茫然传输和茫然传输扩展

《安全多方计算——可证明安全视角》第五章

2026 年 1 月 1 日

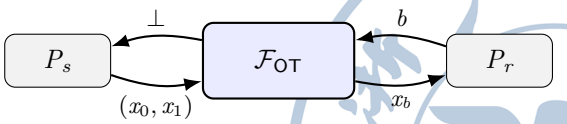
目录

信息论安全的两方 OT 协议？

理想功能 $\mathcal{F}_{\mathsf{OT}}$

$\mathcal{F}_{\mathsf{OT}}$ 与发送方 P_s，接收方 P_r 交互.

- P_r 将 b 发送给 $\mathcal{F}_{\mathsf{OT}}$.
- P_s 将 x_0, x_1 发送给 $\mathcal{F}_{\mathsf{OT}}$.
- P_r 收到 x_b，P_s 收到 $\perp$.

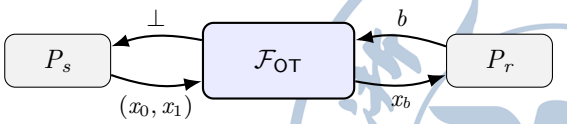


信息论安全的两方 OT 协议？

理想功能 $\mathcal{F}_{\mathsf{OT}}$

$\mathcal{F}_{\mathsf{OT}}$ 与发送方 P_s，接收方 P_r 交互.

- P_r 将 b 发送给 $\mathcal{F}_{\mathsf{OT}}$.
- P_s 将 x_0, x_1 发送给 $\mathcal{F}_{\mathsf{OT}}$.
- P_r 收到 x_b，P_s 收到 $\perp$.



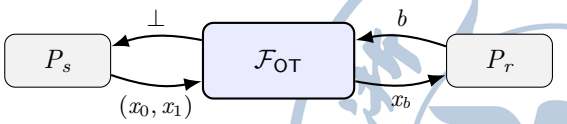
Q：如何构造信息论安全的两方 OT 协议？

信息论安全的两方 OT 协议？

理想功能 $\mathcal{F}_{\mathsf{OT}}$

$\mathcal{F}_{\mathsf{OT}}$ 与发送方 P_s，接收方 P_r 交互.

- P_r 将 b 发送给 $\mathcal{F}_{\mathsf{OT}}$.
- P_s 将 x_0, x_1 发送给 $\mathcal{F}_{\mathsf{OT}}$.
- P_r 收到 x_b，P_s 收到 $\perp$.



Q：如何构造信息论安全的两方 OT 协议？

信息论安全两方 OT 协议的不存在性

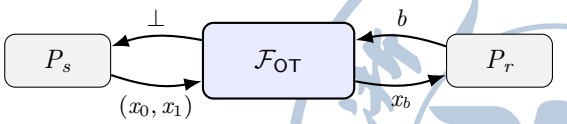
不存在**信息论安全**的两方 OT 协议.

信息论安全的两方 OT 协议？

理想功能 $\mathcal{F}_{\mathsf{OT}}$

$\mathcal{F}_{\mathsf{OT}}$ 与发送方 P_s，接收方 P_r 交互.

- P_r 将 b 发送给 $\mathcal{F}_{\mathsf{OT}}$.
- P_s 将 x_0, x_1 发送给 $\mathcal{F}_{\mathsf{OT}}$.
- P_r 收到 x_b，P_s 收到 $\perp$.



Q：如何构造信息论安全的两方 OT 协议？

信息论安全两方 OT 协议的不存在性

不存在**信息论安全**的两方 OT 协议.

- 证明思路：OT 可用于构造两方 AND 计算，而不存在信息论安全的两方 AND 协议.

从 OT 到 AND

- **注意到**：当 $x_0, x_1 \in \{0,1\}$ 时，

$$x_b = (1 \oplus b)x_0 \oplus bx_1.$$

从 OT 到 AND

- **注意到**：当 $x_0, x_1 \in \{0,1\}$ 时，

$$x_b = (1 \oplus b)x_0 \oplus bx_1.$$

使用两方 OT 构造两方 AND 协议

- **参与方输入**：P_s 持有 a，P_r 持有 b.
- **运行 OT**：令 P_s 发送 $(x_0 = 0,\ x_1 = a)$，P_r 选择 b.
- **输出**：P_r 得到 $x_b = (1 \oplus b) \cdot 0 \oplus b \cdot a = ab$.

从 OT 到 AND

- **注意到**：当 $x_0, x_1 \in \{0,1\}$ 时，

$$x_b = (1 \oplus b)x_0 \oplus bx_1.$$

使用两方 OT 构造两方 AND 协议

- **参与方输入**：P_s 持有 a，P_r 持有 b.
- **运行 OT**：令 P_s 发送 $(x_0 = 0,\ x_1 = a)$，P_r 选择 b.
- **输出**：P_r 得到 $x_b = (1 \oplus b) \cdot 0 \oplus b \cdot a = ab$.

- **若 P_s 被攻陷**：接收方隐私性保证 P_s 不知道 b.
- **若 P_r 被攻陷**：当 $b = 0$ 时发送方隐私性保证不知道 $x_1 = a$.

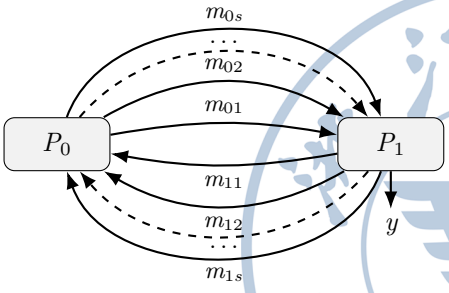
假设存在信息论安全的两方 AND 协议……

消息集合

令 $\mathcal{T}(c,d)$ 为在输入 $b_0=c, b_1=d$ 下，协议可能产生的

$$\mathcal{T}=(m_{01},m_{11},\ldots,m_{0s},m_{1s},y)$$

的所有集合.



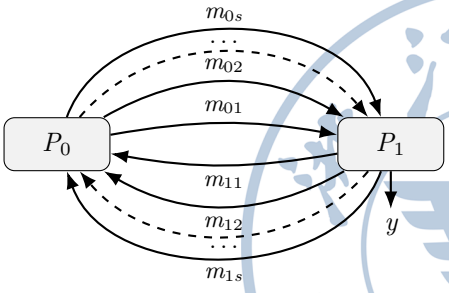
假设存在信息论安全的两方 AND 协议……

消息集合

令 $\mathcal{T}(c,d)$ 为在输入 $b_0=c, b_1=d$ 下，协议可能产生的

$$\mathcal{T}=(m_{01},m_{11},\ldots,m_{0s},m_{1s},y)$$

的所有集合.



断言：

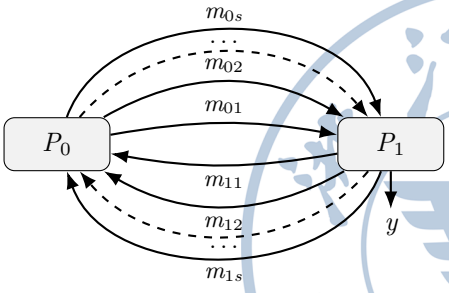
假设存在信息论安全的两方 AND 协议……

消息集合

令 $\mathcal{T}(c,d)$ 为在输入 $b_0=c, b_1=d$ 下，协议可能产生的

$$\mathcal{T}=(m_{01},m_{11},\ldots,m_{0s},m_{1s},y)$$

的所有集合.



断言：

1. $\mathcal{T}(0,0)=\mathcal{T}(0,1)$.

