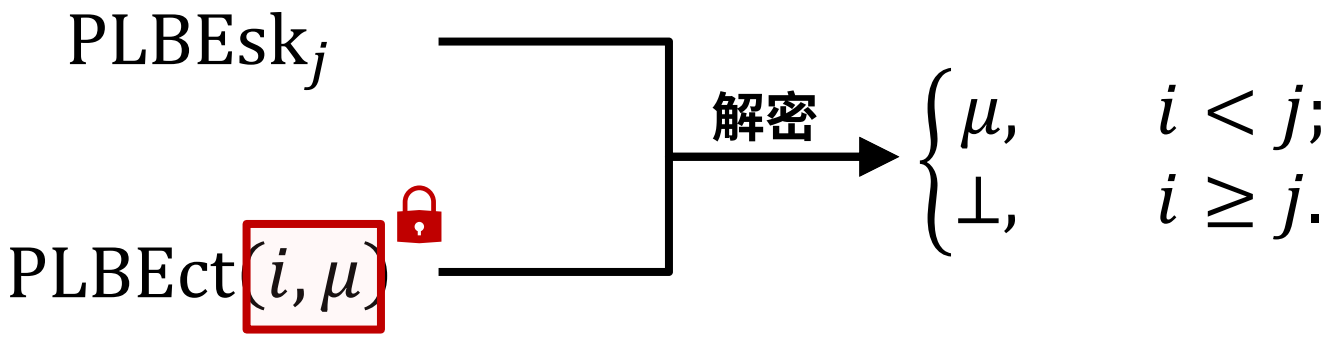
叛徒追踪与隐私区间广播加密 (PLBE) [BSW]

private linear broadcast encryption



叛徒追踪与隐私区间广播加密 (PLBE) [BSW]

private linear broadcast encryption

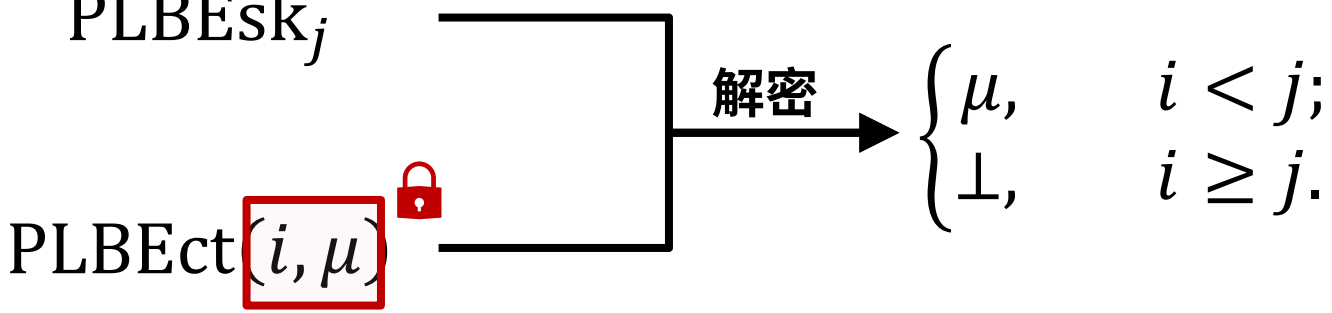


从 **PLBE 到 TT**

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

叛徒追踪与隐私区间广播加密 (PLBE) [BSW]

private linear broadcast encryption



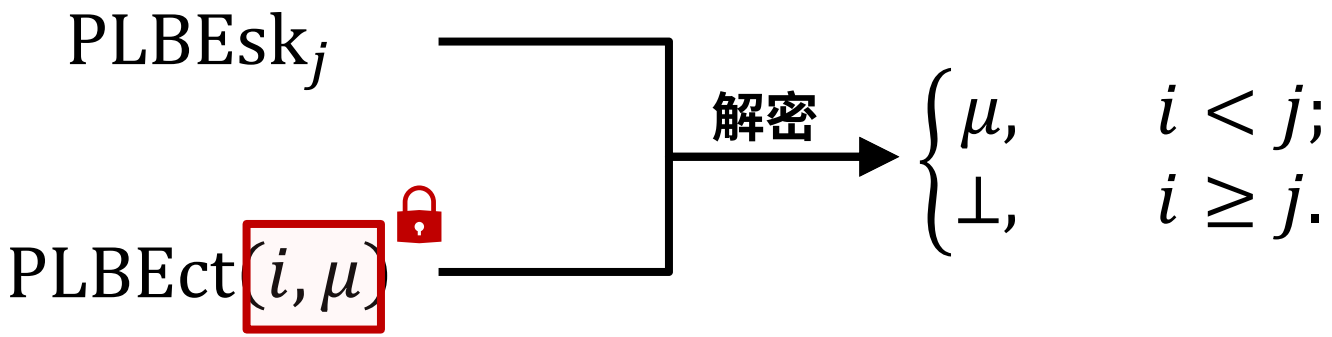
从 **PLBE 到 TT**

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

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

叛徒追踪与隐私区间广播加密 (PLBE) [BSW]

private linear broadcast encryption



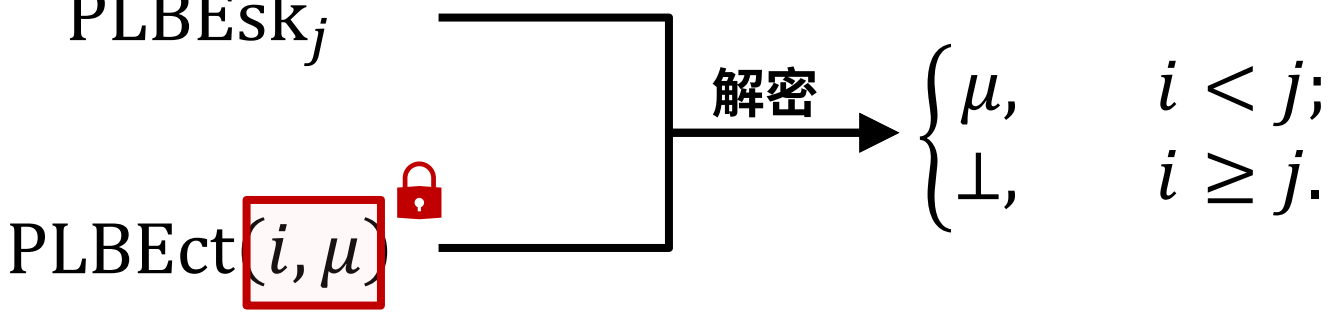
从 **PLBE 到 TT**

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

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

叛徒追踪与隐私区间广播加密 (PLBE) [BSW]

private linear broadcast encryption



从 **PLBE 到 TT**

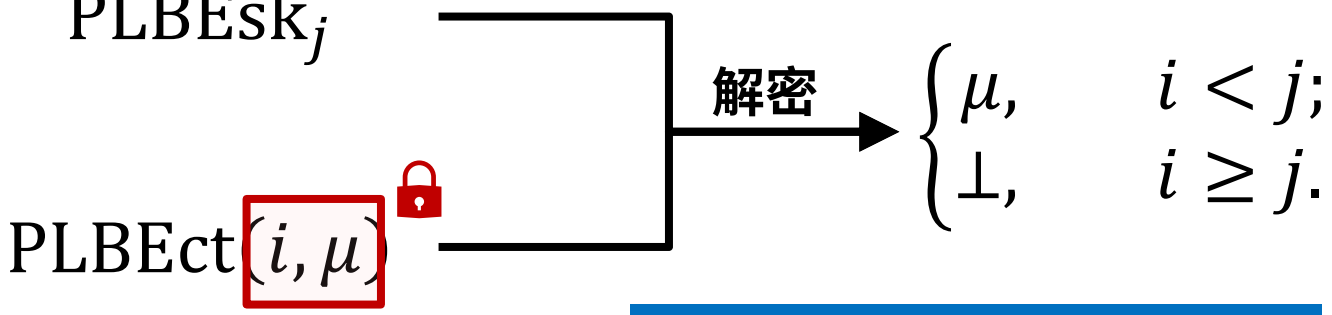
$$\mathrm{TTsk}_j = \mathrm{PLBEsk}_j$$

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

$$\geq \varepsilon^*$$

叛徒追踪与隐私区间广播加密 (PLBE) [BSW]

private linear broadcast encryption



消息隐藏 (message-hiding)

即使掌握 $\mathrm{PLBEsk}_\star$，也有 $\mathrm{PLBEct}(N,\mu)\approx\mathrm{PLBEct}(N,0)$

从 **PLBE 到 TT**

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

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

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

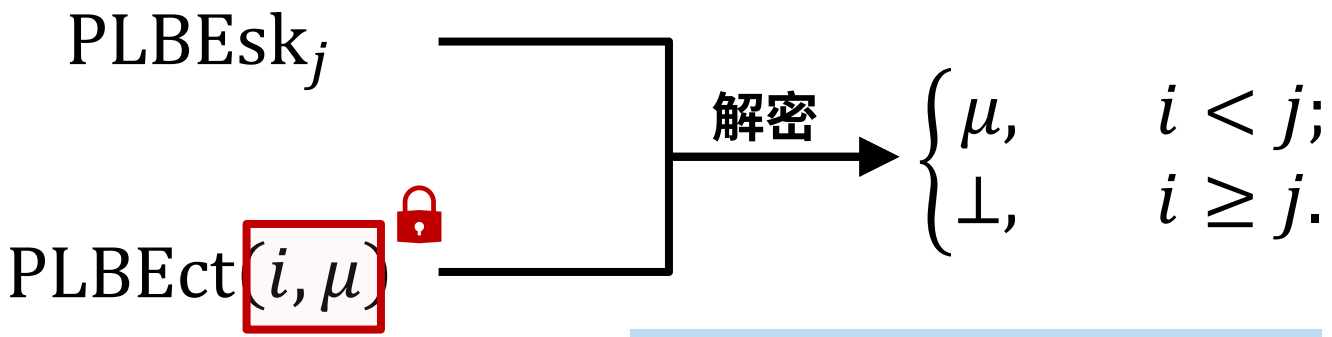
$\geq\varepsilon^*$

消息隐藏： ≈ 0

总共下降 $\Omega(\varepsilon^*)$

叛徒追踪与隐私区间广播加密 (PLBE) [BSW]

private linear broadcast encryption



消息隐藏 (message-hiding)

即使掌握 $\mathrm{PLBEsk}_\star$，也有 $\mathrm{PLBEct}(N,\mu)\approx\mathrm{PLBEct}(N,0)$

从 **PLBE 到 TT**

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

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

下标隐藏 (index-hiding)

即使掌握 $\mathrm{PLBEsk}_{\neq i}$，也有 $\mathrm{PLBEct}(i-1,\mu)\approx\mathrm{PLBEct}(i,\mu)$

$\mathrm{PLBEct}(0,\mu)$ … $\mathrm{PLBEct}(i-1,\mu)$ $\mathrm{PLBEct}(i,\mu)$ … $\mathrm{PLBEct}(N,\mu)$

$\geq\varepsilon^*$

下标隐藏： 若用户 i 无辜，则下降 ≈ 0

若下降 $\Omega(\varepsilon^*/N)$ 则用户 i 是叛徒

消息隐藏： ≈ 0

总共下降 $\Omega(\varepsilon^*)$

自组型隐私区间广播加密 (AH-PLBE)

***ad hoc* private linear broadcast encryption**

$$\mathrm{Gen}() \to \mathrm{pk}, \mathrm{sk}$$

$$\mathrm{Enc}(\{\mathrm{pk}_j\}_{j\in[N]}, i_\perp, \mu \in \{0,1\}^\lambda) \to \mathrm{ct}$$

$$\mathrm{Dec}^{\{\mathrm{pk}_j\}_{j\in[N]},\mathrm{ct}}(N, i, \mathrm{sk}_i) \to \mu \quad (\text{若 } i > i_\perp)$$

自组型隐私区间广播加密 (AH-PLBE)

***ad hoc* private linear broadcast encryption**

$$\mathrm{Gen}() \to \mathrm{pk}, \mathrm{sk}$$

$$\mathrm{Enc}(\{\mathrm{pk}_j\}_{j\in[N]}, i_\perp, \mu \in \{0,1\}^\lambda) \to \mathrm{ct}$$

$$\mathrm{Dec}^{\{\mathrm{pk}_j\}_{j\in[N]},\mathrm{ct}}(N, i, \mathrm{sk}_i) \to \mu \quad (\text{若 } i > i_\perp)$$

牢靠正确性

$$\forall N \ \forall i \ \forall \{\mathrm{pk}_j\}_{j\in[N]\setminus\{i\}} \text{ s.t. } \forall j: |\mathrm{pk}_j| = \ell_{\mathrm{pk}} \ \forall \mu,$$

$$\Pr\left[\begin{array}{c}(\mathrm{pk}_i, \mathrm{sk}_i) \xleftarrow{\$} \mathrm{Gen}() \\ \mathrm{ct} \xleftarrow{\$} \mathrm{Enc}(\{\mathrm{pk}_j\}_{j\in[N]}, 0, \mu) \\ : \ \mathrm{Dec}^{\{\mathrm{pk}_j\}_{j\in[N]},\mathrm{ct}}(N, i, \mathrm{sk}_i) = \mu\end{array}\right] = 1.$$

AH-PLBE 安全性：消息隐藏与下标隐藏

消息隐藏

$$\mathrm{Exp}_{\mathrm{MH}}^{0} \approx \mathrm{Exp}_{\mathrm{MH}}^{1}$$

AH-PLBE 安全性：消息隐藏与下标隐藏

消息隐藏

$$\mathrm{Exp}_{\mathrm{MH}}^{0} \approx \mathrm{Exp}_{\mathrm{MH}}^{1}$$

$\{\mathrm{pk}_j^*\}_{j\in[N]}$

AH-PLBE 安全性：消息隐藏与下标隐藏

消息隐藏

$$\mathrm{Exp}_{\mathrm{MH}}^{0} \approx \mathrm{Exp}_{\mathrm{MH}}^{1}$$

$$\{\mathrm{pk}_j^*\}_{j\in[N]}$$

$$\mu_0 \xleftarrow{\$} \{0,1\}^\lambda, \mu_1 \xleftarrow{\$} \{0,1\}^\lambda$$

$$\mathrm{Enc}(\{\mathrm{pk}_j^*\}_{j\in[N]}, N, \mu_b)$$

AH-PLBE 安全性：消息隐藏与下标隐藏

消息隐藏

$$\mathrm{Exp}_{\mathrm{MH}}^{0} \approx \mathrm{Exp}_{\mathrm{MH}}^{1}$$

$\{\mathrm{pk}_j^*\}_{j\in[N]}$

$\mu_0 \xleftarrow{\$} \{0,1\}^\lambda, \mu_1 \xleftarrow{\$} \{0,1\}^\lambda$

$\mathrm{Enc}(\{\mathrm{pk}_j^*\}_{j\in[N]}, N, \mu_b)$

AH-PLBE 安全性：消息隐藏与下标隐藏

消息隐藏

$\mathrm{Exp}_{\mathrm{MH}}^{0} \approx \mathrm{Exp}_{\mathrm{MH}}^{1}$

$\{\mathrm{pk}_j^*\}_{j\in[N]}$

$\mu_0 \xleftarrow{\$} \{0,1\}^\lambda, \mu_1 \xleftarrow{\$} \{0,1\}^\lambda$

$\mathrm{Enc}(\{\mathrm{pk}_j^*\}_{j\in[N]}, N, \mu_b)$

b'

下标隐藏

$\mathrm{Exp}_{\mathrm{IH}}^{0} \approx \mathrm{Exp}_{\mathrm{IH}}^{1}$

pk

AH-PLBE 安全性：消息隐藏与下标隐藏

消息隐藏

$\mathrm{Exp}^{0}_{\mathrm{MH}} \approx \mathrm{Exp}^{1}_{\mathrm{MH}}$

$\{\mathrm{pk}^*_j\}_{j\in[N]}$

$\mu_0 \xleftarrow{\$} \{0,1\}^\lambda, \mu_1 \xleftarrow{\$} \{0,1\}^\lambda$

$\mathrm{Enc}(\{\mathrm{pk}^*_j\}_{j\in[N]}, N, \mu_b)$

b'

下标隐藏

$\mathrm{Exp}^{0}_{\mathrm{IH}} \approx \mathrm{Exp}^{1}_{\mathrm{IH}}$

pk

$N, i^*_\perp, \{\mathrm{pk}^*_j\}_{j\in[N]\setminus\{i^*_\perp\}}$

AH-PLBE 安全性：消息隐藏与下标隐藏

消息隐藏

$\mathrm{Exp}^{0}_{\mathrm{MH}} \approx \mathrm{Exp}^{1}_{\mathrm{MH}}$

$\{\mathrm{pk}^*_j\}_{j\in[N]}$

$\mu_0 \xleftarrow{\$} \{0,1\}^\lambda, \mu_1 \xleftarrow{\$} \{0,1\}^\lambda$

$\mathrm{Enc}(\{\mathrm{pk}^*_j\}_{j\in[N]}, N, \mu_b)$

b'

下标隐藏

$\mathrm{Exp}^{0}_{\mathrm{IH}} \approx \mathrm{Exp}^{1}_{\mathrm{IH}}$

$\mathrm{pk}^*_{i^*_\perp} \leftarrow \mathrm{pk}$

pk

$N, i^*_\perp, \{\mathrm{pk}^*_j\}_{j\in[N]\setminus\{i^*_\perp\}}$

$\mu \xleftarrow{\$} \{0,1\}^\lambda$

$\mathrm{Enc}(\{\mathrm{pk}^*_j\}_{j\in[N]}, i^*_\perp - 1 + b, \mu)$

b'