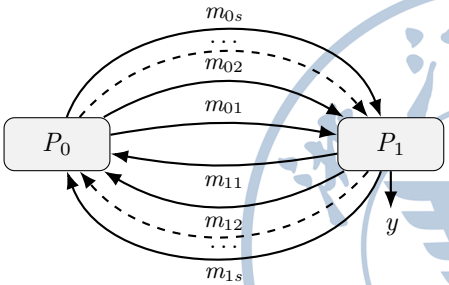
假设存在信息论安全的两方 AND 协议……

消息集合

令 $\mathcal{T}(c,d)$ 为在输入 $b_0=c, b_1=d$ 下，协议可能产生的

$$\mathcal{T}=(m_{01},m_{11},\ldots,m_{0s},m_{1s},y)$$

的所有集合.



断言：

1. $\mathcal{T}(0,0)=\mathcal{T}(0,1)$.
   - 若存在只出现在 $\mathcal{T}(0,0)$ 的消息集合，P_0 可据此区分 b_1.

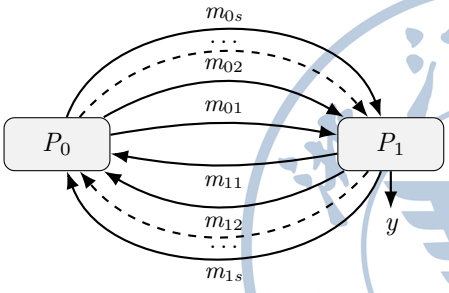
假设存在信息论安全的两方 AND 协议……

消息集合

令 $\mathcal{T}(c,d)$ 为在输入 $b_0=c, b_1=d$ 下，协议可能产生的

$$\mathcal{T}=(m_{01},m_{11},\ldots,m_{0s},m_{1s},y)$$

的所有集合.



断言：

1. $\mathcal{T}(0,0)=\mathcal{T}(0,1)$.
2. $\mathcal{T}(0,0)=\mathcal{T}(1,0)$.

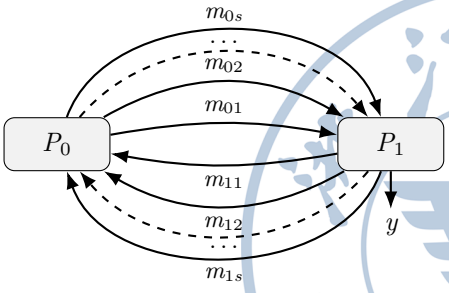
假设存在信息论安全的两方 AND 协议……

消息集合

令 $\mathcal{T}(c,d)$ 为在输入 $b_0=c, b_1=d$ 下，协议可能产生的

$$\mathcal{T}=(m_{01},m_{11},\ldots,m_{0s},m_{1s},y)$$

的所有集合.



断言：

1. $\mathcal{T}(0,0)=\mathcal{T}(0,1)$.
2. $\mathcal{T}(0,0)=\mathcal{T}(1,0)$.
   - 与断言 1 同理（对称地保护 P_1 的隐私）.

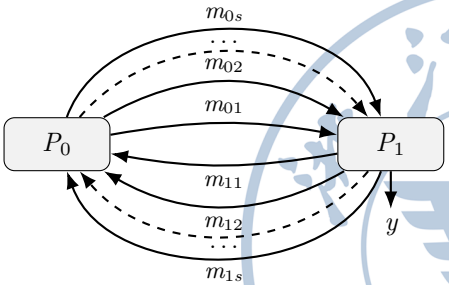
假设存在信息论安全的两方 AND 协议……

消息集合

令 $\mathcal{T}(c,d)$ 为在输入 $b_0=c, b_1=d$ 下，协议可能产生的

$$\mathcal{T}=(m_{01},m_{11},\ldots,m_{0s},m_{1s},y)$$

的所有集合.



断言：

1. $\mathcal{T}(0,0)=\mathcal{T}(0,1)$.
2. $\mathcal{T}(0,0)=\mathcal{T}(1,0)$.
3. $\mathcal{T}(0,1)\cap\mathcal{T}(1,0)\subset\mathcal{T}(1,1)$.

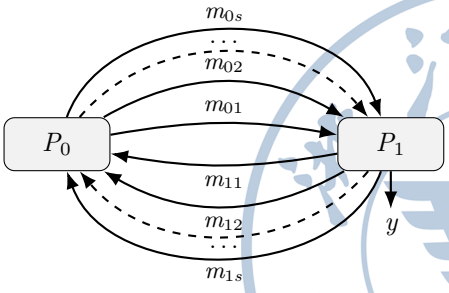
假设存在信息论安全的两方 AND 协议……

消息集合

令 $\mathcal{T}(c,d)$ 为在输入 $b_0=c, b_1=d$ 下，协议可能产生的

$$\mathcal{T}=(m_{01},m_{11},\ldots,m_{0s},m_{1s},y)$$

的所有集合.



断言：

1. $\mathcal{T}(0,0)=\mathcal{T}(0,1)$.
2. $\mathcal{T}(0,0)=\mathcal{T}(1,0)$.
3. $\mathcal{T}(0,1)\cap\mathcal{T}(1,0)\subset\mathcal{T}(1,1)$.
   - 若 $\mathcal{T}$ 同时可由 $(0,1)$ 与 $(1,0)$ 产生，则用对应随机数同时执行可得到 $(1,1)$.

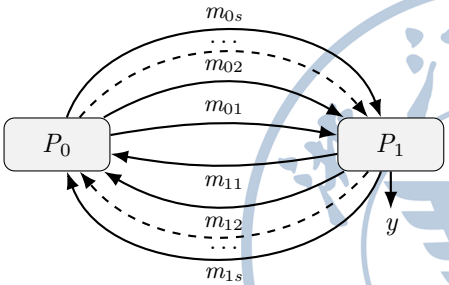
假设存在信息论安全的两方 AND 协议……

消息集合

令 $\mathcal{T}(c,d)$ 为在输入 $b_0=c, b_1=d$ 下，协议可能产生的

$$\mathcal{T}=(m_{01},m_{11},\ldots,m_{0s},m_{1s},y)$$

的所有集合.



断言：

1. $\mathcal{T}(0,0)=\mathcal{T}(0,1)$.
2. $\mathcal{T}(0,0)=\mathcal{T}(1,0)$.
3. $\mathcal{T}(0,1)\cap\mathcal{T}(1,0)\subset\mathcal{T}(1,1)$.
4. $\mathcal{T}(0,0)\cap\mathcal{T}(1,1)=\emptyset$.

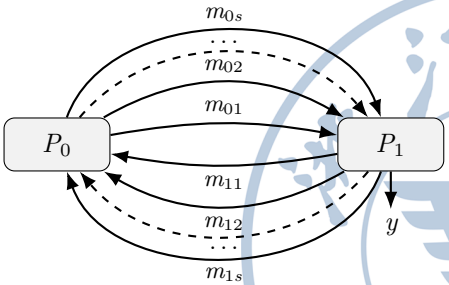
假设存在信息论安全的两方 AND 协议……

消息集合

令 $\mathcal{T}(c,d)$ 为在输入 $b_0=c, b_1=d$ 下，协议可能产生的

$$\mathcal{T}=(m_{01},m_{11},\ldots,m_{0s},m_{1s},y)$$

的所有集合.



断言：

1. $\mathcal{T}(0,0)=\mathcal{T}(0,1)$.
2. $\mathcal{T}(0,0)=\mathcal{T}(1,0)$.
3. $\mathcal{T}(0,1)\cap\mathcal{T}(1,0)\subset\mathcal{T}(1,1)$.
4. $\mathcal{T}(0,0)\cap\mathcal{T}(1,1)=\emptyset$.
   - 当 $(b_0,b_1)=(0,0)$ 时输出 $y=0$，当 $(1,1)$ 时输出 $y=1$.

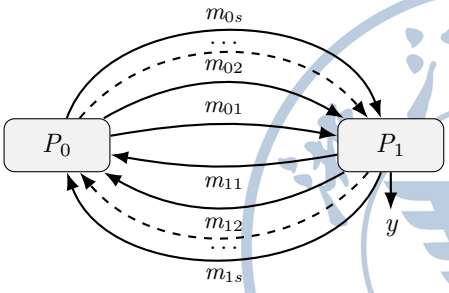
假设存在信息论安全的两方 AND 协议……

消息集合

令 $\mathcal{T}(c,d)$ 为在输入 $b_0=c, b_1=d$ 下，协议可能产生的

$$\mathcal{T}=(m_{01},m_{11},\ldots,m_{0s},m_{1s},y)$$

的所有集合.



断言：

1. $\mathcal{T}(0,0)=\mathcal{T}(0,1)$.
2. $\mathcal{T}(0,0)=\mathcal{T}(1,0)$.
3. $\mathcal{T}(0,1)\cap\mathcal{T}(1,0)\subset\mathcal{T}(1,1)$.
4. $\mathcal{T}(0,0)\cap\mathcal{T}(1,1)=\emptyset$.
   - **矛盾!**

从 OT 中来，到 OT 中去

OT 可以用来：

从 OT 中来，到 OT 中去

OT 可以用来：

- 安全地计算任何函数.

从 OT 中来，到 OT 中去

OT 可以用来：

- 安全地计算任何函数.
- 构造发送方和接收方角色互换的 OT.

从 OT 中来，到 OT 中去

OT 可以用来：

- 安全地计算任何函数.
- 构造发送方和接收方角色互换的 OT.
- 构造 N 选 k OT(k-out-of-N-OT).

从 OT 中来，到 OT 中去

OT 可以用来：

- 安全地计算任何函数.
- 构造发送方和接收方角色互换的 OT.
- 构造 N 选 k OT(k-out-of-N-OT).

基于以下方法可以构造 OT 协议：

从 OT 中来，到 OT 中去

OT 可以用来：

- 安全地计算任何函数.
- 构造发送方和接收方角色互换的 OT.
- 构造 N 选 k OT(k-out-of-N-OT).

基于以下方法可以构造 OT 协议：

- 增强陷门置换 (enhanced trapdoor permutation)

从 OT 中来，到 OT 中去

OT 可以用来：

- 安全地计算任何函数.
- 构造发送方和接收方角色互换的 OT.
- 构造 N 选 k OT(k-out-of-N-OT).

基于以下方法可以构造 OT 协议：

- 增强陷门置换 (enhanced trapdoor permutation)
- DDH 假设

从 OT 中来，到 OT 中去

OT 可以用来：

- 安全地计算任何函数.
- 构造发送方和接收方角色互换的 OT.
- 构造 N 选 k OT(k-out-of-N-OT).

基于以下方法可以构造 OT 协议：

- 增强陷门置换 (enhanced trapdoor permutation)
- DDH 假设
- RSA 假设

从 OT 中来，到 OT 中去

OT 可以用来：

- 安全地计算任何函数.
- 构造发送方和接收方角色互换的 OT.
- 构造 N 选 k OT(k-out-of-N-OT).

基于以下方法可以构造 OT 协议：

- 增强陷门置换 (enhanced trapdoor permutation)
- DDH 假设
- RSA 假设
- 格密码学 (lattice-based cryptography)

从 OT 中来，到 OT 中去

OT 可以用来：

- 安全地计算任何函数.
- 构造发送方和接收方角色互换的 OT.
- 构造 N 选 k OT(k-out-of-N-OT).

基于以下方法可以构造 OT 协议：

- 增强陷门置换 (enhanced trapdoor permutation)
- DDH 假设
- RSA 假设
- 格密码学 (lattice-based cryptography)

注：不能以黑盒的方式基于公钥加密 (Public Key Encryption, PKE) 构造 OT.

半诚实 OT 协议 (基于 DDH 假设)

设 $\mathbb{G}$ 为阶 q 的群（生成元 g），$x_0, x_1 \in \mathbb{G}$，接收方输入 $b \in \{0,1\}$.

输入：x_0, x_1

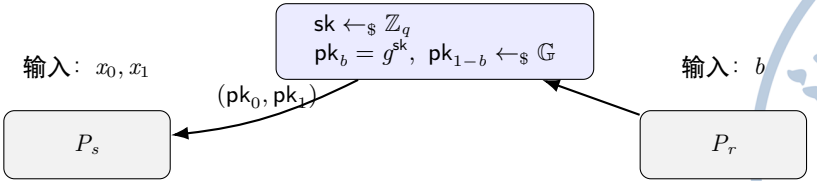
P_s

输入：b

P_r

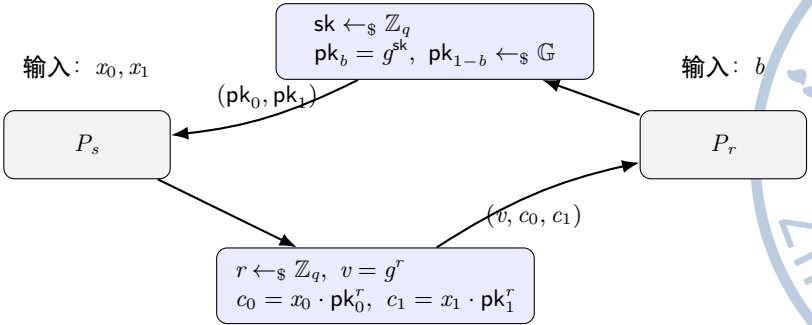
半诚实 OT 协议 (基于 DDH 假设)

设 $\mathbb{G}$ 为阶 q 的群（生成元 g），$x_0, x_1 \in \mathbb{G}$，接收方输入 $b \in \{0,1\}$.



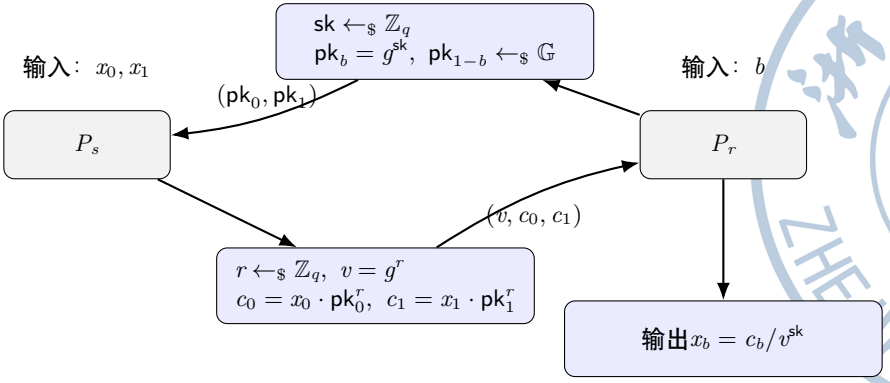
半诚实 OT 协议 (基于 DDH 假设)

设 $\mathbb{G}$ 为阶 q 的群（生成元 g），$x_0, x_1 \in \mathbb{G}$，接收方输入 $b \in \{0,1\}$.



半诚实 OT 协议 (基于 DDH 假设)

设 $\mathbb{G}$ 为阶 q 的群（生成元 g），$x_0, x_1 \in \mathbb{G}$，接收方输入 $b \in \{0,1\}$.



安全性分析

安全性分析

- **接收方隐私**:
  - pk_0 和 pk_1 都是群中的随机元素.
  - P_s 无法区分哪个公钥对应已知的私钥.

安全性分析

- **接收方隐私**:
  - pk_0 和 pk_1 都是群中的随机元素.
  - P_s 无法区分哪个公钥对应已知的私钥.
- **发送方隐私**:
  - 对于 pk_{1-b}，三元组 $(g^r, \mathsf{pk}_{1-b}, \mathsf{pk}_{1-b}^r)$ 是 DDH 三元组.
  - 基于 DDH 假设，pk_{1-b}^r 看起来像随机数.
  - 因此 $c_{1-b} = x_{1-b} \cdot \mathsf{pk}_{1-b}^r$ 完美隐藏了 x_{1-b}（类似于一次一密）.