AH-PLBE 安全性：消息隐藏与下标隐藏

消息隐藏

$$\mathrm{Exp}^{0}_{\mathrm{MH}} \approx \mathrm{Exp}^{1}_{\mathrm{MH}}$$

$\{\mathrm{pk}^*_j\}_{j\in[N]}$

$\mu_0 \xleftarrow{\$} \{0,1\}^\lambda, \mu_1 \xleftarrow{\$} \{0,1\}^\lambda$

$\mathrm{Enc}(\{\mathrm{pk}^*_j\}_{j\in[N]}, N, \mu_b)$

b'

定理． AH-PLBE $\Longrightarrow$ AH-BTR；消息隐藏 $\Longrightarrow$ 完备性；下标隐藏 $\Longrightarrow$ 可靠性

下标隐藏

$$\mathrm{Exp}^{0}_{\mathrm{IH}} \approx \mathrm{Exp}^{1}_{\mathrm{IH}}$$

$\mathrm{pk}^*_{i^*_\perp} \leftarrow \mathrm{pk}$

pk

$N, i^*_\perp, \{\mathrm{pk}^*_j\}_{j\in[N]\setminus\{i^*_\perp\}}$

$\mu \xleftarrow{\$} \{0,1\}^\lambda$

$\mathrm{Enc}(\{\mathrm{pk}^*_j\}_{j\in[N]}, i^*_\perp - 1 + b, \mu)$

b'

构造 AH-PLBE：从朴素方案出发

naïve

$$\mathrm{pk} = \mathrm{PKEpk}, \quad \mathrm{sk} = \mathrm{PKEsk},$$

$$\mathrm{ct}(\{\mathrm{pk}_j\}_{j\in[N]}, i_\perp, \mu) = \{\mathrm{PKEct}_j(\mathrm{pk}_j, \perp)\}_{j\le i_\perp}, \{\mathrm{PKEct}_j(\mathrm{pk}_j, \mu)\}_{j>i_\perp}.$$

构造 AH-PLBE：从朴素方案出发

naïve

$$\mathrm{pk} = \mathrm{PKEpk}, \quad \mathrm{sk} = \mathrm{PKEsk},$$

$|\mathbf{ct}| = \boldsymbol{\Omega}(\boldsymbol{N})$

$$\mathrm{ct}(\{\mathrm{pk}_j\}_{j\in[N]}, i_\perp, \mu) = \{\mathrm{PKEct}_j(\mathrm{pk}_j, \perp)\}_{j\le i_\perp}, \{\mathrm{PKEct}_j(\mathrm{pk}_j, \mu)\}_{j>i_\perp}.$$

构造 AH-PLBE：从朴素方案出发

naïve

$$\mathrm{pk} = \mathrm{PKEpk}, \quad \mathrm{sk} = \mathrm{PKEsk},$$

$|\mathrm{ct}| = \Omega(N)$

$$\mathrm{ct}(\{\mathrm{pk}_j\}_{j\in[N]}, i_\perp, \mu) = \{\mathrm{PKEct}_j(\mathrm{pk}_j, \perp)\}_{j\le i_\perp}, \{\mathrm{PKEct}_j(\mathrm{pk}_j, \mu)\}_{j>i_\perp}.$$

PKE 语义安全 ⟹ PLBE 消息隐藏、下标隐藏

构造 AH-PLBE：从朴素方案出发

naïve

$$\mathrm{pk} = \mathrm{PKEpk}, \quad \mathrm{sk} = \mathrm{PKEsk},$$

$|\mathrm{ct}| = \Omega(N)$

$$\mathrm{ct}(\{\mathrm{pk}_j\}_{j\in[N]}, i_\perp, \mu) = \{\mathrm{PKEct}_j(\mathrm{pk}_j, \perp)\}_{j\le i_\perp}, \{\mathrm{PKEct}_j(\mathrm{pk}_j, \mu)\}_{j>i_\perp}.$$

PKE 语义安全 $\Longrightarrow$ PLBE 消息隐藏、下标隐藏

令 ct 为**程序** $\mathrm{GetCT}(i \in [N]) \to \mathrm{PKEct}_i$ 的**短代码**？（用**程序混淆**（obfuscation）保证安全）

构造 AH-PLBE：从朴素方案出发

naïve

$$\mathrm{pk} = \mathrm{PKEpk}, \quad \mathrm{sk} = \mathrm{PKEsk},$$

$|\mathrm{ct}| = \Omega(N)$

$$\mathrm{ct}(\{\mathrm{pk}_j\}_{j\in[N]}, i_\perp, \mu) = \{\mathrm{PKEct}_j(\mathrm{pk}_j, \perp)\}_{j\le i_\perp}, \{\mathrm{PKEct}_j(\mathrm{pk}_j, \mu)\}_{j>i_\perp}.$$

PKE 语义安全 ⟹ PLBE 消息隐藏、下标隐藏

令 ct 为**程序** $\mathrm{GetCT}(i \in [N]) \to \mathrm{PKEct}_i$ 的**短代码**？（用**程序混淆**（obfuscation）保证安全）

GetCT 必须**知道**所有 pk（列表的熵可达 $\Omega(N)$），代码长度是 $\Omega(N)$

构造 AH-PLBE：从朴素方案出发

naïve

$$\mathrm{pk} = \mathrm{PKEpk}, \quad \mathrm{sk} = \mathrm{PKEsk}, \qquad \boxed{|\mathrm{ct}| = \Omega(N)}$$

$$\mathrm{ct}(\{\mathrm{pk}_j\}_{j\in[N]}, i_\perp, \mu) = \{\mathrm{PKEct}_j(\mathrm{pk}_j, \perp)\}_{j\le i_\perp}, \{\mathrm{PKEct}_j(\mathrm{pk}_j, \mu)\}_{j>i_\perp}.$$

PKE 语义安全 ⟹ PLBE 消息隐藏、下标隐藏

obfuscation

令 ct 为**程序** $\mathrm{GetCT}(i \in [N]) \to \mathrm{PKEct}_i$ 的**短代码**？（用**程序混淆**保证安全）

GetCT 必须**知道**所有 pk（列表的熵可达 $\Omega(N)$），代码长度是 $\Omega(N)$

garbled circuits

用**乱码电路**：$\mathrm{GetCT}(i \in [N]) \to \hat{C}_i$ 是 $C_i(\mathrm{pk}_i) \to \mathrm{PKEct}_i$ 的**乱码化**

garbling

构造 AH-PLBE：从朴素方案出发

naïve

$$\mathrm{pk} = \mathrm{PKEpk}, \quad \mathrm{sk} = \mathrm{PKEsk},$$

$|\mathrm{ct}| = \Omega(N)$

$$\mathrm{ct}(\{\mathrm{pk}_j\}_{j\in[N]}, i_\perp, \mu) = \{\mathrm{PKEct}_j(\mathrm{pk}_j, \perp)\}_{j\le i_\perp}, \{\mathrm{PKEct}_j(\mathrm{pk}_j, \mu)\}_{j>i_\perp}.$$

PKE 语义安全 ⟹ PLBE 消息隐藏、下标隐藏

令 ct 为**程序** $\mathrm{GetCT}(i \in [N]) \to \mathrm{PKEct}_i$ 的**短代码**？（用**程序混淆**保证安全）

obfuscation

GetCT 必须**知道**所有 pk（列表的熵可达 $\Omega(N)$），代码长度是 $\Omega(N)$

garbled circuits

用**乱码电路**：$\mathrm{GetCT}(i \in [N]) \to \hat{C}_i$ 是 $C_i(\mathrm{pk}_i) \to \mathrm{PKEct}_i$ 的**乱码化**

garbling

- GetCT 不用知道 pk，代码长度是 $O(1)$

构造 AH-PLBE：从朴素方案出发

naïve

$$\mathrm{pk} = \mathrm{PKEpk}, \quad \mathrm{sk} = \mathrm{PKEsk}, \qquad \boxed{|\mathrm{ct}| = \Omega(N)}$$

$$\mathrm{ct}(\{\mathrm{pk}_j\}_{j\in[N]}, i_\perp, \mu) = \{\mathrm{PKEct}_j(\mathrm{pk}_j, \perp)\}_{j\le i_\perp}, \{\mathrm{PKEct}_j(\mathrm{pk}_j, \mu)\}_{j>i_\perp}.$$

PKE 语义安全 ⟹ PLBE 消息隐藏、下标隐藏

令 ct 为**程序** $\mathrm{GetCT}(i \in [N]) \to \mathrm{PKEct}_i$ 的**短代码**？（用**程序混淆**保证安全）

obfuscation

GetCT 必须**知道**所有 pk（列表的熵可达 $\Omega(N)$），代码长度是 $\Omega(N)$

garbled circuits

用**乱码电路**：$\mathrm{GetCT}(i \in [N]) \to \hat{C}_i$ 是 $C_i(\mathrm{pk}_i) \to \mathrm{PKEct}_i$ 的**乱码化**

garbling

- ✓ GetCT 不用知道 pk，代码长度是 $O(1)$
- ? 如何选择 $\hat{C}_i$ 的**标签**？（对应 pk_i）

labels

构造 AH-PLBE：从朴素方案出发

naïve

$$\mathrm{pk} = \mathrm{PKEpk}, \quad \mathrm{sk} = \mathrm{PKEsk},$$

$|\mathrm{ct}| = \Omega(N)$

$$\mathrm{ct}(\{\mathrm{pk}_j\}_{j\in[N]}, i_\perp, \mu) = \{\mathrm{PKEct}_j(\mathrm{pk}_j, \perp)\}_{j\le i_\perp}, \{\mathrm{PKEct}_j(\mathrm{pk}_j, \mu)\}_{j>i_\perp}.$$

PKE 语义安全 ⟹ PLBE 消息隐藏、下标隐藏

令 ct 为**程序** $\mathrm{GetCT}(i \in [N]) \to \mathrm{PKEct}_i$ 的**短代码**？（用**程序混淆**保证安全）

obfuscation

GetCT 必须**知道**所有 pk（列表的熵可达 $\Omega(N)$），代码长度是 $\Omega(N)$

garbled circuits

用**乱码电路**：$\mathrm{GetCT}(i \in [N]) \to \hat{C}_i$ 是 $C_i(\mathrm{pk}_i) \to \mathrm{PKEct}_i$ 的**乱码化**

garbling

- ✓ GetCT 不用知道 pk，代码长度是 $O(1)$
- ? 如何选择 $\hat{C}_i$ 的**标签**？（对应 pk_i）

labels

凝练的安全选择

laconic OT

工具：不可区分安全的混淆、乱码电路

indistinguishability obfuscation **garbled circuits**

工具：不可区分安全的混淆、乱码电路

indistinguishability obfuscation **garbled circuits**

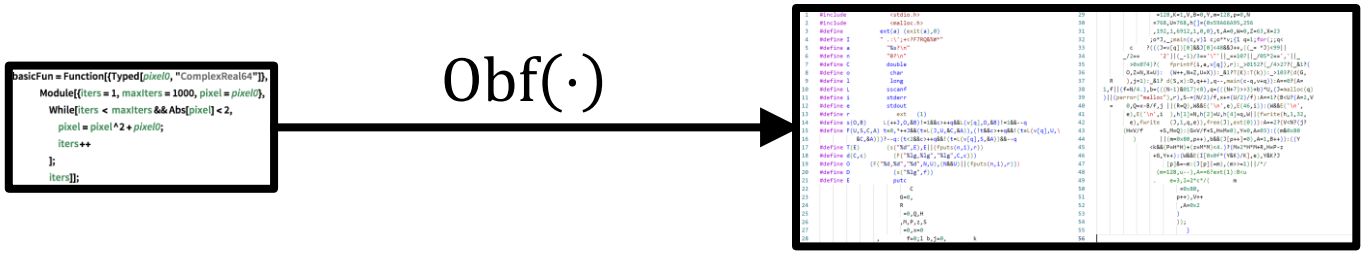
```
basicFun = Function[{Typed[pixel0, "ComplexReal64"]},
    Module[{iters = 1, maxIters = 1000, pixel = pixel0},
      While[iters < maxIters && Abs[pixel] < 2,
        pixel = pixel^2 + pixel0;
        iters++
      ];
      iters]];
```

$\mathrm{Obf}(\cdot)$

$= \tilde{C}$

工具：不可区分安全的混淆、乱码电路

indistinguishability obfuscation　　garbled circuits

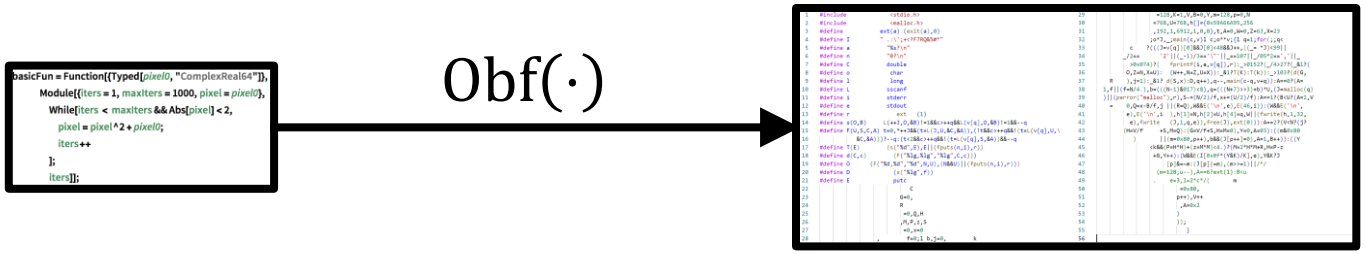


正确．$\forall C, x\colon\ \tilde{C}(x) = C(x)$

安全．$|C_0| = |C_1|$ 且 $\forall x\colon\ C_0(x) = C_1(x)$，则 $\mathrm{Obf}(C_0) \approx \mathrm{Obf}(C_1)$

工具：不可区分安全的混淆、乱码电路

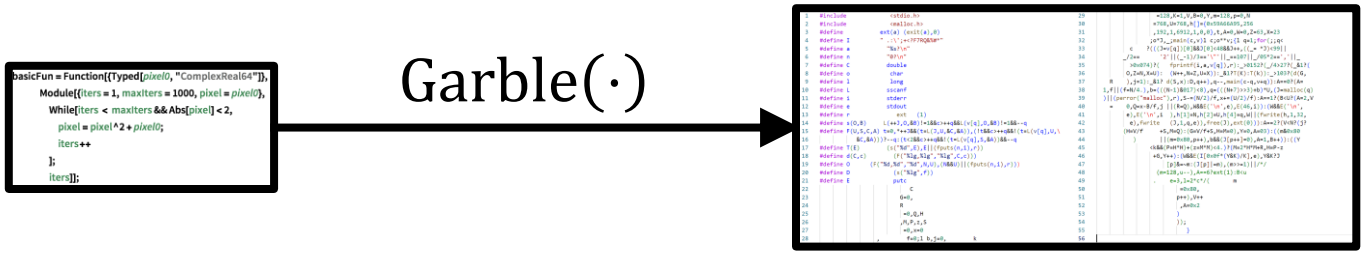
indistinguishability obfuscation　　garbled circuits



$= \tilde{C}$

正确. $\forall C, x\colon\ \tilde{C}(x) = C(x)$

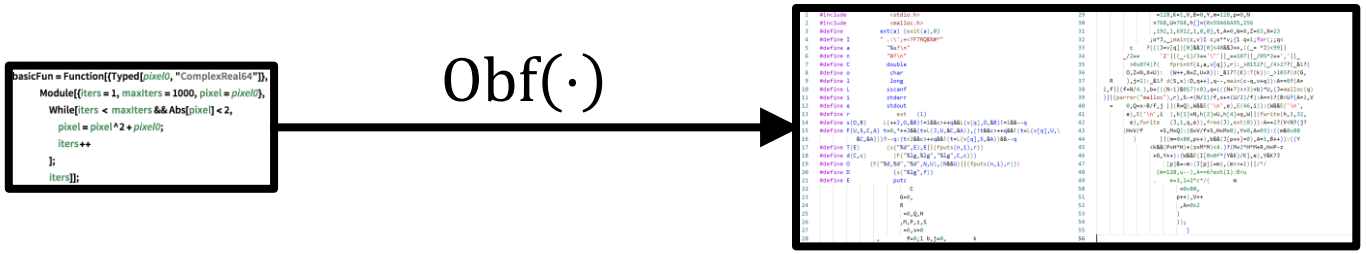
安全. $|C_0| = |C_1|$ 且 $\forall x\colon\ C_0(x) = C_1(x)$，则 $\mathrm{Obf}(C_0) \approx \mathrm{Obf}(C_1)$



$= \hat{C}, \left\{L_i^b\right\}_{i\in[|x|]}^{b\in\{0,1\}}$

工具：不可区分安全的混淆、乱码电路

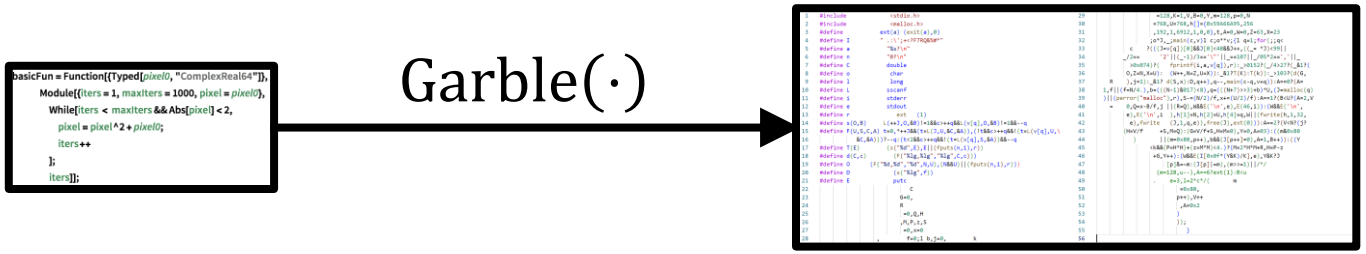
indistinguishability obfuscation **garbled circuits**



$= \tilde{C}$

正确. $\forall C, x\colon\ \tilde{C}(x) = C(x)$

安全. $|C_0| = |C_1|$ 且 $\forall x\colon\ C_0(x) = C_1(x)$，则 $\mathrm{Obf}(C_0) \approx \mathrm{Obf}(C_1)$



$= \hat{C}, \{L_i^b\}_{i\in[|x|]}^{b\in\{0,1\}}$

正确. $\forall C, x\colon\ \hat{C}(\{L_i^{x_i}\}_{i\in[|x|]}) = C(x)$

安全. $(\hat{C}, \{L_i^{x_i}\}_{i\in[|x|]}) \approx \mathrm{Sim}(1^{|C|}, 1^{|x|}, C(x))$

工具：凝练的安全选择

laconic oblivious transfer

D

工具：凝练的安全选择
laconic oblivious transfer

$$D \xrightarrow[\text{确定性算法}]{\mathrm{Hash}(\mathrm{hk},\cdot)} h, \widehat{D} \qquad |h| = \mathrm{O}(1)$$

工具：凝练的安全选择
laconic oblivious transfer

$$D \xrightarrow[\text{确定性算法}]{\mathrm{Hash}(\mathrm{hk},\cdot)} h, \widehat{D} \qquad |h| = \mathrm{O}(1)$$

$$\mathrm{Send}(h, i, L_0, L_1) \to \mathrm{ct}$$

依 $D[i]$ 选择 L_0, L_1 之一

工具：凝练的安全选择
laconic oblivious transfer

$$D \xrightarrow[\text{确定性算法}]{\text{Hash}(\text{hk},\cdot)} h, \widehat{D}$$

$|h| = \text{O}(1)$

$\text{Send}(h, i, L_0, L_1) \to \text{ct}$

依 $D[i]$ 选择 L_0, L_1 之一

凝练。 Send 只需要 h（不需要 D）

工具：凝练的安全选择
laconic oblivious transfer

$$D \xrightarrow[\text{确定性算法}]{\text{Hash}(\text{hk},\cdot)} h, \widehat{D} \qquad |h| = \text{O}(1)$$

$$\text{Send}(h, i, L_0, L_1) \to \text{ct}$$

依 $D[i]$ 选择 L_0, L_1 之一

凝练。 Send 只需要 h（不需要 D）

$$\text{Recv}^{\widehat{D}}(h, i, \text{ct}) \to L_{D[i]}$$

工具：凝练的安全选择
laconic oblivious transfer

$$D \xrightarrow[\text{确定性算法}]{\mathrm{Hash}(\mathrm{hk},\cdot)} h, \widehat{D} \qquad |h| = \mathrm{O}(1)$$

$$\mathrm{Send}(h, i, L_0, L_1) \to \mathrm{ct}$$

依 $D[i]$ 选择 L_0, L_1 之一

凝练. Send 只需要 h（不需要 D）

$$\mathrm{Recv}^{\widehat{D}}(h, i, \mathrm{ct}) \to L_{D[i]}$$

安全性. 不能获取**没有被选择**的消息：

$$(\mathrm{hk}, D, i, L_0, L_1, \mathrm{Send}(h, i, L_0, L_1)) \approx (\cdots, \mathrm{SimSend}(\mathrm{hk}, D, i, L_{D[i]}))$$

构造 AH-PLBE：大炮开火！

heavy hammers

$$\mathrm{pk} = \mathrm{PKEpk}, \quad \mathrm{sk} = \mathrm{PKEsk},$$

$$\mathrm{ct}(\{\mathrm{pk}_j\}_{j\in[N]}, i_\perp, \mu) = \mathrm{hk}, h, \widetilde{\mathrm{GenCT}} = \mathrm{Obf}(\mathrm{GenCT}[\mathrm{hk}, h, i_\perp, \mu, k])$$

$$(h, \widetilde{D}) = \mathrm{Hash}(\mathrm{hk}, \mathrm{pk}_1 \| \cdots \| \mathrm{pk}_N)$$

构造 AH-PLBE：大炮开火！

heavy hammers

$$\mathrm{pk} = \mathrm{PKEpk}, \quad \mathrm{sk} = \mathrm{PKEsk},$$

$$\mathrm{ct}(\{\mathrm{pk}_j\}_{j\in[N]}, i_\perp, \mu) = \mathrm{hk}, h, \widetilde{\mathrm{GenCT}} = \mathrm{Obf}(\mathrm{GenCT}[\mathrm{hk}, h, i_\perp, \mu, k])$$

$$(h, \widetilde{D}) = \mathrm{Hash}(\mathrm{hk}, \mathrm{pk}_1 \| \cdots \| \mathrm{pk}_N)$$

电路 $\mathrm{GenCT}[\mathrm{hk}, h, i_\perp, \mu, k](i \in [N])$

- 用 $\mathrm{PRF}(k, i)$ 产生各种所需的随机数

构造 AH-PLBE：大炮开火！

heavy hammers

$$\mathrm{pk} = \mathrm{PKEpk}, \quad \mathrm{sk} = \mathrm{PKEsk},$$

$$\mathrm{ct}(\{\mathrm{pk}_j\}_{j\in[N]}, i_\perp, \mu) = \mathrm{hk}, h, \widetilde{\mathrm{GenCT}} = \mathrm{Obf}(\mathrm{GenCT}[\mathrm{hk}, h, i_\perp, \mu, k])$$

$$(h, \widetilde{D}) = \mathrm{Hash}(\mathrm{hk}, \mathrm{pk}_1 \| \cdots \| \mathrm{pk}_N)$$

电路 $\mathrm{GenCT}[\mathrm{hk}, h, i_\perp, \mu, k](i \in [N])$

- 用 $\mathrm{PRF}(k, i)$ 产生各种所需的随机数
- 输出 $\mathrm{Garble}\left(C\left[\begin{cases}\perp, & i \le i_\perp;\\ \mu, & i > i_\perp;\end{cases}\right]\right)$ 的 $\hat{C}$

电路 $C[\mu'](\mathrm{pk})$

输出 $\mathrm{PKEEnc}(\mathrm{pk}, \mu')$

构造 AH-PLBE：大炮开火！

heavy hammers

$$\mathrm{pk} = \mathrm{PKEpk}, \quad \mathrm{sk} = \mathrm{PKEsk},$$

$$\mathrm{ct}(\{\mathrm{pk}_j\}_{j\in[N]}, i_\perp, \mu) = \mathrm{hk}, h, \widetilde{\mathrm{GenCT}} = \mathrm{Obf}(\mathrm{GenCT}[\mathrm{hk}, h, i_\perp, \mu, k])$$

$$(h, \widetilde{D}) = \mathrm{Hash}(\mathrm{hk}, \mathrm{pk}_1 \| \cdots \| \mathrm{pk}_N)$$

电路 $\mathrm{GenCT}[\mathrm{hk}, h, i_\perp, \mu, k](i \in [N])$

- 用 $\mathrm{PRF}(k, i)$ 产生各种所需的随机数
- 输出 $\mathrm{Garble}\left(C\left[\begin{cases}\perp, & i \le i_\perp;\\ \mu, & i > i_\perp;\end{cases}\right]\right)$ 的 $\hat{C}$
- 输出 $\mathrm{rct}_{i,z} \xleftarrow{\$} \mathrm{Send}(\mathrm{hk}, h, (i-1)\ell_{\mathrm{pk}} + z, L_z^0, L_z^1)$

依 pk_i 的每一位选择 $\hat{C}$ 的标签

电路 $C[\mu'](\mathrm{pk})$

输出 $\mathrm{PKEEnc}(\mathrm{pk}, \mu')$

构造 AH-PLBE：大炮开火！（续）

heavy hammers

$$\mathrm{pk} = \mathrm{PKEpk}, \quad \mathrm{sk} = \mathrm{PKEsk},$$

$$\mathrm{ct}(\{\mathrm{pk}_j\}_{j\in[N]}, i_\perp, \mu) = \mathrm{hk}, h, \widetilde{\mathrm{GenCT}} = \mathrm{Obf}(\mathrm{GenCT}[\mathrm{hk}, h, i_\perp, \mu, k])$$

构造 AH-PLBE：大炮开火！（续）

heavy hammers

$$\mathrm{pk} = \mathrm{PKEpk}, \quad \mathrm{sk} = \mathrm{PKEsk},$$

$$\mathrm{ct}(\{\mathrm{pk}_j\}_{j\in[N]}, i_\perp, \mu) = \mathrm{hk}, h, \widetilde{\mathrm{GenCT}} = \mathrm{Obf}(\mathrm{GenCT}[\mathrm{hk}, h, i_\perp, \mu, k])$$

用 sk_i 解密

1. $\widetilde{\mathrm{GenCT}}(i) \to (\hat{C}, \{\mathrm{rct}_{i,z}\})$ 获得乱码电路

构造 AH-PLBE：大炮开火！（续）

heavy hammers

$$\mathrm{pk} = \mathrm{PKEpk}, \quad \mathrm{sk} = \mathrm{PKEsk},$$

$$\mathrm{ct}(\{\mathrm{pk}_j\}_{j\in[N]}, i_\perp, \mu) = \mathrm{hk}, h, \widetilde{\mathrm{GenCT}} = \mathrm{Obf}(\mathrm{GenCT}[\mathrm{hk}, h, i_\perp, \mu, k])$$

用 sk_i 解密

1. $\widetilde{\mathrm{GenCT}}(i) \to (\hat{C}, \{\mathrm{rct}_{i,z}\})$ 获得乱码电路
2. $\mathrm{Hash}(\mathrm{hk}, D) \to (\cdots, \widetilde{D})$ 重新处理公钥列表
3. $\mathrm{Recv}^{\widetilde{D}}(\cdots, \mathrm{rct}_{i,z}) \to L_z$ 选出标签

构造 AH-PLBE：大炮开火！（续）

heavy hammers

$$\mathrm{pk} = \mathrm{PKEpk}, \quad \mathrm{sk} = \mathrm{PKEsk},$$

$$\mathrm{ct}(\{\mathrm{pk}_j\}_{j\in[N]}, i_\perp, \mu) = \mathrm{hk}, h, \widetilde{\mathrm{GenCT}} = \mathrm{Obf}(\mathrm{GenCT}[\mathrm{hk}, h, i_\perp, \mu, k])$$

用 sk_i 解密

1.	$\widetilde{\mathrm{GenCT}}(i) \to (\hat{C}, \{\mathrm{rct}_{i,z}\})$	获得乱码电路
2.	$\mathrm{Hash}(\mathrm{hk}, D) \to (\cdots, \widetilde{D})$	重新处理公钥列表
3.	$\mathrm{Recv}^{\widetilde{D}}(\cdots, \mathrm{rct}_{i,z}) \to L_z$	选出标签
4.	$\hat{C}(\{L_z\}) \to \mathrm{PKEct}_i$	乱码电路求值
5.	$\mathrm{PKEDec}(\mathrm{sk}_i, \mathrm{PKEct}_i) \to \mu'$	还原消息

构造 AH-PLBE：大炮开火！（续）

heavy hammers

$$\mathrm{pk} = \mathrm{PKEpk}, \quad \mathrm{sk} = \mathrm{PKEsk},$$

$$\mathrm{ct}(\{\mathrm{pk}_j\}_{j\in[N]}, i_\perp, \mu) = \mathrm{hk}, h, \widetilde{\mathrm{GenCT}} = \mathrm{Obf}(\mathrm{GenCT}[\mathrm{hk}, h, i_\perp, \mu, k])$$

定理. 若工具分别有合适的安全性，则该 AH-PLBE 满足消息隐藏、下标隐藏

用 sk_i 解密

1. $\widetilde{\mathrm{GenCT}}(i) \to (\hat{C}, \{\mathrm{rct}_{i,z}\})$ 获得乱码电路
2. $\mathrm{Hash}(\mathrm{hk}, D) \to (\cdots, \widetilde{D})$ 重新处理公钥列表
3. $\mathrm{Recv}^{\widetilde{D}}(\cdots, \mathrm{rct}_{i,z}) \to L_z$ 选出标签
4. $\hat{C}(\{L_z\}) \to \mathrm{PKEct}_i$ 乱码电路求值
5. $\mathrm{PKEDec}(\mathrm{sk}_i, \mathrm{PKEct}_i) \to \mu'$ 还原消息

构造 AH-PLBE：大炮开火！（续）

heavy hammers

$$\mathrm{pk} = \mathrm{PKEpk}, \quad \mathrm{sk} = \mathrm{PKEsk},$$

$$\mathrm{ct}(\{\mathrm{pk}_j\}_{j\in[N]}, i_\perp, \mu) = \mathrm{hk}, h, \widetilde{\mathrm{GenCT}} = \mathrm{Obf}(\mathrm{GenCT}[\mathrm{hk}, h, i_\perp, \mu, k])$$

✅ **密文长度 $O(1)$**

定理. 若工具分别有合适的安全性，则该 AH-PLBE 满足消息隐藏、下标隐藏

用 sk_i 解密

1.	$\widetilde{\mathrm{GenCT}}(i) \to (\hat{C}, \{\mathrm{rct}_{i,z}\})$	获得乱码电路
2.	$\mathrm{Hash}(\mathrm{hk}, D) \to (\cdots, \widetilde{D})$	重新处理公钥列表
3.	$\mathrm{Recv}^{\widetilde{D}}(\cdots, \mathrm{rct}_{i,z}) \to L_z$	选出标签
4.	$\hat{C}(\{L_z\}) \to \mathrm{PKEct}_i$	乱码电路求值
5.	$\mathrm{PKEDec}(\mathrm{sk}_i, \mathrm{PKEct}_i) \to \mu'$	还原消息

构造 AH-PLBE：大炮开火！（续）

heavy hammers

$$\mathrm{pk} = \mathrm{PKEpk}, \quad \mathrm{sk} = \mathrm{PKEsk},$$

$$\mathrm{ct}(\{\mathrm{pk}_j\}_{j\in[N]}, i_\perp, \mu) = \mathrm{hk}, h, \widetilde{\mathrm{GenCT}} = \mathrm{Obf}(\mathrm{GenCT}[\mathrm{hk}, h, i_\perp, \mu, k])$$

✓ **密文长度 $O(1)$**

定理. 若工具分别有合适的安全性，则该 AH-PLBE 满足消息隐藏、下标隐藏

用 sk_i 解密

1.	$\widetilde{\mathrm{GenCT}}(i) \to (\hat{C}, \{\mathrm{rct}_{i,z}\})$	获得乱码电路
2.	$\mathrm{Hash}(\mathrm{hk}, D) \to (\cdots, \widetilde{D})$	重新处理公钥列表
3.	$\mathrm{Recv}^{\widetilde{D}}(\cdots, \mathrm{rct}_{i,z}) \to L_z$	选出标签
4.	$\hat{C}(\{L_z\}) \to \mathrm{PKEct}_i$	乱码电路求值
5.	$\mathrm{PKEDec}(\mathrm{sk}_i, \mathrm{PKEct}_i) \to \mu'$	还原消息

✗ **解密时间 $\Omega(N)$**

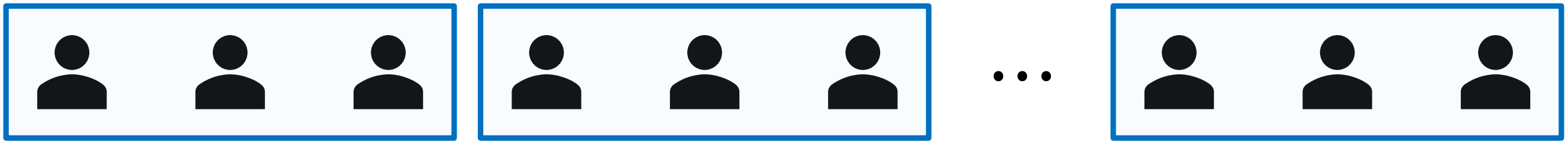
AD HOC BROADCAST TRACE AND REVOKE

EPISODE: 1.5

YOU CAN (NOT) OPTIMIZE

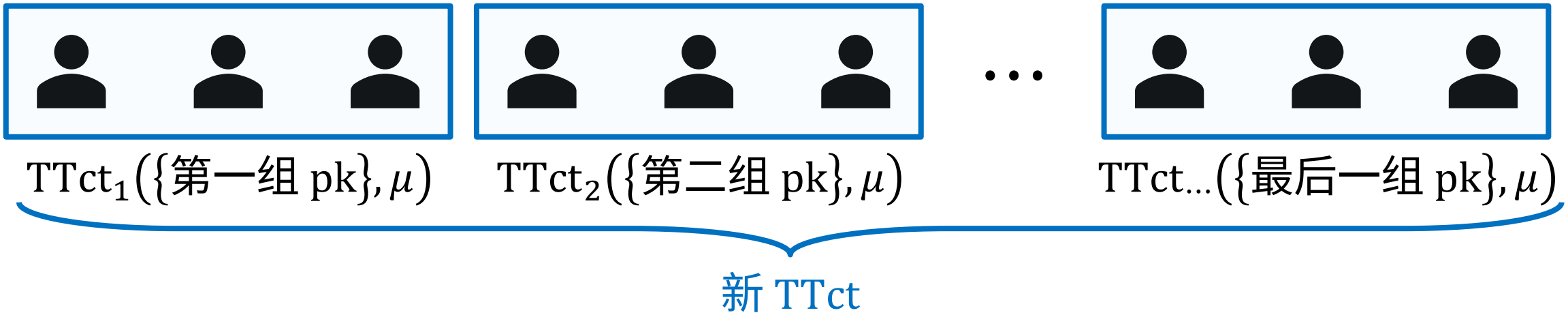
空间换时间：套一层朴素 PLBE [Z]