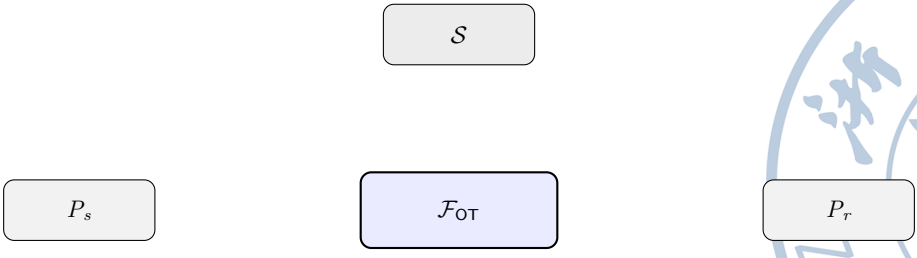
安全性分析

- **接收方隐私**:
  - pk_0 和 pk_1 都是群中的随机元素.
  - P_s 无法区分哪个公钥对应已知的私钥.
- **发送方隐私**:
  - 对于 pk_{1-b}，三元组 $(g^r, \mathsf{pk}_{1-b}, \mathsf{pk}_{1-b}^r)$ 是 DDH 三元组.
  - 基于 DDH 假设，pk_{1-b}^r 看起来像随机数.
  - 因此 $c_{1-b} = x_{1-b} \cdot \mathsf{pk}_{1-b}^r$ 完美隐藏了 x_{1-b}（类似于一次一密）.

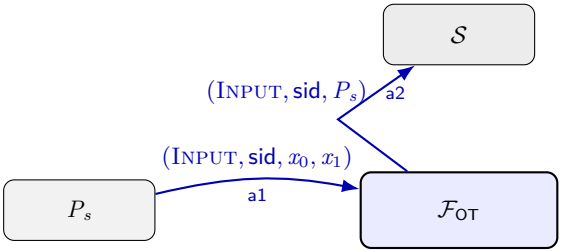
基于 DDH 假设的 OT 协议的安全性

假设 DDH 问题在群 $\mathbb{G}$ 上是困难的. 上一页的协议 Π 对于静态半诚实敌手 UC-安全实现了理想功能 $\mathcal{F}_{\mathsf{OT}}$.

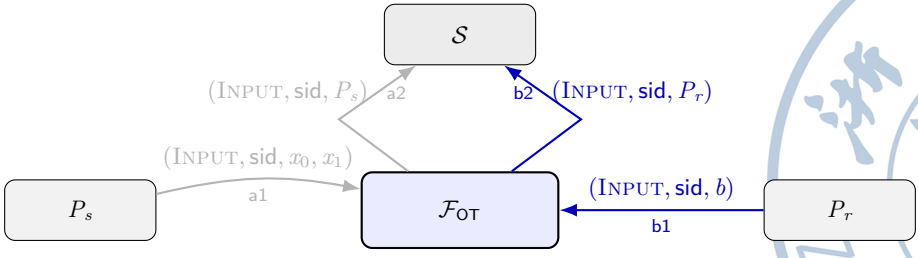
茫然传输理想功能 $\mathcal{F}_{\mathsf{OT}}$



茫然传输理想功能 $\mathcal{F}_{\mathsf{OT}}$

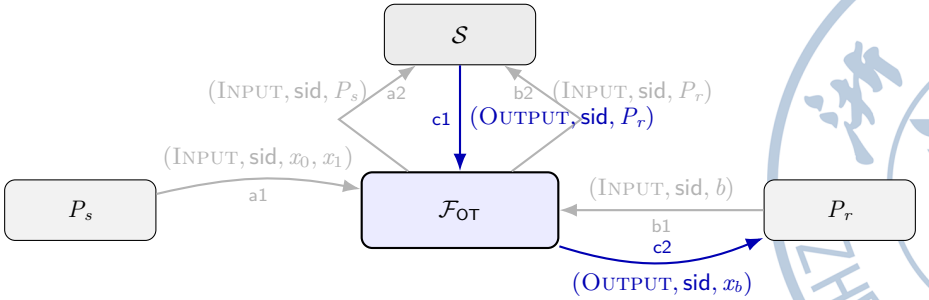


茫然传输理想功能 $\mathcal{F}_{\text{OT}}$



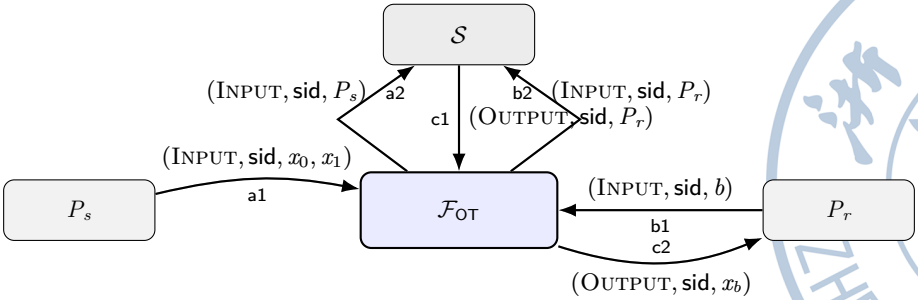
注：理想世界参与方的输入（此页与前一页）顺序由 $\mathcal{Z}$ 指定，无明确顺序关系.

茫然传输理想功能 $\mathcal{F}_{\text{OT}}$

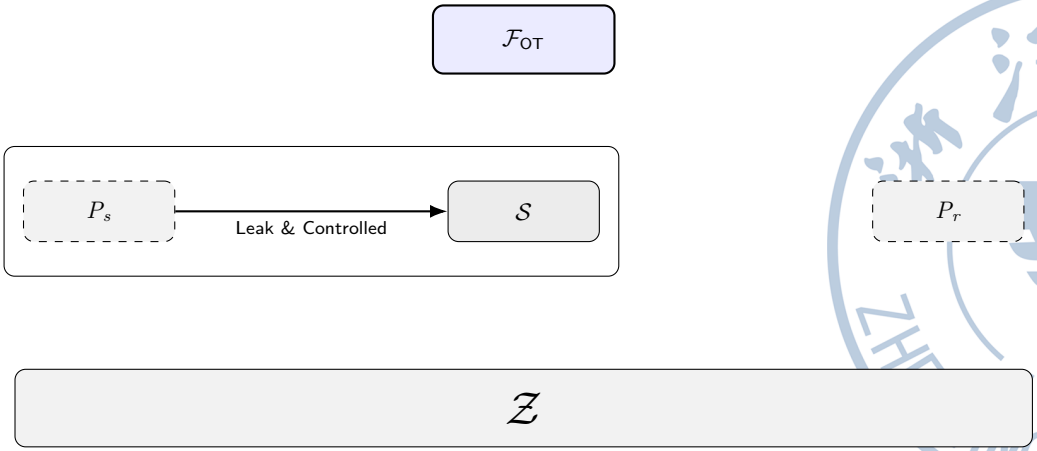


注：该步骤（输出）在前两页（输入）全部执行完毕后才能进行.