空间换时间：套一层朴素 PLBE [Z]



$\mathrm{TTct}_1(\{\text{第一组 pk}\},\mu)$ $\mathrm{TTct}_2(\{\text{第二组 pk}\},\mu)$ … $\mathrm{TTct}_{\ldots}(\{\text{最后一组 pk}\},\mu)$

空间换时间：套一层朴素 PLBE [Z]



空间换时间：套一层朴素 PLBE [Z]

新 $\mathbf{Trace}^{D}(\{\mathbf{pk}_j\}_{j\in[N]}, \mathbf{1}^{1/\varepsilon^*})$

考虑 $H_{i_\perp}$: $\{\mathrm{TTct}_j(\perp)\}_{j\le i_\perp}, \{\mathrm{TTct}_j(\mu)\}_{j>i_\perp}$

空间换时间：套一层朴素 PLBE [Z]

新 $\mathbf{Trace}^{D}(\{\mathbf{pk}_j\}_{j\in[N]}, \mathbf{1}^{1/\varepsilon^*})$

考虑 $H_{i_\perp}$: $\{\mathrm{TTct}_j(\perp)\}_{j\le i_\perp}, \{\mathrm{TTct}_j(\mu)\}_{j>i_\perp}$

设 D 在 $H_{i_\perp}$ 上的优势是 $\varepsilon_{i_\perp}$

- $\forall i_\perp$，可从 D 构造 $D_{i_\perp}$，使 $D_{i_\perp}$ 对 $\mathrm{TTct}_{i_\perp}$ 的优势是 $(\varepsilon_{i_\perp-1} - \varepsilon_{i_\perp})$

空间换时间：套一层朴素 PLBE [Z]

新 $\mathbf{Trace}^{D}(\{\mathbf{pk}_j\}_{j\in[N]}, \mathbf{1}^{1/\varepsilon^*})$

考虑 $H_{i_\perp}$: $\{\mathrm{TTct}_j(\perp)\}_{j\le i_\perp}, \{\mathrm{TTct}_j(\mu)\}_{j>i_\perp}$

设 D 在 $H_{i_\perp}$ 上的优势是 $\varepsilon_{i_\perp}$

- $\forall i_\perp$，可从 D 构造 $D_{i_\perp}$，使 $D_{i_\perp}$ 对 $\mathrm{TTct}_{i_\perp}$ 的优势是 $(\varepsilon_{i_\perp-1} - \varepsilon_{i_\perp})$
- $|\varepsilon_0| \ge \varepsilon^*$, $\varepsilon_N = 0$

空间换时间：套一层朴素 PLBE [Z]

新 $\mathbf{Trace}^{D}(\{\mathbf{pk}_j\}_{j\in[N]}, \mathbf{1}^{1/\varepsilon^*})$

考虑 $H_{i_\perp}$: $\{\mathrm{TTct}_j(\perp)\}_{j\le i_\perp}, \{\mathrm{TTct}_j(\mu)\}_{j>i_\perp}$

设 D 在 $H_{i_\perp}$ 上的优势是 $\varepsilon_{i_\perp}$

- $\forall i_\perp$，可从 D 构造 $D_{i_\perp}$，使 $D_{i_\perp}$ 对 $\mathrm{TTct}_{i_\perp}$ 的优势是 $(\varepsilon_{i_\perp-1} - \varepsilon_{i_\perp})$
- $|\varepsilon_0| \ge \varepsilon^*,\ \varepsilon_N = 0 \implies \exists i_\perp^*: |\varepsilon_{i_\perp^*-1} - \varepsilon_{i_\perp^*}| \ge \varepsilon^*/\#[\text{组数}]$

空间换时间：套一层朴素 PLBE [Z]

新 $\mathbf{Trace}^{D}(\{\mathbf{pk}_j\}_{j\in[N]}, \mathbf{1}^{1/\varepsilon^*})$

考虑 $H_{i_\perp}$: $\{\mathrm{TTct}_j(\perp)\}_{j\le i_\perp}, \{\mathrm{TTct}_j(\mu)\}_{j>i_\perp}$

设 D 在 $H_{i_\perp}$ 上的优势是 $\varepsilon_{i_\perp}$

- $\forall i_\perp$，可从 D 构造 $D_{i_\perp}$，使 $D_{i_\perp}$ 对 $\mathrm{TTct}_{i_\perp}$ 的优势是 $(\varepsilon_{i_\perp-1}-\varepsilon_{i_\perp})$
- $|\varepsilon_0|\ge\varepsilon^*,\ \varepsilon_N=0 \implies \exists i_\perp^*: |\varepsilon_{i_\perp^*-1}-\varepsilon_{i_\perp^*}|\ge\varepsilon^*/\#[\text{组数}]$

$\forall i_\perp$，运行**旧** $\mathrm{Trace}^{D_{i_\perp}}\left(\{\text{第 } i_\perp \text{ 组 pk}\}, 1^{\#[\text{组数}]/\varepsilon^*}\right)$，汇总输出

空间换时间：套一层朴素 PLBE [Z]

$$\#[\text{组数}] = N^{\gamma}$$
$$|\mathrm{ct}| = \Theta(N^{\gamma})$$
$$T_{\mathrm{Dec}} = \Theta(N^{1-\gamma})$$

新 $\mathbf{Trace}^{D}(\{\mathbf{pk}_j\}_{j\in[N]}, \mathbf{1}^{1/\varepsilon^*})$

考虑 $H_{i_\perp}$: $\{\mathrm{TTct}_j(\perp)\}_{j\le i_\perp}, \{\mathrm{TTct}_j(\mu)\}_{j>i_\perp}$

设 D 在 $H_{i_\perp}$ 上的优势是 $\varepsilon_{i_\perp}$

- $\forall i_\perp$，可从 D 构造 $D_{i_\perp}$，使 $D_{i_\perp}$ 对 $\mathrm{TTct}_{i_\perp}$ 的优势是 $(\varepsilon_{i_\perp-1} - \varepsilon_{i_\perp})$
- $|\varepsilon_0| \ge \varepsilon^*,\ \varepsilon_N = 0 \implies \exists i_\perp^*: |\varepsilon_{i_\perp^*-1} - \varepsilon_{i_\perp^*}| \ge \varepsilon^*/\#[\text{组数}]$

$\forall i_\perp$，运行**旧** $\mathrm{Trace}^{D_{i_\perp}}\left(\{\text{第 } i_\perp \text{ 组 pk}\}, 1^{\#[\text{组数}]/\varepsilon^*}\right)$，汇总输出

空间换时间：套一层朴素 PLBE [Z]

$$\#[\text{组数}] = N^{\gamma}$$
$$|\mathrm{ct}| = \Theta(N^{\gamma})$$
$$T_{\mathrm{Dec}} = \Theta(N^{1-\gamma})$$

必要之繁？
技巧匮乏？

新 $\mathrm{Trace}^{D}(\{\mathbf{pk}_j\}_{j\in[N]}, 1^{1/\varepsilon^*})$

考虑 $H_{i_\perp}$: $\{\mathrm{TTct}_j(\perp)\}_{j\le i_\perp}, \{\mathrm{TTct}_j(\mu)\}_{j>i_\perp}$

设 D 在 $H_{i_\perp}$ 上的优势是 $\varepsilon_{i_\perp}$

- $\forall i_\perp$，可从 D 构造 $D_{i_\perp}$，使 $D_{i_\perp}$ 对 $\mathrm{TTct}_{i_\perp}$ 的优势是 $(\varepsilon_{i_\perp-1} - \varepsilon_{i_\perp})$
- $|\varepsilon_0| \ge \varepsilon^*,\ \varepsilon_N = 0 \implies \exists i_\perp^*: |\varepsilon_{i_\perp^*-1} - \varepsilon_{i_\perp^*}| \ge \varepsilon^*/\#[\text{组数}]$

$\forall i_\perp$，运行**旧** $\mathrm{Trace}^{D_{i_\perp}}\left(\{\text{第 } i_\perp \text{ 组 pk}\}, 1^{\#[\text{组数}]/\varepsilon^*}\right)$，汇总输出

必要之繁

定理. 任意**可追踪**的 **AH-BTR** 都必须满足 $\max|\mathrm{ct}| \cdot \max T_{\mathrm{Dec}} = \Omega(N)$

必要之繁

传统叛徒追踪可以做到
$|\mathrm{pk}|, |\mathrm{sk}|, |\mathrm{ct}|, T_{\mathrm{Dec}}$ 同时是 $O(1)$

定理. 任意**可追踪**的 **AH-BTR** 都必须满足 $\max|\mathrm{ct}| \cdot \max T_{\mathrm{Dec}} = \Omega(N)$

必要之繁

传统叛徒追踪可以做到
$|\mathrm{pk}|, |\mathrm{sk}|, |\mathrm{ct}|, T_{\mathrm{Dec}}$ 同时是 $O(1)$

定理. 任意**可追踪**的 **AH-BTR** 都必须满足 $\max|\mathrm{ct}| \cdot \max T_{\mathrm{Dec}} = \Omega(N)$

“罪魁祸首”是广播，而不是追踪

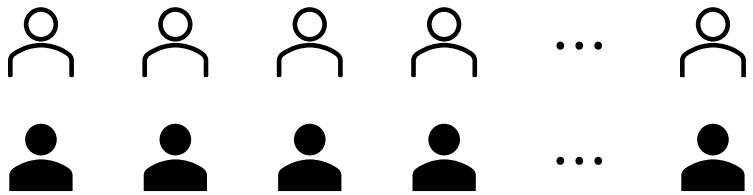
必要之繁

传统叛徒追踪可以做到
$|\mathrm{pk}|, |\mathrm{sk}|, |\mathrm{ct}|, T_{\mathrm{Dec}}$ 同时是 $O(1)$

定理. 任意**可追踪**的 **AH-BTR** 都必须满足 $\max|\mathrm{ct}| \cdot \max T_{\mathrm{Dec}} = \Omega(N)$

“罪魁祸首”是广播，而不是追踪

restricted BE
受限广播加密



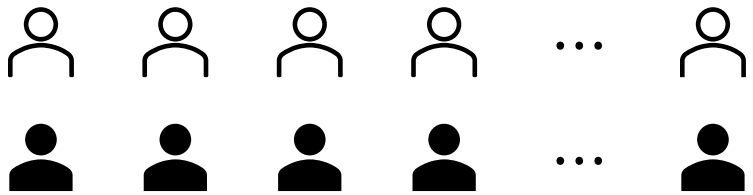
必要之繁

传统叛徒追踪可以做到
$|\mathrm{pk}|, |\mathrm{sk}|, |\mathrm{ct}|, T_{\mathrm{Dec}}$ 同时是 $O(1)$

定理. 任意**可追踪**的 **AH-BTR** 都必须满足 $\max|\mathrm{ct}| \cdot \max T_{\mathrm{Dec}} = \Omega(N)$

“罪魁祸首”是广播，而不是追踪

restricted BE
受限广播加密



$$\mathrm{Gen}(1^N) \to \mathrm{mpk}, \{\mathrm{sk}_{i,r}\}_{i\in[N],r\in\{0,1\}}$$

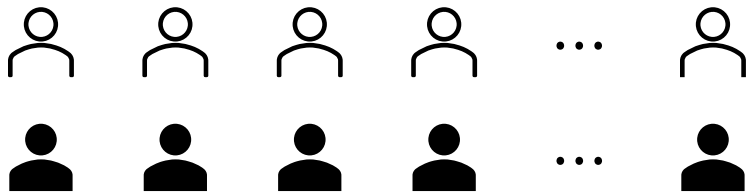
必要之繁

传统叛徒追踪可以做到
$|\mathrm{pk}|, |\mathrm{sk}|, |\mathrm{ct}|, T_{\mathrm{Dec}}$ 同时是 $O(1)$

定理. 任意**可追踪**的 **AH-BTR** 都必须满足 $\max|\mathrm{ct}| \cdot \max T_{\mathrm{Dec}} = \Omega(N)$

“罪魁祸首”是广播，而不是追踪

restricted BE
受限广播加密



$$\mathrm{Gen}(1^N) \to \mathrm{mpk}, \{\mathrm{sk}_{i,r}\}_{i\in[N],r\in\{0,1\}}$$

$$\mathrm{Enc}(\mathrm{mpk}, R, \mu) \to \mathrm{ct}_R$$

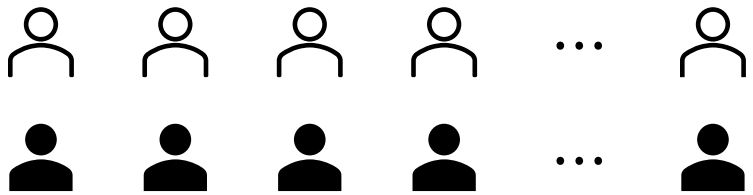
必要之繁

传统叛徒追踪可以做到
$|\mathrm{pk}|, |\mathrm{sk}|, |\mathrm{ct}|, T_{\mathrm{Dec}}$ 同时是 $O(1)$

定理. 任意**可追踪**的 **AH-BTR** 都必须满足 $\max|\mathrm{ct}| \cdot \max T_{\mathrm{Dec}} = \Omega(N)$

“罪魁祸首”是广播，而不是追踪

restricted BE
受限广播加密



$$\mathrm{Gen}(1^N) \to \mathrm{mpk}, \{\mathrm{sk}_{i,r}\}_{i\in[N],r\in\{0,1\}}$$

$$\mathrm{Enc}(\mathrm{mpk}, R, \mu) \to \mathrm{ct}_R$$

$$\mathrm{Dec}^{\mathrm{mpk},i,r,\mathrm{sk}_{i,r},R,\mathrm{ct}_R}() \to \mathrm{ct} \quad (\text{若 } R[i] = r)$$

必要之繁

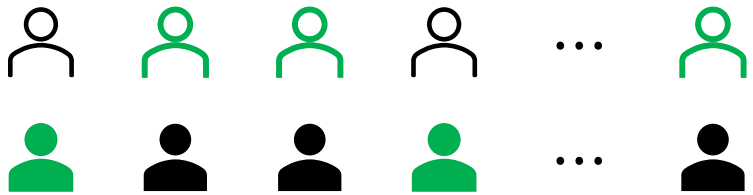
传统叛徒追踪可以做到
$|\mathrm{pk}|, |\mathrm{sk}|, |\mathrm{ct}|, T_{\mathrm{Dec}}$ 同时是 $O(1)$

定理. 任意**可追踪**的 **AH-BTR** 都必须满足 $\max|\mathrm{ct}| \cdot \max T_{\mathrm{Dec}} = \Omega(N)$

“罪魁祸首”是广播，而不是追踪

restricted BE
受限广播加密

例. $R = 1001 \cdots 0$



$$\mathrm{Gen}(1^N) \to \mathrm{mpk}, \{\mathrm{sk}_{i,r}\}_{i\in[N],r\in\{0,1\}}$$

$$\mathrm{Enc}(\mathrm{mpk}, R, \mu) \to \mathrm{ct}_R$$

$$\mathrm{Dec}^{\mathrm{mpk},i,r,\mathrm{sk}_{i,r},R,\mathrm{ct}_R}() \to \mathrm{ct} \quad (\text{若 } R[i] = r)$$

必要之繁

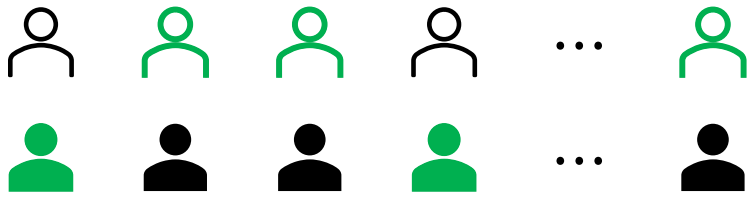
传统叛徒追踪可以做到
$|\mathrm{pk}|, |\mathrm{sk}|, |\mathrm{ct}|, T_{\mathrm{Dec}}$ 同时是 $O(1)$

定理．任意**可追踪**的 **AH-BTR** 都必须满足 $\max|\mathrm{ct}| \cdot \max T_{\mathrm{Dec}} = \Omega(N)$

“罪魁祸首”是广播，而不是追踪

restricted BE
受限广播加密

例． $R = 1001\cdots0$



$$\mathrm{Gen}(1^N) \to \mathrm{mpk}, \{\mathrm{sk}_{i,r}\}_{i\in[N],r\in\{0,1\}}$$

$$\mathrm{Enc}(\mathrm{mpk}, R, \mu) \to \mathrm{ct}_R$$

$$\mathrm{Dec}^{\mathrm{mpk},i,r,\mathrm{sk}_{i,r},R,\mathrm{ct}_R}() \to \mathrm{ct}\ （若\ R[i] = r）$$

（弱）安全性． $\{R, i, \mu_0, \mathrm{mpk}, \mathrm{sk}_{i,\neg R[i]}, \mathrm{ct}_R(\mu_0)\} \approx \{\cdots, \mathrm{ct}_R(\mu_1)\}$ 对所有 $N \le \mathrm{poly}(\lambda)$，其中

$$R \xleftarrow{\$} \{0,1\}^N,\ i \xleftarrow{\$} [N],\ \mu_0 \xleftarrow{\$} \{0,1\}^\lambda, \mu_1 \xleftarrow{\$} \{0,1\}^\lambda.$$

必要之繁：受限广播加密版

定理. 任意**弱安全**的**受限 BE** 都必须满足 $\max|\mathrm{ct}| \cdot \max T_{\mathrm{Dec}} = \Omega(N)$，
其中 T_{Dec} 只计读取 R 的位数

必要之繁：受限广播加密版

ABE

首个属性加密时空下界

定理. 任意**弱安全**的**受限 BE** 都必须满足 $\max|\mathrm{ct}| \cdot \max T_{\mathrm{Dec}} = \Omega(N)$，
其中 T_{Dec} 只计读取 R 的位数

必要之繁：受限广播加密版

ABE

首个属性加密时空下界

定理. 任意**弱安全**的**受限 BE** 都必须满足 $\max|\mathrm{ct}| \cdot \max T_{\mathrm{Dec}} = \Omega(N)$，
其中 T_{Dec} 只计读取 R 的位数

归约. AH-BTR $\Longrightarrow$ 受限 BE：

必要之繁：受限广播加密版

ABE
首个属性加密时空下界

定理. 任意**弱安全**的**受限 BE** 都必须满足 $\max|\mathrm{ct}| \cdot \max T_{\mathrm{Dec}} = \Omega(N)$，
其中 T_{Dec} 只计读取 R 的位数

归约. AH-BTR $\Longrightarrow$ 受限 BE：

$$\mathrm{RBEmpk} = \{\mathrm{AHBTRpk}_{j,s}\}_{j\in[N],s\in\{0,1\}}$$
$$\mathrm{RBEsk}_{j,s} = \mathrm{AHBTRsk}_{j,s}$$
$$\mathrm{RBEct}_{R}(\mu) = \mathrm{AHBTRct}\left(\{\mathrm{AHBTRpk}_{j,R[j]}\}_{j\in[N]}, \mu\right)$$

必要之繁：受限广播加密版

ABE
首个属性加密时空下界

定理. 任意**弱安全**的**受限 BE** 都必须满足 $\max|\mathrm{ct}| \cdot \max T_{\mathrm{Dec}} = \Omega(N)$，
其中 T_{Dec} 只计读取 R 的位数

归约. AH-BTR $\Longrightarrow$ 受限 BE：

$$\mathrm{RBEmpk} = \{\mathrm{AHBTRpk}_{j,s}\}_{j\in[N],s\in\{0,1\}}$$

$$\mathrm{RBEsk}_{j,s} = \mathrm{AHBTRsk}_{j,s}$$

$$\mathrm{RBEct}_{R}(\mu) = \mathrm{AHBTRct}\left(\{\mathrm{AHBTRpk}_{j,R[j]}\}_{j\in[N]}, \mu\right)$$

解密用 AH-BTR 的算法，每次要读取 pk_j 时，
先读取 $r \leftarrow R[j]$ 再读取 $\mathrm{AHBTRpk}_{j,r}$

必要之繁：受限广播加密版

ABE
首个属性加密时空下界

定理. 任意**弱安全**的**受限 BE** 都必须满足 $\max|\mathrm{ct}| \cdot \max T_{\mathrm{Dec}} = \Omega(N)$，
其中 T_{Dec} 只计读取 R 的位数

归约. AH-BTR $\Longrightarrow$ 受限 BE：

$$\mathrm{RBEmpk} = \{\mathrm{AHBTRpk}_{j,s}\}_{j\in[N],s\in\{0,1\}}$$

$$\mathrm{RBEsk}_{j,s} = \mathrm{AHBTRsk}_{j,s} \qquad |\mathrm{RBEct}| = |\mathrm{AHBTRct}|$$

$$\mathrm{RBEct}_{R}(\mu) = \mathrm{AHBTRct}\left(\{\mathrm{AHBTRpk}_{j,R[j]}\}_{j\in[N]}, \mu\right)$$

解密用 AH-BTR 的算法，每次要读取 pk_j 时，
先读取 $r \leftarrow R[j]$ 再读取 $\mathrm{AHBTRpk}_{j,r}$

必要之繁：受限广播加密版

ABE
首个属性加密时空下界

定理. 任意**弱安全**的**受限 BE** 都必须满足 $\max|\mathrm{ct}| \cdot \max T_{\mathrm{Dec}} = \Omega(N)$，
其中 T_{Dec} 只计读取 R 的位数

归约. AH-BTR $\Longrightarrow$ 受限 BE：

$$\mathrm{RBEmpk} = \{\mathrm{AHBTRpk}_{j,s}\}_{j\in[N],s\in\{0,1\}}$$

$$\mathrm{RBEsk}_{j,s} = \mathrm{AHBTRsk}_{j,s} \qquad |\mathrm{RBEct}| = |\mathrm{AHBTRct}|$$

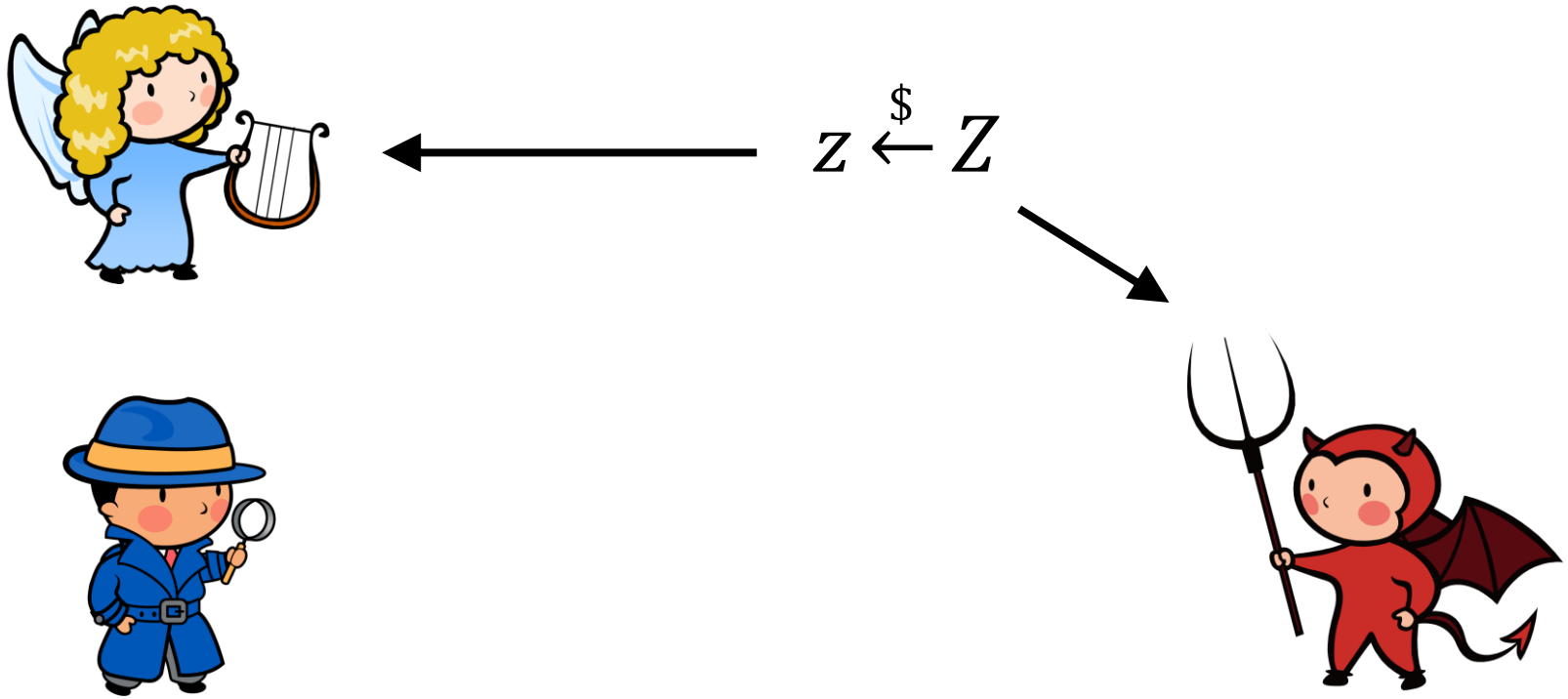
$$\mathrm{RBEct}_{R}(\mu) = \mathrm{AHBTRct}\left(\{\mathrm{AHBTRpk}_{j,R[j]}\}_{j\in[N]}, \mu\right)$$

解密用 AH-BTR 的算法，每次要读取 pk_j 时，
先读取 $r \leftarrow R[j]$ 再读取 $\mathrm{AHBTRpk}_{j,r}$

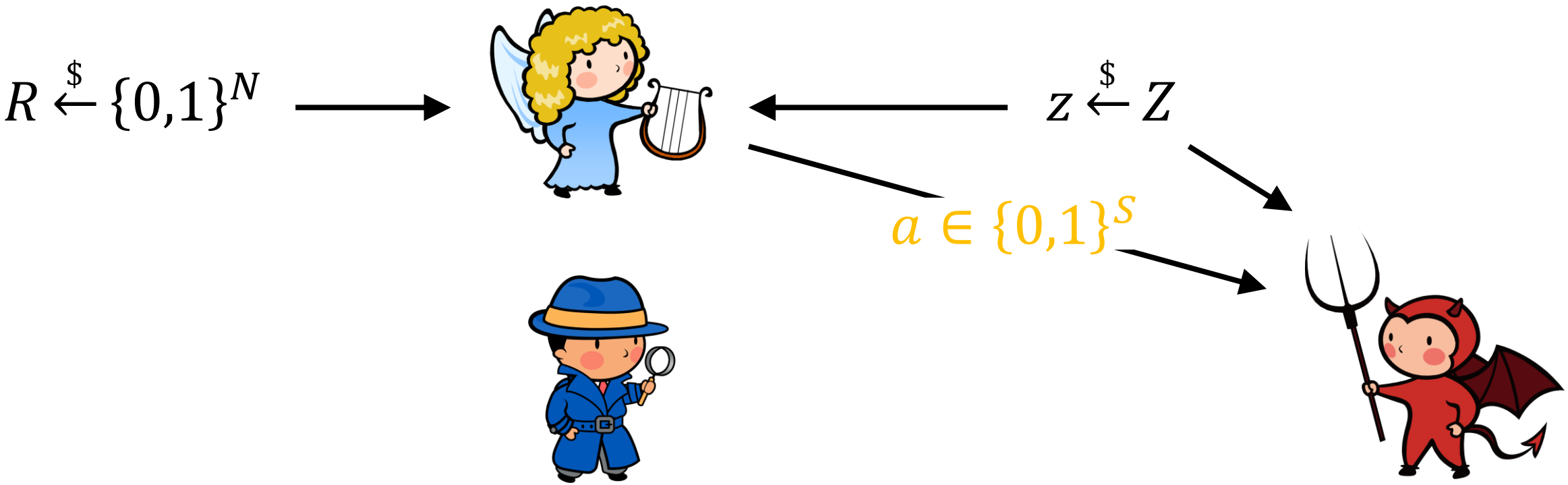
受限 BE 解密读取 R 的位数 = AH-BTR 解密读取诸 pk 的总位数 $\leq$ AH-BTR 解密时间