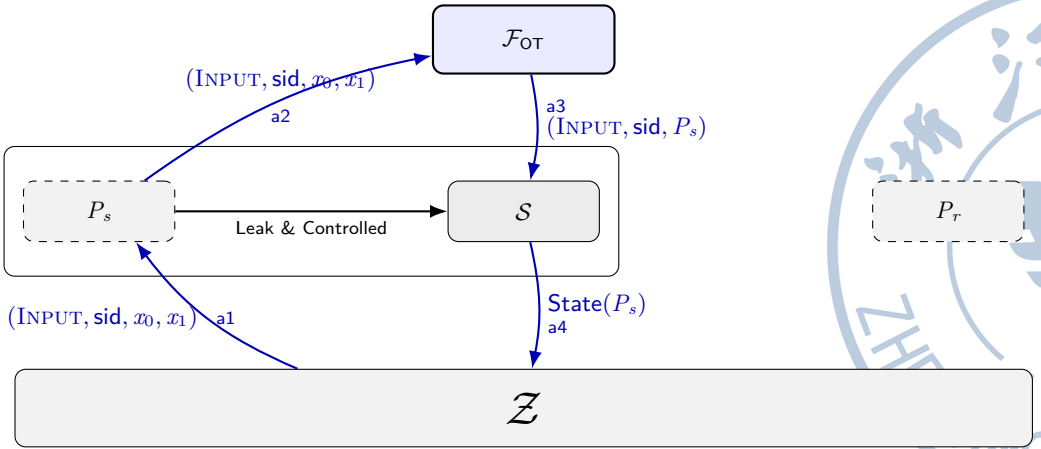
茫然传输理想功能 $\mathcal{F}_{\text{OT}}$



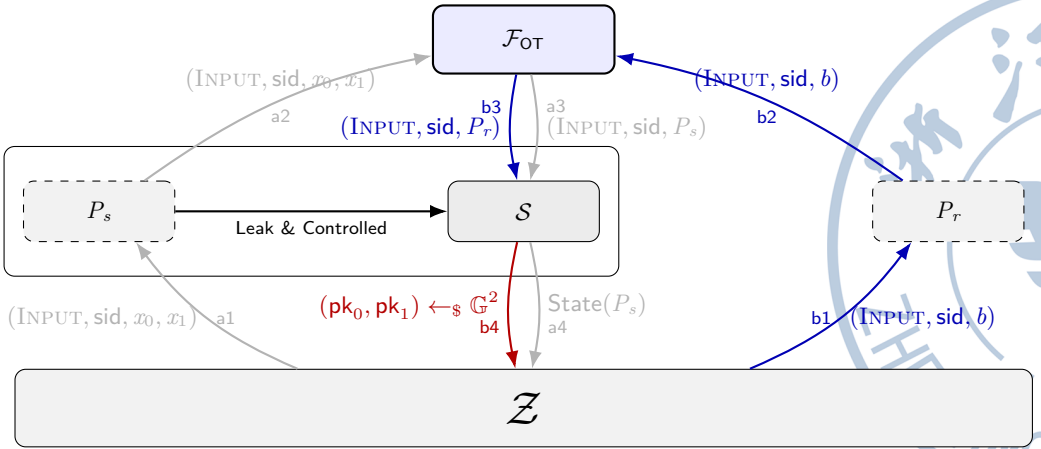
情况 1：发送方 P_s 被攻陷



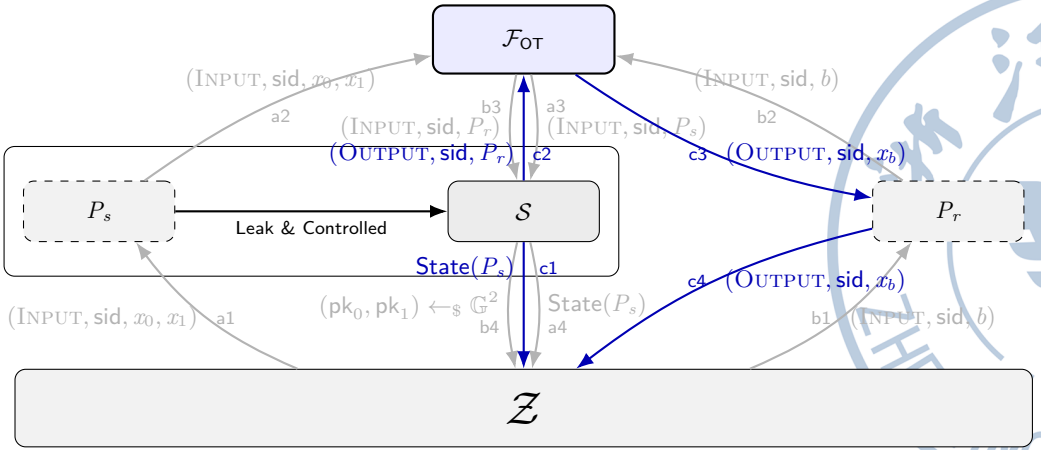
情况 1：发送方 P_s 被攻陷



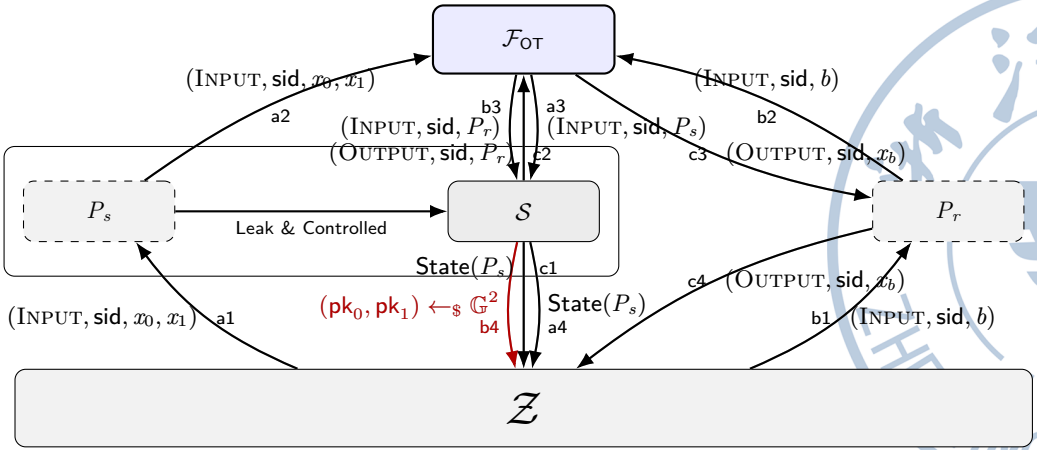
情况 1：发送方 P_s 被攻陷



情况 1：发送方 P_s 被攻陷

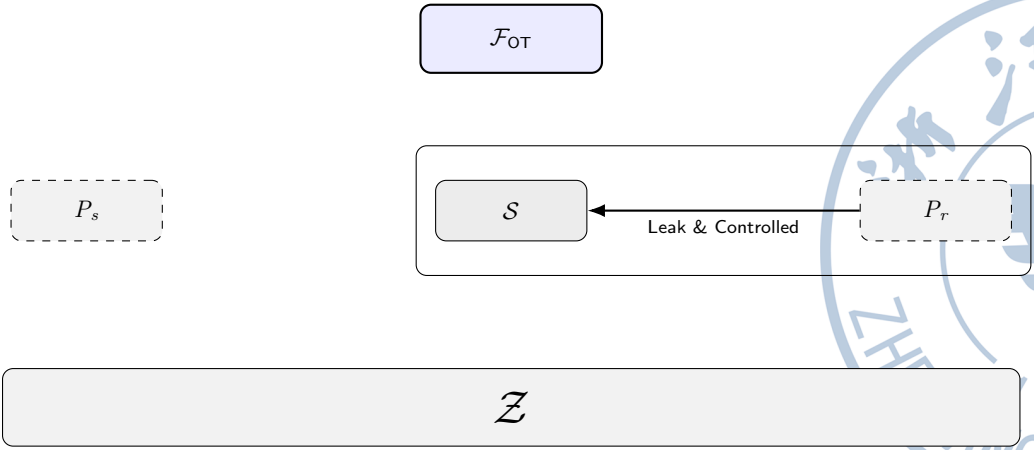


情况 1：发送方 P_s 被攻陷

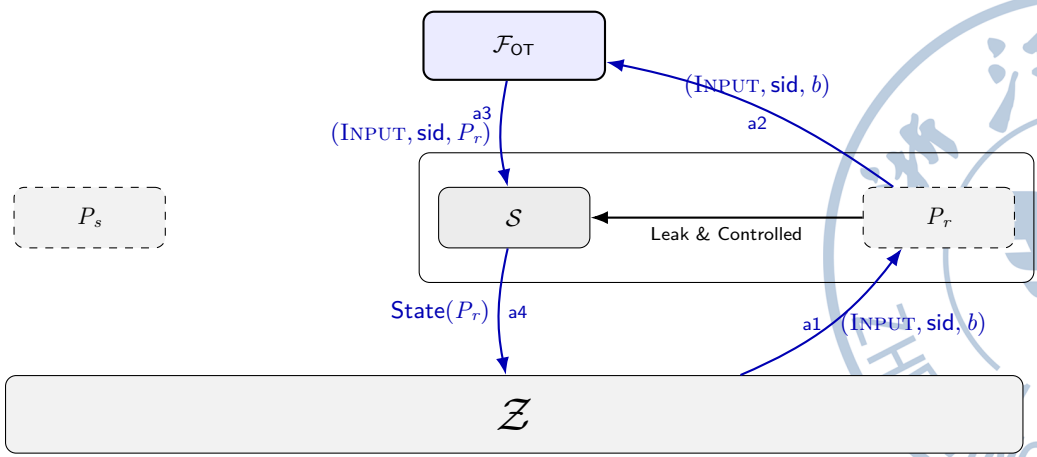


- 不论在理想世界和真实世界中，无论 P_r 的输入 b 是 0 还是 1，$(\text{pk}_0, \text{pk}_1)$ 都是两个群上的随机元素.

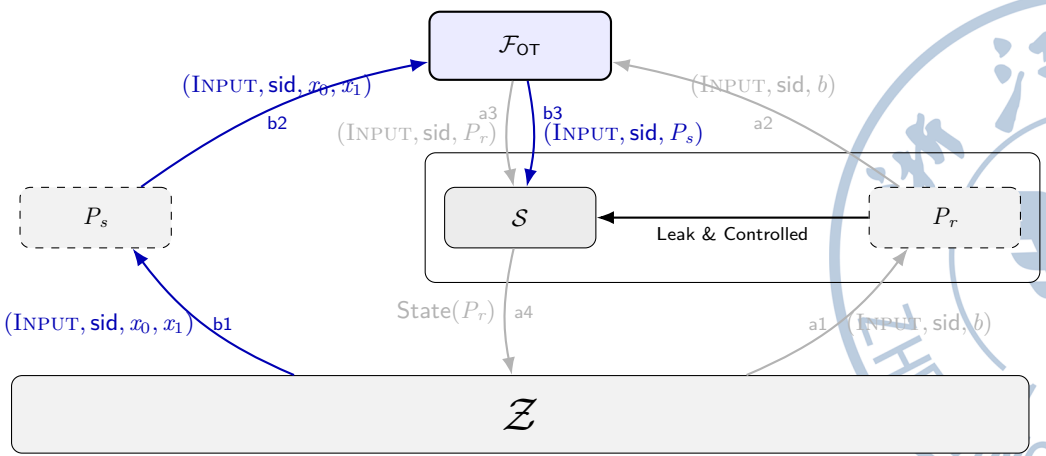
情况 2：接收方 P_r 被攻陷



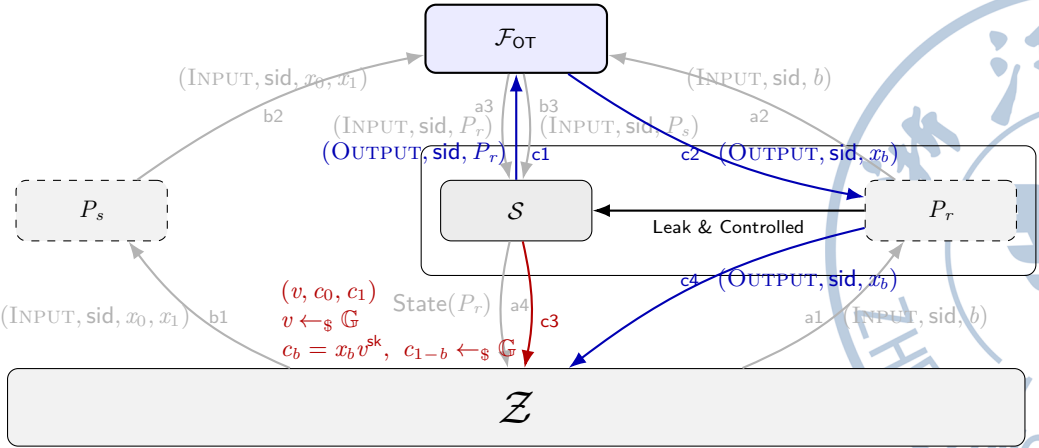