时空下界证明：来自 AI-ROM 的工具

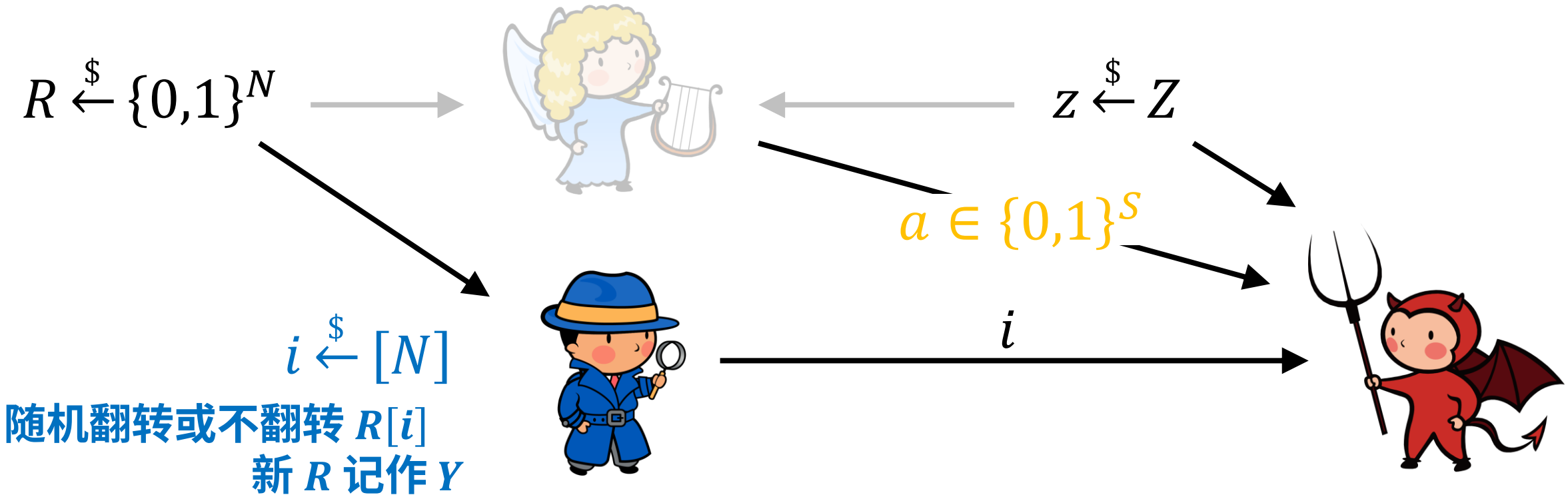
时空下界证明：来自 AI-ROM 的工具



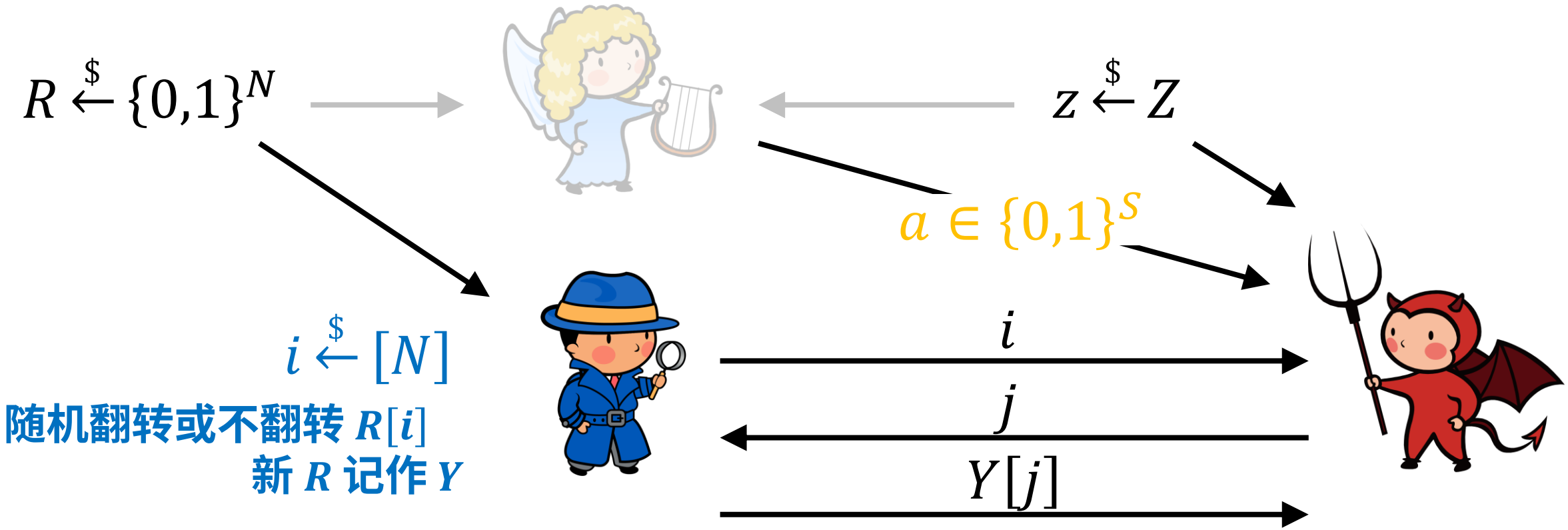
时空下界证明：来自 AI-ROM 的工具



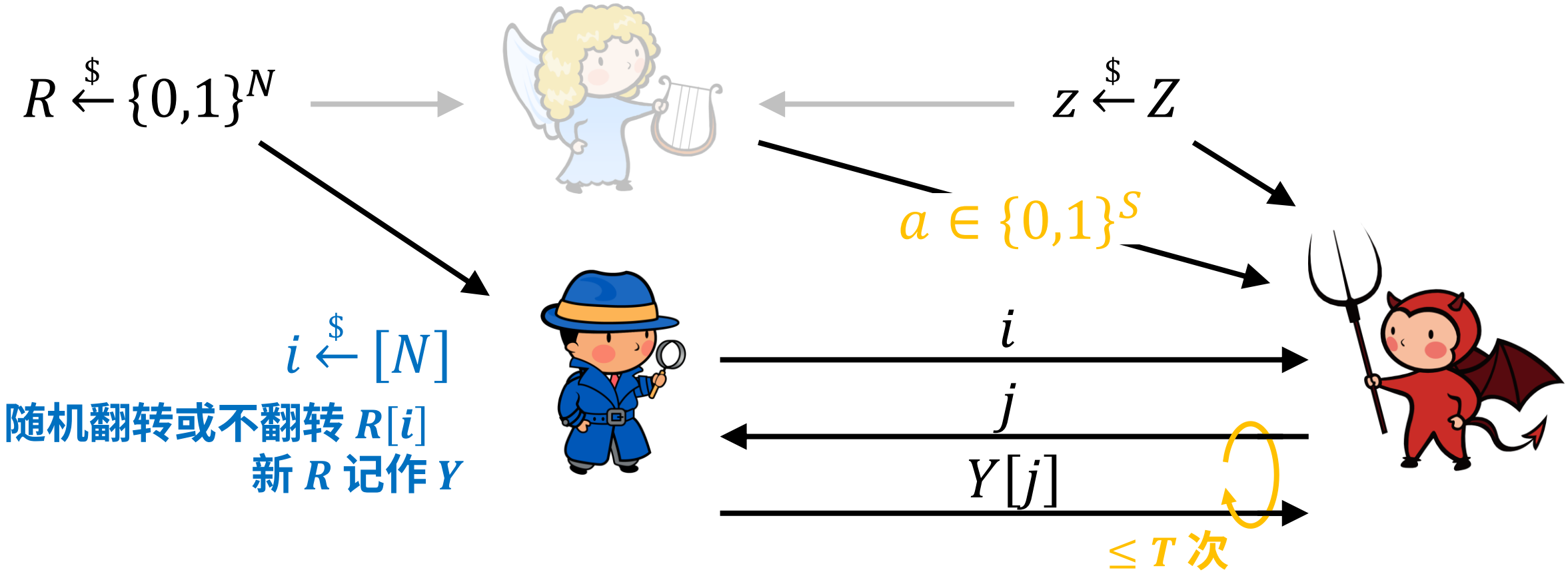
时空下界证明：来自 AI-ROM 的工具



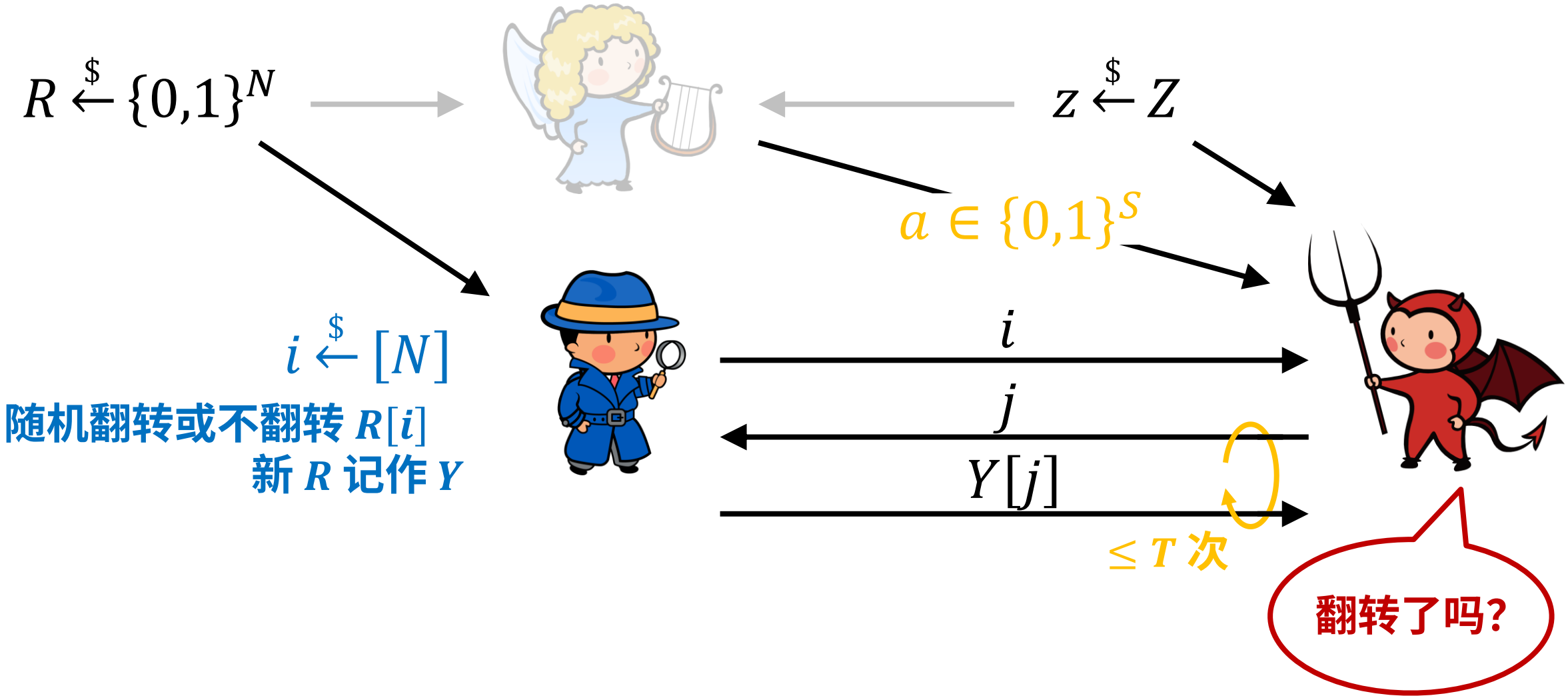
时空下界证明：来自 AI-ROM 的工具



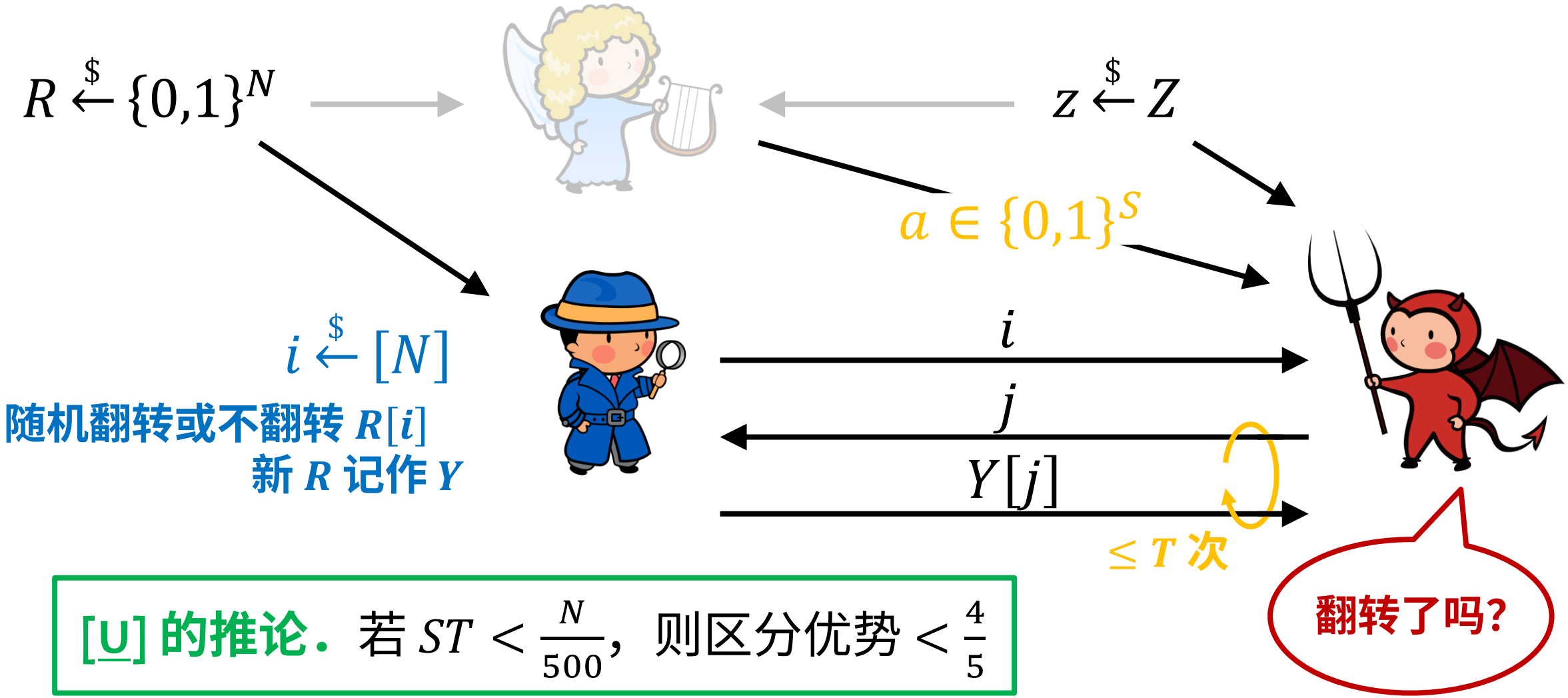
时空下界证明：来自 AI-ROM 的工具



时空下界证明：来自 AI-ROM 的工具



时空下界证明：来自 AI-ROM 的工具



[U] 的推论. 若 $ST < \frac{N}{500}$，则区分优势 $< \frac{4}{5}$

时空下界证明

若 $|\mathrm{ct}| \cdot (T_{\mathrm{Dec}} + 1) < N/500$（暂设 $|\mathrm{ct}|, T_{\mathrm{Dec}}$ 不受随机数影响），**欲证不安全**

时空下界证明

若 $|\mathrm{ct}| \cdot (T_{\mathrm{Dec}} + 1) < N/500$（暂设 $|\mathrm{ct}|, T_{\mathrm{Dec}}$ 不受随机数影响），**欲证不安全**

adversarial strategy

使坏策略. 收到 $\{R, i, \mu_0, \mathrm{mpk}, \mathrm{sk}_{i,\neg R[i]}, \mathrm{ct}_R\}$ 后，
需要判断 ct_R 加密的是 μ_0 还是 μ_1.

时空下界证明

若 $|\mathrm{ct}| \cdot (T_{\mathrm{Dec}} + 1) < N/500$（暂设 $|\mathrm{ct}|, T_{\mathrm{Dec}}$ 不受随机数影响），**欲证不安全**

adversarial strategy

使坏策略. 收到 $\{R, i, \mu_0, \mathrm{mpk}, \mathrm{sk}_{i,\neg R[i]}, \mathrm{ct}_R\}$ 后，

需要判断 ct_R 加密的是 μ_0 还是 μ_1.

做法：翻转 $R[i]$（新 R 记作 R'）后 **“强行解密”**

$$\mu' \leftarrow \mathrm{Dec}^{\mathrm{mpk},i,r=R'[i]=\neg R[i],\mathrm{sk}_{i,r},R',\mathrm{ct}_R}()$$

判定 ct_R 加密了 μ_0 当且仅当 $\mu' = \mu_0$.

时空下界证明

若 $|\mathrm{ct}| \cdot (T_{\mathrm{Dec}} + 1) < N/500$（暂设 $|\mathrm{ct}|, T_{\mathrm{Dec}}$ 不受随机数影响），**欲证不安全**

adversarial strategy

使坏策略. 收到 $\{R, i, \mu_0, \mathrm{mpk}, \mathrm{sk}_{i,\neg R[i]}, \mathrm{ct}_R\}$ 后，
需要判断 ct_R 加密的是 μ_0 还是 μ_1.

做法：翻转 $R[i]$（新 R 记作 R'）后“**强行解密**”

$$\mu' \leftarrow \mathrm{Dec}^{\mathrm{mpk},i,r=R'[i]=\neg R[i],\mathrm{sk}_{i,r},R',\mathrm{ct}_R}()$$

判定 ct_R 加密了 μ_0 当且仅当 $\mu' = \mu_0$.

若 ct_R 加密了 μ_1，则 μ' 和 μ_0 **独立**，故 $\Pr[\mu' = \mu_0] \leq 2^{-\lambda}$

时空下界证明

若 $|\mathrm{ct}| \cdot (T_{\mathrm{Dec}} + 1) < N/500$（暂设 $|\mathrm{ct}|, T_{\mathrm{Dec}}$ 不受随机数影响），**欲证不安全**

adversarial strategy

使坏策略. 收到 $\{R, i, \mu_0, \mathrm{mpk}, \mathrm{sk}_{i,\neg R[i]}, \mathrm{ct}_R\}$ 后，

需要判断 ct_R 加密的是 μ_0 还是 μ_1.

做法：翻转 $R[i]$（新 R 记作 R'）后 **“强行解密”**

$$\mu' \leftarrow \mathrm{Dec}^{\mathrm{mpk},i,r=R'[i]=\neg R[i],\mathrm{sk}_{i,r},R',\mathrm{ct}_R}()$$

判定 ct_R 加密了 μ_0 当且仅当 $\mu' = \mu_0$.

若 ct_R 加密了 μ_1，则 μ' 和 μ_0 **独立**，故 $\Pr[\mu' = \mu_0] \leq 2^{-\lambda}$

若 ct_R 加密了 μ_0，**欲证** $\Pr[\mu' = \mu_0] \geq \frac{1}{5}$

时空下界证明

若 $|\mathrm{ct}| \cdot (T_{\mathrm{Dec}} + 1) < N/500$（暂设 $|\mathrm{ct}|, T_{\mathrm{Dec}}$ 不受随机数影响），**欲证不安全**

adversarial strategy

使坏策略. 收到 $\{R, i, \mu_0, \mathrm{mpk}, \mathrm{sk}_{i,\neg R[i]}, \mathrm{ct}_R\}$ 后，
需要判断 ct_R 加密的是 μ_0 还是 μ_1.

做法：翻转 $R[i]$（新 R 记作 R'）后 **“强行解密”**

$$\mu' \leftarrow \mathrm{Dec}^{\mathrm{mpk},i,r=R'[i]=\neg R[i],\mathrm{sk}_{i,r},R',\mathrm{ct}_R}()$$

判定 ct_R 加密了 μ_0 当且仅当 $\mu' = \mu_0$.

若 ct_R 加密了 μ_1，则 μ' 和 μ_0 **独立**，故 $\Pr[\mu' = \mu_0] \le 2^{-\lambda}$

若 ct_R 加密了 μ_0，**欲证** $\Pr[\mu' = \mu_0] \ge \frac{1}{5}$

$\Rightarrow$ **不安全**

时空下界证明（续）

若 ct_R 加密了 μ_0，**欲证** $\Pr[\mu' = \mu_0] \geq \frac{1}{5}$

时空下界证明（续）

思路. 利用 AI-ROM 推论，从 $\mathrm{sk}_{i,R[i]}$ 能解密（**正确性**）推出 $\mathrm{sk}_{i,\neg R[i]}$ 能解密

若 ct_R 加密了 μ_0，**欲证** $\Pr[\mu' = \mu_0] \geq \frac{1}{5}$

时空下界证明（续）

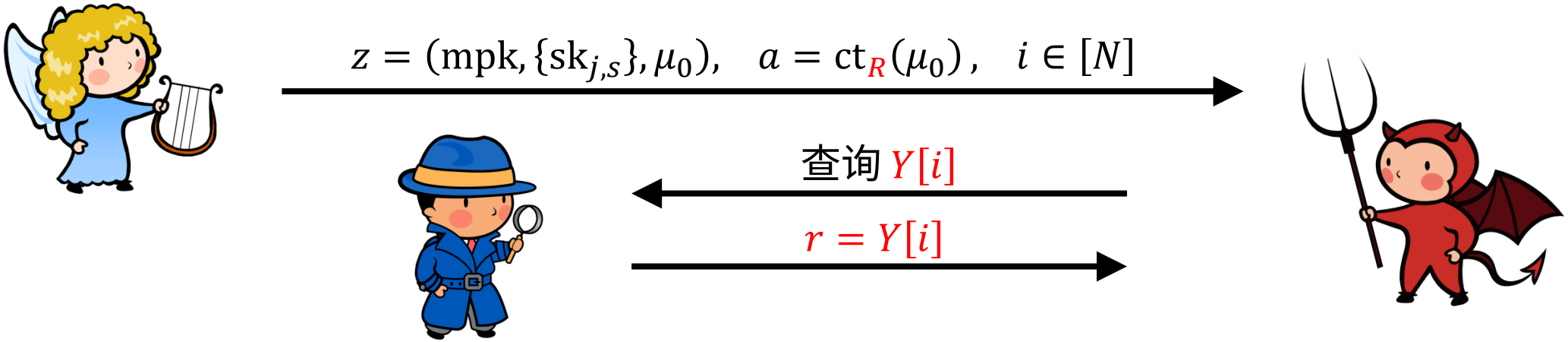
思路. 利用 AI-ROM 推论，从 $\mathrm{sk}_{i,R[i]}$ 能解密（**正确性**）推出 $\mathrm{sk}_{i,\neg R[i]}$ 能解密

$$z = (\mathrm{mpk}, \{\mathrm{sk}_{j,s}\}, \mu_0), \quad a = \mathrm{ct}_R(\mu_0), \quad i \in [N]$$

若 ct_R 加密了 μ_0，**欲证** $\Pr[\mu' = \mu_0] \geq \frac{1}{5}$

时空下界证明（续）

思路. 利用 AI-ROM 推论，从 $\mathrm{sk}_{i,R[i]}$ 能解密（**正确性**）推出 $\mathrm{sk}_{i,\neg R[i]}$ 能解密



若 ct_R 加密了 μ_0，**欲证** $\Pr[\mu' = \mu_0] \geq \frac{1}{5}$

时空下界证明（续）

思路. 利用 AI-ROM 推论，从 $\mathrm{sk}_{i,R[i]}$ 能解密（**正确性**）推出 $\mathrm{sk}_{i,\neg R[i]}$ 能解密

$z = (\mathrm{mpk}, \{\mathrm{sk}_{j,s}\}, \mu_0), \quad a = \mathrm{ct}_R(\mu_0), \quad i \in [N]$

查询 $Y[i]$

$r = Y[i]$

Dec 可以查询 Y

$\mu_0 \overset{?}{=} \mu' \leftarrow \mathrm{Dec}^{\mathrm{mpk},i,r,\mathrm{sk}_{i,r},Y,\mathrm{ct}_R}()$

若 ct_R 加密了 μ_0，**欲证** $\Pr[\mu' = \mu_0] \geq \frac{1}{5}$

时空下界证明（续）

思路. 利用 AI-ROM 推论，从 $\mathrm{sk}_{i,R[i]}$ 能解密（**正确性**）推出 $\mathrm{sk}_{i,\neg R[i]}$ 能解密

$z = (\mathrm{mpk}, \{\mathrm{sk}_{j,s}\}, \mu_0)$，　$a = \mathrm{ct}_R(\mu_0)$，　$i \in [N]$

查询 $Y[i]$

$r = Y[i]$

Dec 可以查询 Y

$\mu_0 \overset{?}{=} \mu' \leftarrow \mathrm{Dec}^{\mathrm{mpk},i,r,\mathrm{sk}_{i,r},Y,\mathrm{ct}_R}()$

总查询位数 $\leq T_{\mathbf{Dec}} + 1$

若 ct_R 加密了 μ_0，**欲证** $\Pr[\mu' = \mu_0] \geq \frac{1}{5}$

时空下界证明（续）

思路. 利用 AI-ROM 推论，从 $\mathrm{sk}_{i,R[i]}$ 能解密（**正确性**）推出 $\mathrm{sk}_{i,\neg R[i]}$ 能解密

$z = (\mathrm{mpk}, \{\mathrm{sk}_{j,s}\}, \mu_0),\quad a = \mathrm{ct}_R(\mu_0),\quad i \in [N]$

查询 $Y[i]$

$r = Y[i]$

Dec 可以查询 Y

总查询位数 $\leq T_{\mathbf{Dec}} + 1$

$\mu_0 \overset{?}{=} \mu' \leftarrow \mathrm{Dec}^{\mathrm{mpk},i,r,\mathrm{sk}_{i,r},Y,\mathrm{ct}_R}()$

当 Y 为 R **本身**时，由**正确性** $\Pr[\mu' = \mu_0] = 1$

若 ct_R 加密了 μ_0，**欲证** $\Pr[\mu' = \mu_0] \geq \frac{1}{5}$

时空下界证明（续）

思路. 利用 AI-ROM 推论，从 $\mathrm{sk}_{i,R[i]}$ 能解密（**正确性**）推出 $\mathrm{sk}_{i,\neg R[i]}$ 能解密

$z = (\mathrm{mpk}, \{\mathrm{sk}_{j,s}\}, \mu_0), \quad a = \mathrm{ct}_R(\mu_0), \quad i \in [N]$

查询 $Y[i]$

$r = Y[i]$

Dec 可以查询 Y

$\mu_0 \overset{?}{=} \mu' \leftarrow \mathrm{Dec}^{\mathrm{mpk},i,r,\mathrm{sk}_{i,r},Y,\mathrm{ct}_R}()$

总查询位数 $\leq T_{\mathbf{Dec}} + 1$

当 Y 为 R **本身**时，由**正确性** $\Pr[\mu' = \mu_0] = 1$

当 Y 为 R **翻转**时，由**推论**知 $\Pr[\mu' = \mu_0] \geq 1 - \frac{4}{5}$

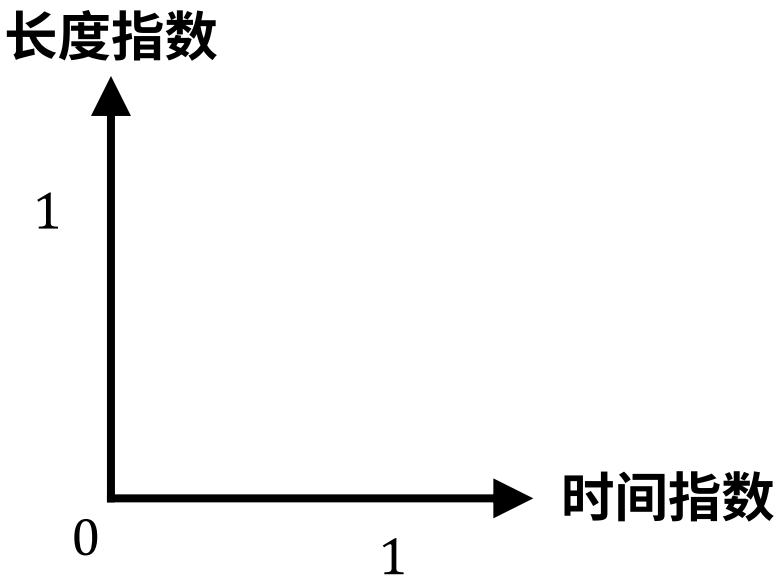
若 ct_R 加密了 μ_0，**欲证** $\Pr[\mu' = \mu_0] \geq \frac{1}{5}$

总结

成果. 定义、构造 AH-BTR，证明了效率下界，完全刻画 Pareto 最优效率前沿

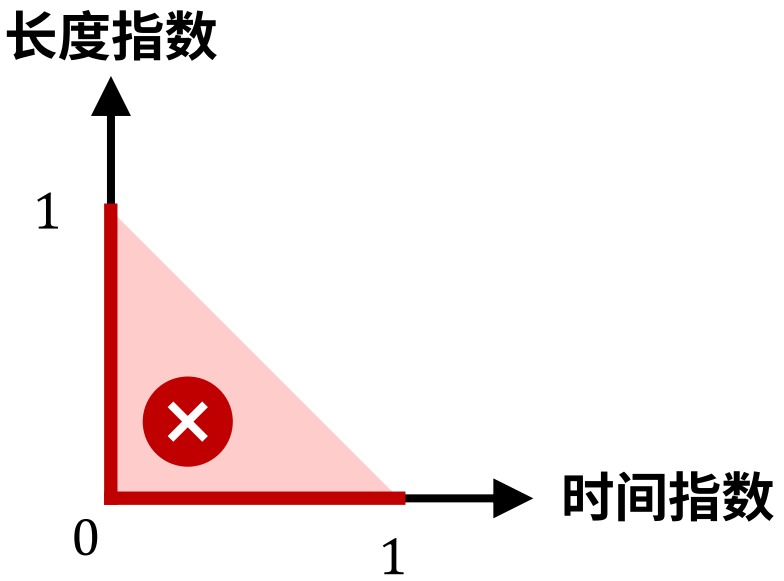
总结

成果. 定义、构造 AH-BTR，证明了效率下界，完全刻画 Pareto 最优效率前沿



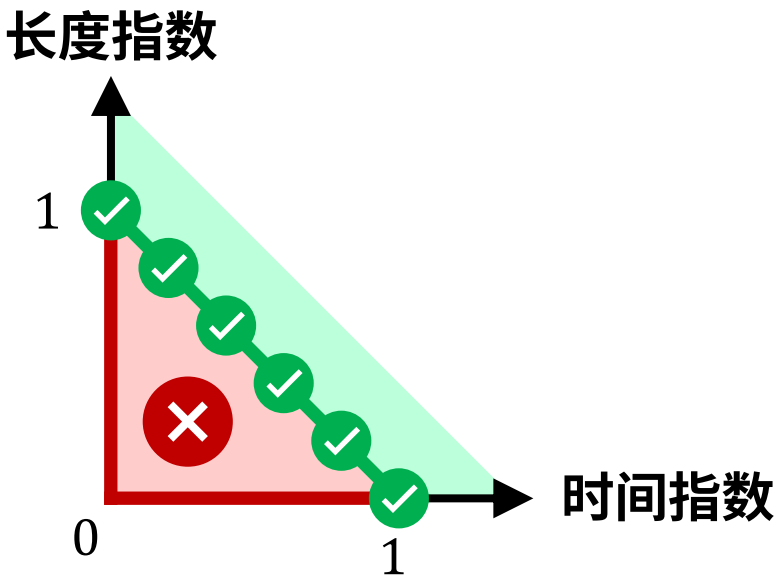
总结

成果. 定义、构造 AH-BTR，证明了效率下界，完全刻画 Pareto 最优效率前沿



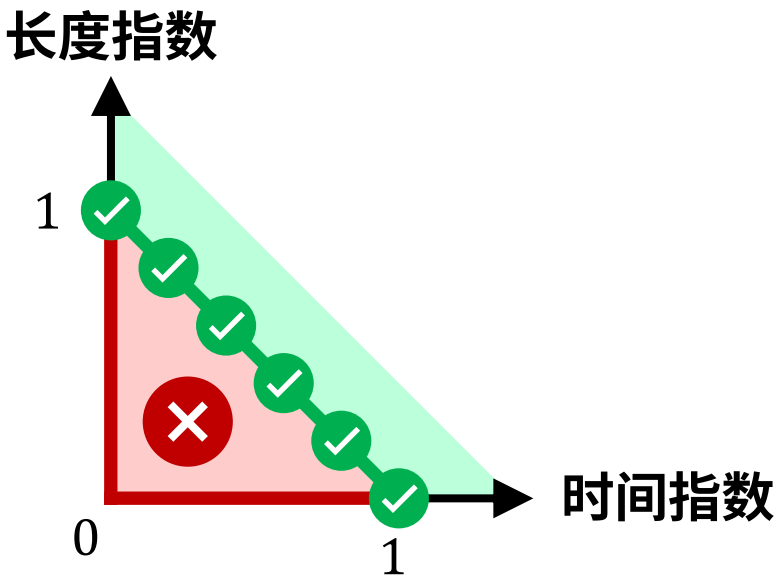
总结

成果. 定义、构造 AH-BTR，证明了效率下界，完全刻画 Pareto 最优效率前沿



总结

成果. 定义、构造 AH-BTR，证明了效率下界，完全刻画 Pareto 最优效率前沿

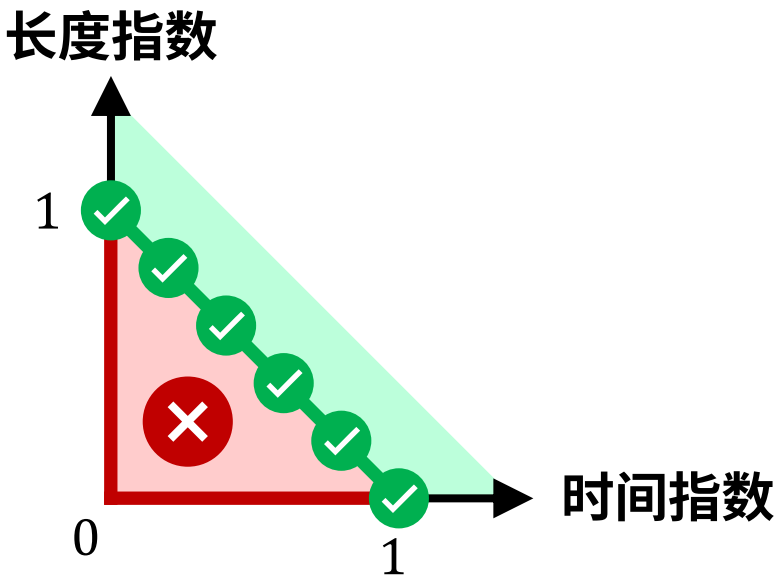


未解问题.

1. 本作要用程序混淆的“大炮”，如何基于更弱的假设构造 AH-BTR?

总结

成果. 定义、构造 AH-BTR，证明了效率下界，完全刻画 Pareto 最优效率前沿

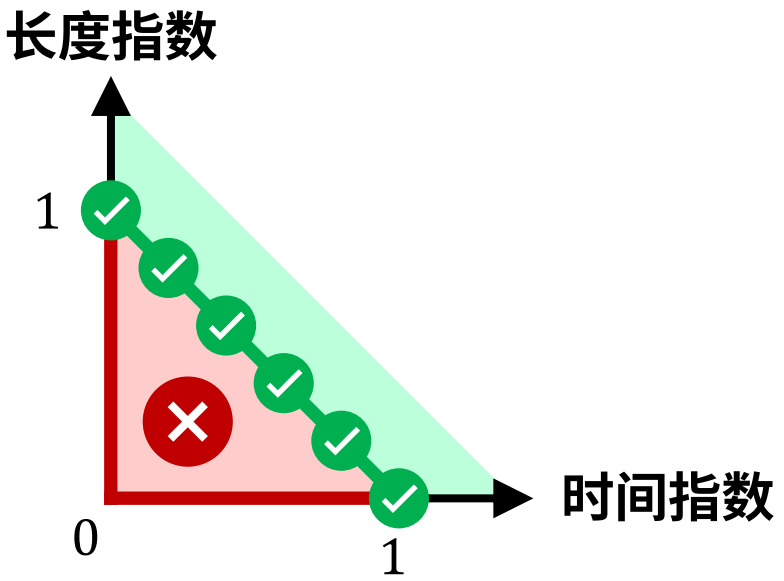


未解问题.

1. 本作要用程序混淆的“大炮”，如何基于更弱的假设构造 AH-BTR?
2. 其他叛徒追踪（白盒、量子等）的自组型方案的研究?

总结

成果. 定义、构造 AH-BTR，证明了效率下界，完全刻画 Pareto 最优效率前沿



未解问题.

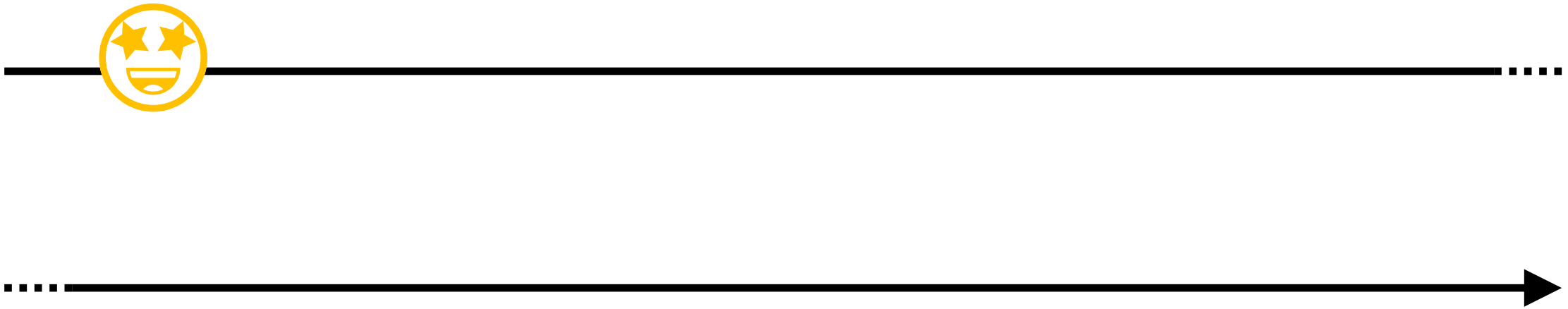
1. 本作要用程序混淆的“大炮”，如何基于更弱的假设构造 AH-BTR?
2. 其他叛徒追踪（白盒、量子等）的自组型方案的研究?
3. 已经刻画了 BE 的 Pareto 最优效率前沿，一般的 ABE 和 FE 呢? [JLL]