情况 2：接收方 P_r 被攻陷



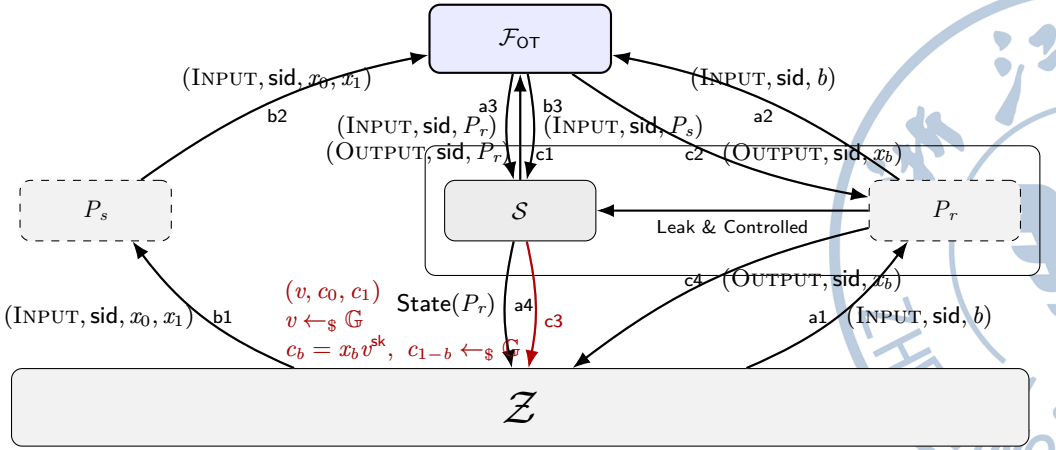
情况 2：接收方 P_r 被攻陷



情况 2：接收方 P_r 被攻陷



情况 2：接收方 P_r 被攻陷



- 在真实世界中，$c_{1-b} = x_{1-b} \cdot \text{pk}_{1-b}^{r}$；在理想世界中，$c_{1-b}$ 是随机群元素.
- 基于 DDH 假设，$\mathcal{Z}$ 无法区分理想世界和真实世界的 $(v, \text{pk}_{1-b}, c_{1-b}/x_{1-b})$.

恶意模型下的挑战

DDH-OT 不是恶意安全的

恶意的接收方可以生成**两个**都知道私钥的公钥 $\mathsf{pk}_0, \mathsf{pk}_1$.

- 结果：接收方可以解密 x_0 和 x_1，破坏发送方隐私.

恶意模型下的挑战

DDH-OT 不是恶意安全的

恶意的接收方可以生成**两个**都知道私钥的公钥 $\mathsf{pk}_0, \mathsf{pk}_1$.

- 结果：接收方可以解密 x_0 和 x_1，破坏发送方隐私.

解决方案：引入协助者 (Helper P_h)

- 利用抗碰撞哈希 (CRH) 作为承诺.
- 确保即使一方恶意，协议依然安全.