课题的时间线

课题的时间线

（2021-01 前）

想要**单作者论文**



课题的时间线

（**2021**-01 前）

想要**单作者论文**

（2021-06）

NTT Research 实习

做**叛徒追踪**的工作

课题的时间线

（**2021**-01 前）

想要**单作者论文**

（2021-06）

NTT Research 实习

做**叛徒追踪**的工作

（**2022**-02）

摸鱼得到**课题灵感**

并给出**构造**

课题的时间线

（**2021**-01 前）

想要**单作者论文**

（2021-06）

NTT Research 实习

做**叛徒追踪**的工作

（**2022**-02）

摸鱼得到**课题灵感**

并给出**构造**

（2022-03）

在 UW 密码学**讨论班**讲了进展

并**抛出**了**下界的问题**

课题的时间线

（**2021**-01 前）
想要**单作者论文**

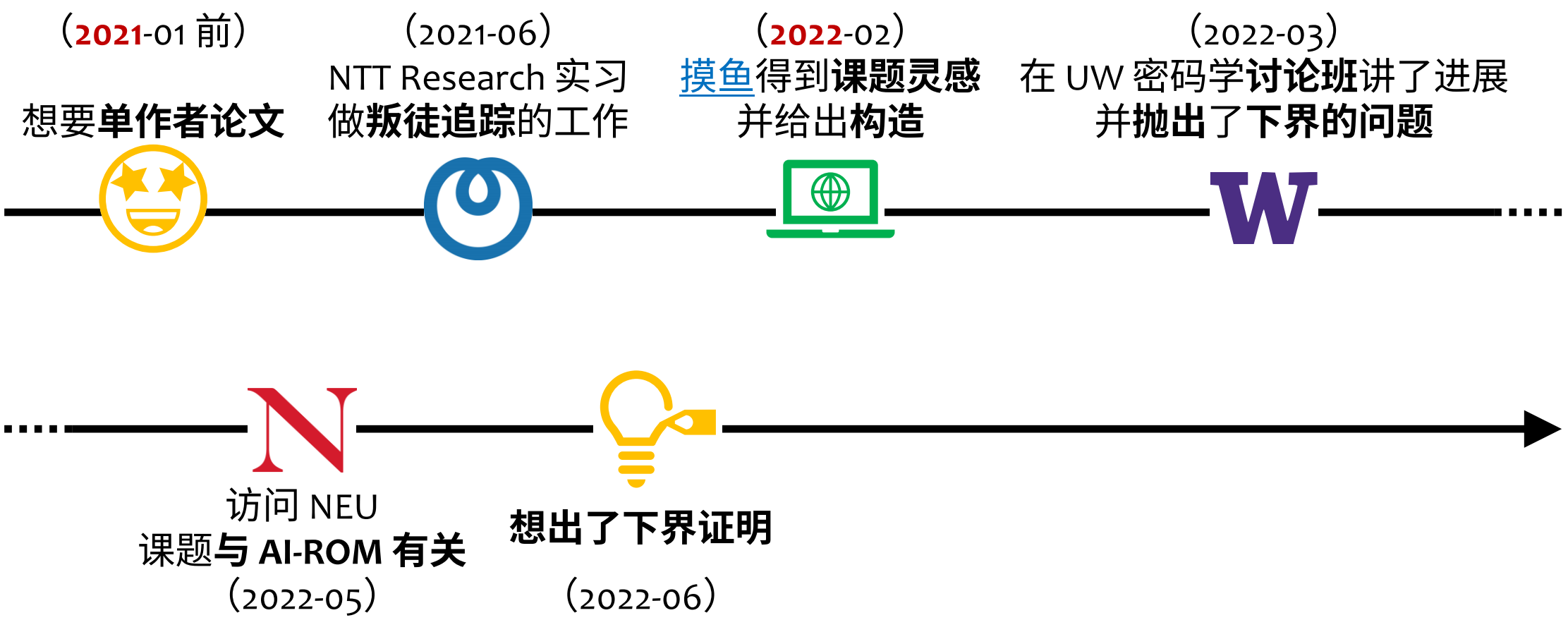
（2021-06）
NTT Research 实习
做**叛徒追踪**的工作

（**2022**-02）
摸鱼得到**课题灵感**
并给出**构造**

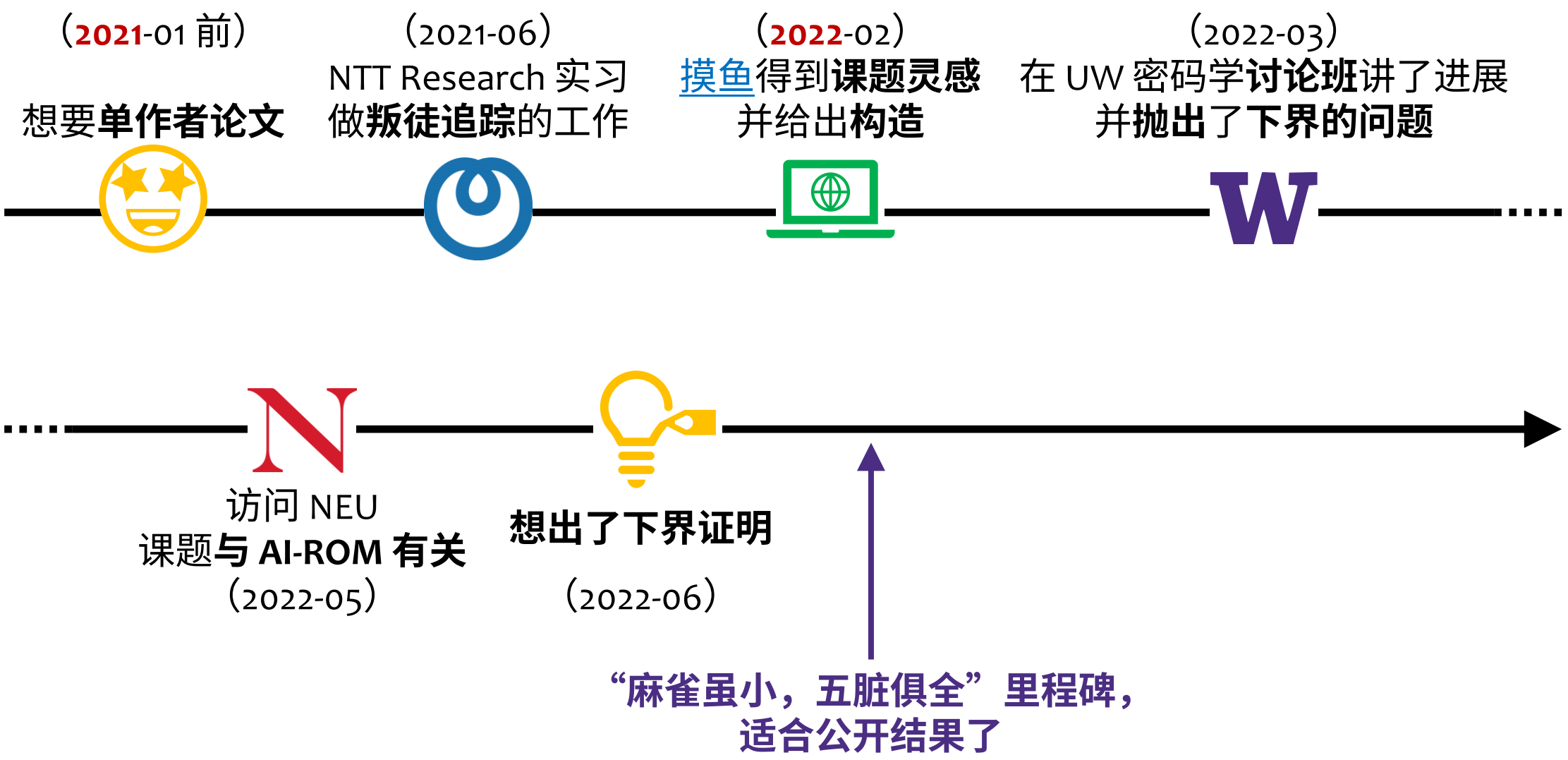
（2022-03）
在 UW 密码学**讨论班**讲了进展
并**抛出**了**下界的问题**

访问 NEU
课题**与 AI-ROM 有关**
（2022-05）

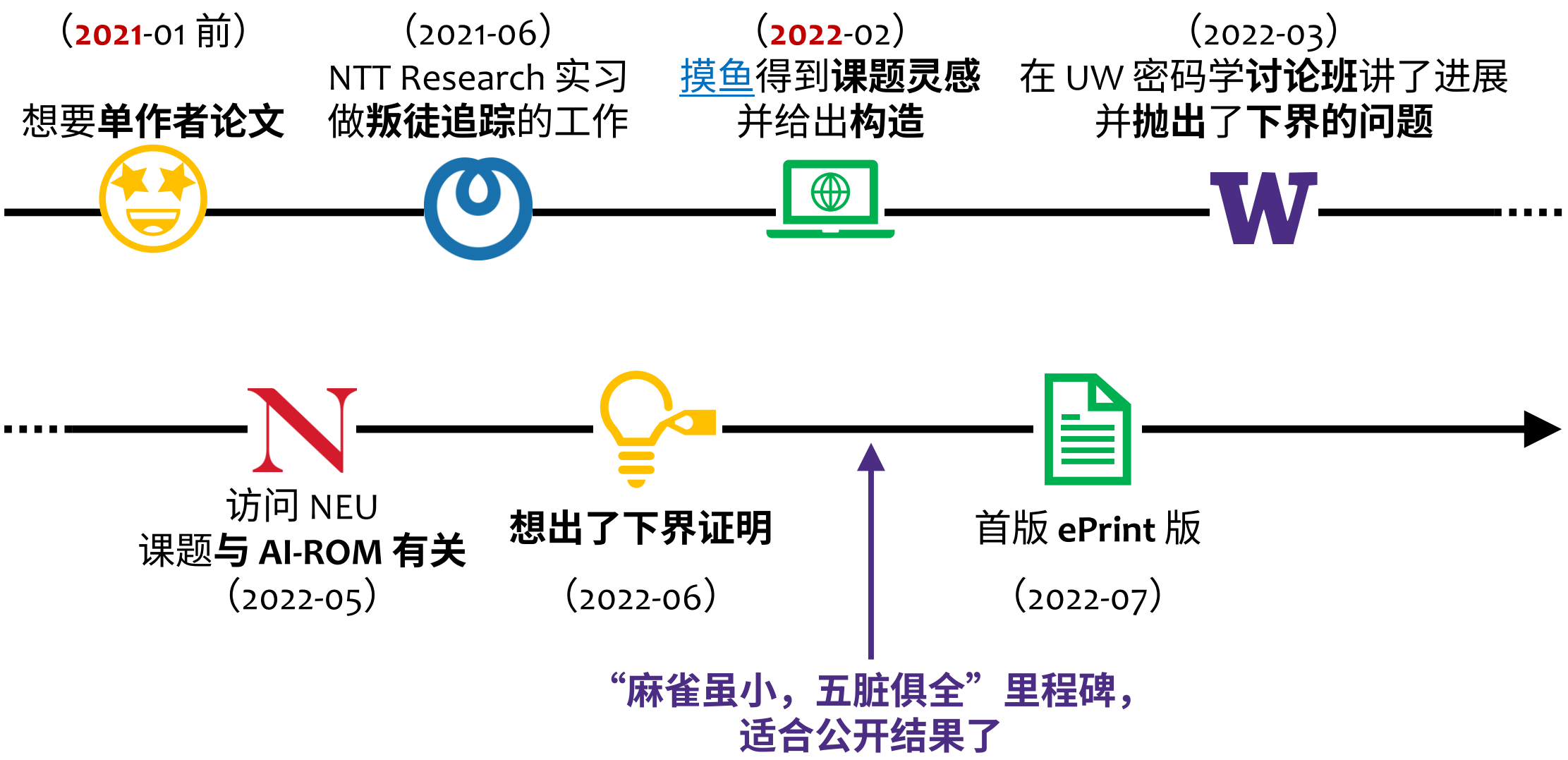
课题的时间线


(2021-01 前)
想要**单作者论文**
(2021-06)
NTT Research 实习
做**叛徒追踪**的工作
(2022-02)
摸鱼得到**课题灵感**
并给出**构造**
(2022-03)
在 UW 密码学**讨论班**讲了进展
并**抛出**了**下界的问题**
访问 NEU
课题**与 AI-ROM 有关**
(2022-05)
想出了下界证明
(2022-06)

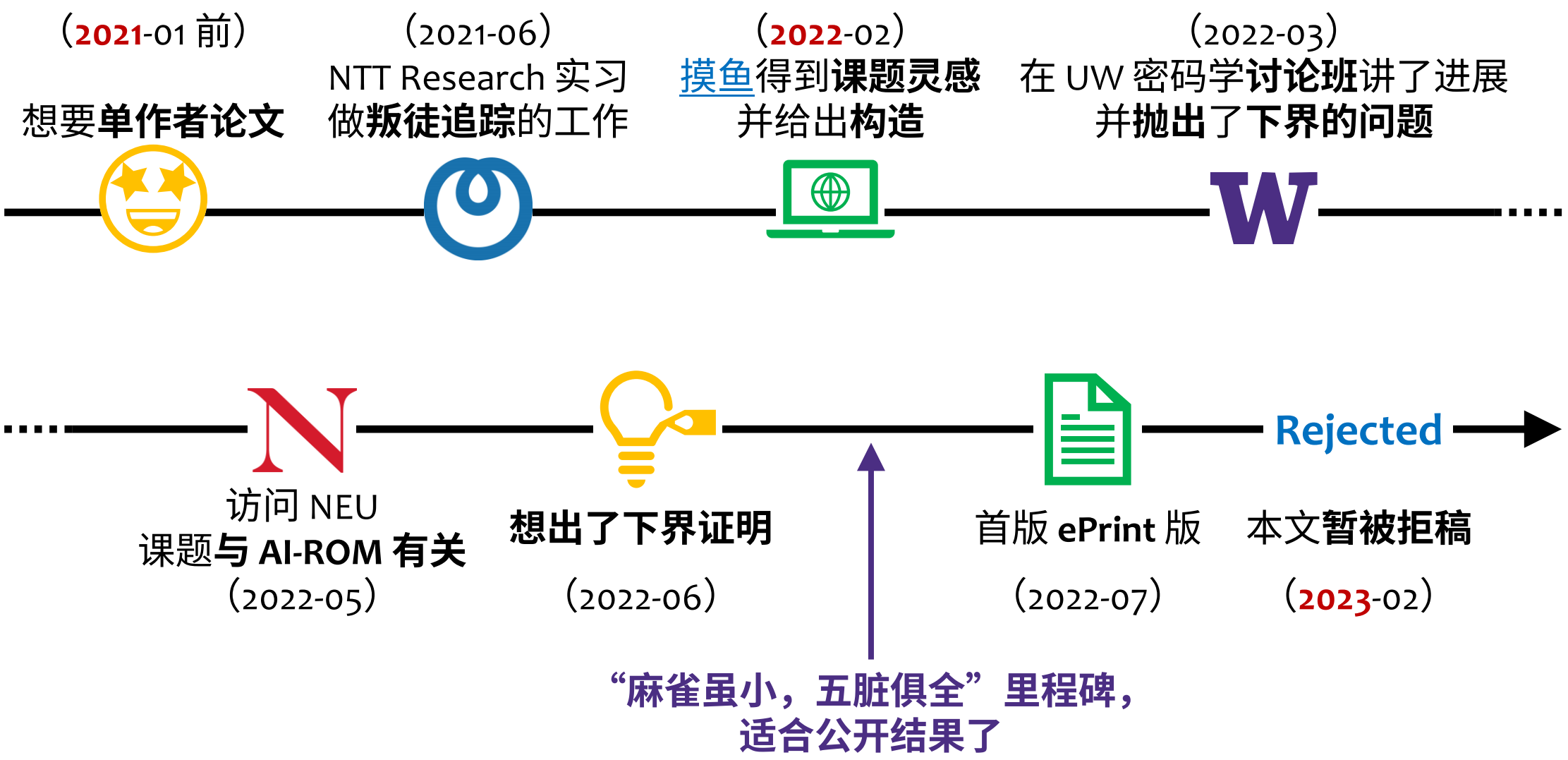
课题的时间线


(2021-01 前)
想要**单作者论文**
(2021-06)
NTT Research 实习
做**叛徒追踪**的工作
(2022-02)
摸鱼得到**课题灵感**
并给出**构造**
(2022-03)
在 UW 密码学**讨论班**讲了进展
并**抛出**了**下界的问题**
W
访问 NEU
课题**与 AI-ROM 有关**
(2022-05)
想出了下界证明
(2022-06)
**“麻雀虽小，五脏俱全”里程碑，
适合公开结果了**

课题的时间线


(2021-01 前)
想要**单作者论文**
(2021-06)
NTT Research 实习
做**叛徒追踪**的工作
(2022-02)
摸鱼得到**课题灵感**
并给出**构造**
(2022-03)
在 UW 密码学**讨论班**讲了进展
并**抛出**了**下界的问题**
访问 NEU
课题**与 AI-ROM 有关**
(2022-05)
想出了下界证明
(2022-06)
首版 **ePrint** 版
(2022-07)
“麻雀虽小，五脏俱全”里程碑，
适合公开结果了

课题的时间线


(2021-01 前)
想要**单作者论文**
(2021-06)
NTT Research 实习
做**叛徒追踪**的工作
(2022-02)
摸鱼得到**课题灵感**
并给出**构造**
(2022-03)
在 UW 密码学**讨论班**讲了进展
并**抛出**了**下界的问题**
访问 NEU
课题**与 AI-ROM 有关**
(2022-05)
想出了下界证明
(2022-06)
首版 ePrint 版
(2022-07)
Rejected
本文**暂被拒稿**
(2023-02)
**“麻雀虽小，五脏俱全”里程碑，
适合公开结果了**

几点感受

几点感受

- **技巧积累、功不唐捐**
  - 我认为本作构造相当朴素，技巧前作都熟知，
    但仔细想的话，学会这些技巧确实费了一番功夫

几点感受

- **技巧积累、功不唐捐**
  - 我认为本作构造相当朴素，技巧前作都熟知，但仔细想的话，学会这些技巧确实费了一番功夫
  - 有些技巧是以前尝试某些“死胡同”课题时学会的，撞南墙的时间并不白费，新学的技巧以后可能有用

几点感受

- **技巧积累、功不唐捐**
  - 我认为本作构造相当朴素，技巧前作都熟知，
    但仔细想的话，学会这些技巧确实费了一番功夫
  - 有些技巧是以前尝试某些“死胡同”课题时学会的，
    撞南墙的时间并不白费，新学的技巧以后可能有用

- **陈酿**
  - 目前的定义是修订过四五轮的结果，
    写下来之时、之后，可能有新想法浮现

几点感受

- **技巧积累、功不唐捐**
  - 我认为本作构造相当朴素，技巧前作都熟知，但仔细想的话，学会这些技巧确实费了一番功夫
  - 有些技巧是以前尝试某些“死胡同”课题时学会的，撞南墙的时间并不白费，新学的技巧以后可能有用

- **陈酿**
  - 目前的定义是修订过四五轮的结果，写下来之时、之后，可能有新想法浮现

- **念念不忘，必有回响**
  - 探究其他问题可能对之前搁置的问题产生启发

再谈、再探“火热的思考”

- ✗ 学术写作　　编造“完美故事”（冰冷的美丽）
- ✓ 已有的尝试　写博客、在一些报告中讲“史实”

再谈、再探“火热的思考”

- ✗ 学术写作　　编造“完美故事”（冰冷的美丽）
- ✓ 已有的尝试　写博客、在一些报告中讲“史实”
- ✓ 本次新尝试　论文修改过程开源
- ○ 未来可尝试　CFAIL

谢谢！

IACR ePrint	2022/925
GitHub	GeeLaw/ahbtr
哔哩哔哩	（无回放，忘记录音了）

luoji@cs.washington.edu
luoji.bio