三方恶意安全 OT 协议

P_h

输入：x_0, x_1

输入：b

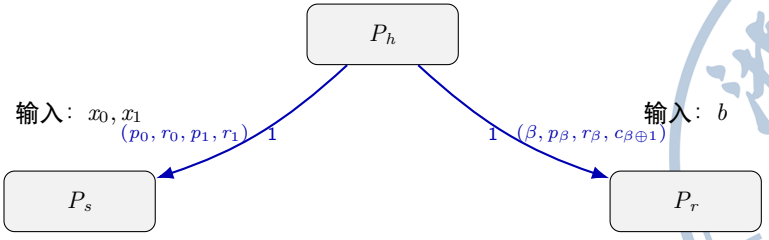
P_s

P_r

准备：$H : \mathcal{M} \times \mathcal{R} \to \mathcal{C}$

三方恶意安全 OT 协议

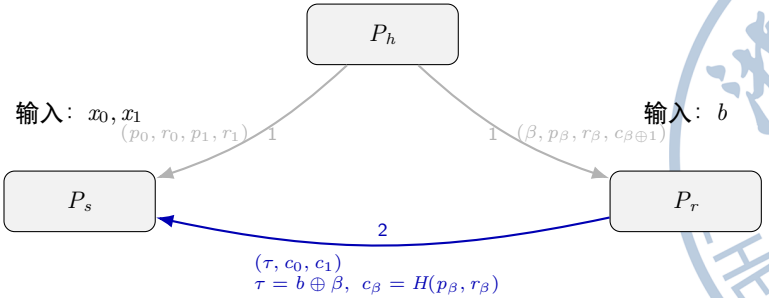
$p_0, p_1 \leftarrow_{\$} \mathcal{M}, \quad r_0, r_1 \leftarrow_{\$} \mathcal{R}, \quad \beta \leftarrow_{\$} \{0,1\}, \quad c_{\beta\oplus 1} = H(p_{\beta\oplus 1}, r_{\beta\oplus 1})$



准备：$H : \mathcal{M} \times \mathcal{R} \to \mathcal{C}$

三方恶意安全 OT 协议

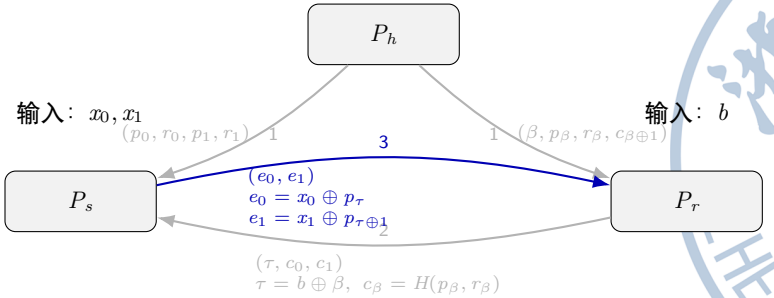
$p_0, p_1 \leftarrow_{\$} \mathcal{M}, \quad r_0, r_1 \leftarrow_{\$} \mathcal{R}, \quad \beta \leftarrow_{\$} \{0,1\}, \quad c_{\beta\oplus 1} = H(p_{\beta\oplus 1}, r_{\beta\oplus 1})$



准备：$H : \mathcal{M} \times \mathcal{R} \to \mathcal{C}$

三方恶意安全 OT 协议

$p_0, p_1 \leftarrow_{\$} \mathcal{M}, \quad r_0, r_1 \leftarrow_{\$} \mathcal{R}, \quad \beta \leftarrow_{\$} \{0,1\}, \quad c_{\beta\oplus 1} = H(p_{\beta\oplus 1}, r_{\beta\oplus 1})$

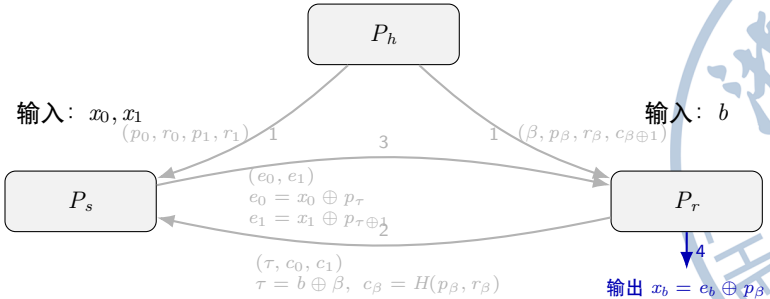


$c_0 \stackrel{?}{=} H(p_0, r_0)$
$c_1 \stackrel{?}{=} H(p_1, r_1)$

准备：$H : \mathcal{M} \times \mathcal{R} \to \mathcal{C}$

三方恶意安全 OT 协议

$p_0, p_1 \leftarrow_{\$} \mathcal{M}, \quad r_0, r_1 \leftarrow_{\$} \mathcal{R}, \quad \beta \leftarrow_{\$} \{0,1\}, \quad c_{\beta\oplus 1} = H(p_{\beta\oplus 1}, r_{\beta\oplus 1})$

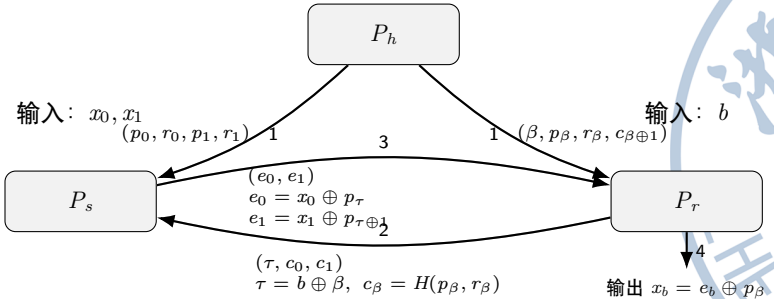


$c_0 \stackrel{?}{=} H(p_0, r_0)$
$c_1 \stackrel{?}{=} H(p_1, r_1)$

准备：$H : \mathcal{M} \times \mathcal{R} \to \mathcal{C}$

三方恶意安全 OT 协议

$$p_0, p_1 \leftarrow_{\$} \mathcal{M}, \quad r_0, r_1 \leftarrow_{\$} \mathcal{R}, \quad \beta \leftarrow_{\$} \{0,1\}, \quad c_{\beta\oplus 1} = H(p_{\beta\oplus 1}, r_{\beta\oplus 1})$$



$$c_0 \stackrel{?}{=} H(p_0, r_0)$$
$$c_1 \stackrel{?}{=} H(p_1, r_1)$$

准备：$H : \mathcal{M} \times \mathcal{R} \to \mathcal{C}$

安全性分析

分析正确性、隐私性与输入独立性；假设最多只有一个参与方被攻陷.

安全性分析

分析正确性、隐私性与输入独立性；假设最多只有一个参与方被攻陷.

协助者被攻陷

- 哈希抗碰撞性保证承诺一致性；否则协议中止.
- 若一致，接收方得到 x_b，正确性成立.
- 协助者无输入且不见安全信道内容，隐私性与输入独立性成立.

安全性分析

分析正确性、隐私性与输入独立性；假设最多只有一个参与方被攻陷.

协助者被攻陷

- 哈希抗碰撞性保证承诺一致性；否则协议中止.
- 若一致，接收方得到 x_b，正确性成立.
- 协助者无输入且不见安全信道内容，隐私性与输入独立性成立.

接收方被攻陷

- $\tau = b \oplus \beta$，b 由诚实协助者的 β 保护.
- 承诺隐藏性保证 $c_{\beta\oplus 1}$ 不泄漏 $p_{\beta\oplus 1}$.
- $e_{b\oplus 1}$ 为一次一密加密，隐私性与正确性成立.

安全性分析

分析正确性、隐私性与输入独立性；假设最多只有一个参与方被攻陷.

协助者被攻陷

- 哈希抗碰撞性保证承诺一致性；否则协议中止.
- 若一致，接收方得到 x_b，正确性成立.
- 协助者无输入且不见安全信道内容，隐私性与输入独立性成立.

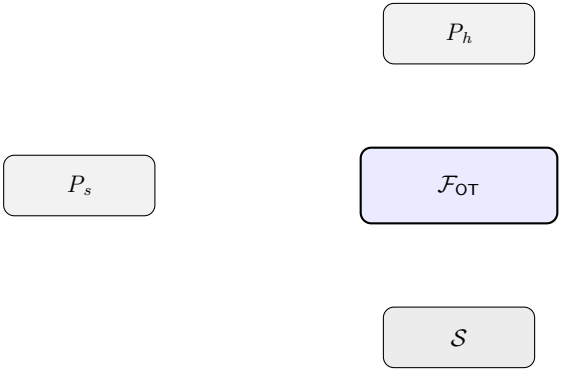
接收方被攻陷

- $\tau = b \oplus \beta$，b 由诚实协助者的 β 保护.
- 承诺隐藏性保证 $c_{\beta\oplus 1}$ 不泄漏 $p_{\beta\oplus 1}$.
- $e_{b\oplus 1}$ 为一次一密加密，隐私性与正确性成立.

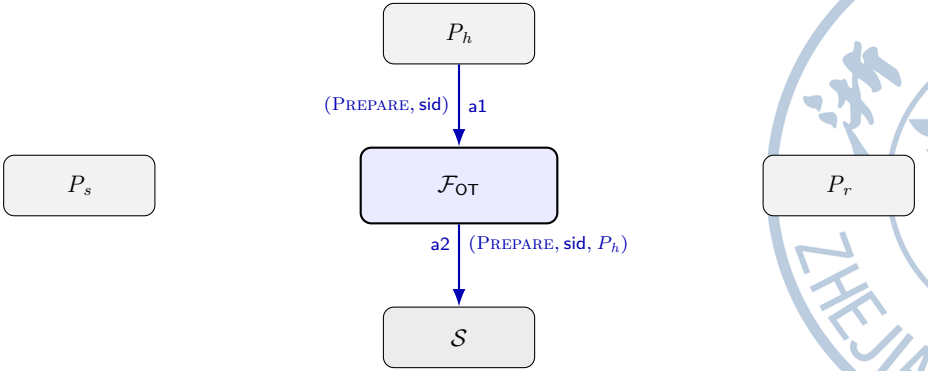
发送方被攻陷

- $x_0 = e_0 \oplus p_\tau$，$x_1 = e_1 \oplus p_{\tau\oplus 1}$.
- 发送方不获知 b，输入独立性与隐私性成立.
- 接收方可由 $e_b \oplus p_\beta$ 恢复 x_b，正确性成立.

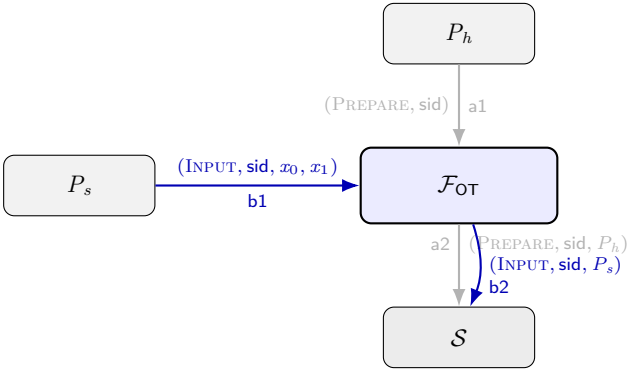
茫然传输理想功能 $\mathcal{F}_{\mathsf{OT}}$



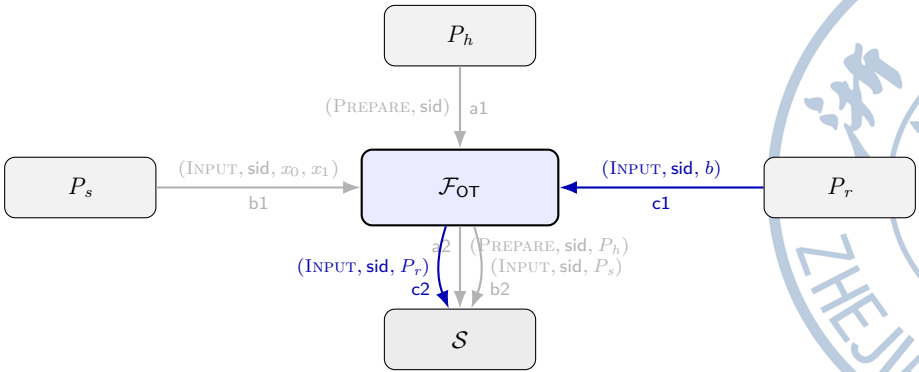
茫然传输理想功能 $\mathcal{F}_{\mathsf{OT}}$



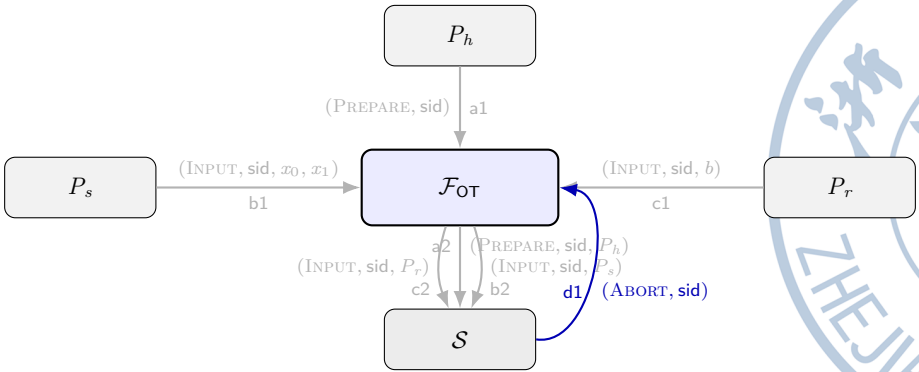
茫然传输理想功能 $\mathcal{F}_{\mathsf{OT}}$



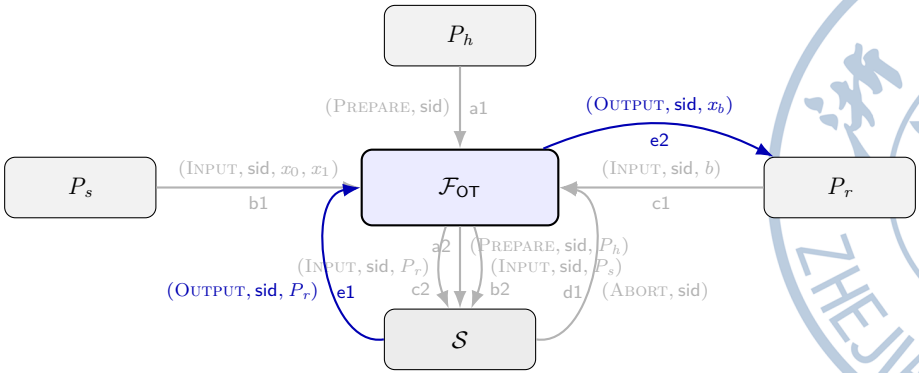
茫然传输理想功能 $\mathcal{F}_{\text{OT}}$



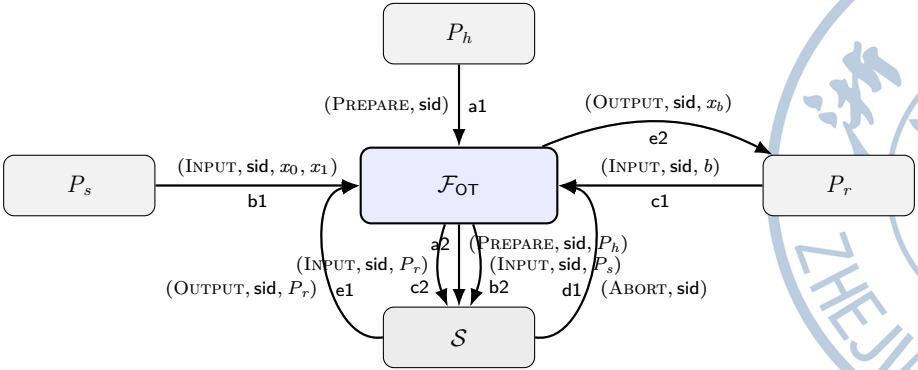
茫然传输理想功能 $\mathcal{F}_{\text{OT}}$



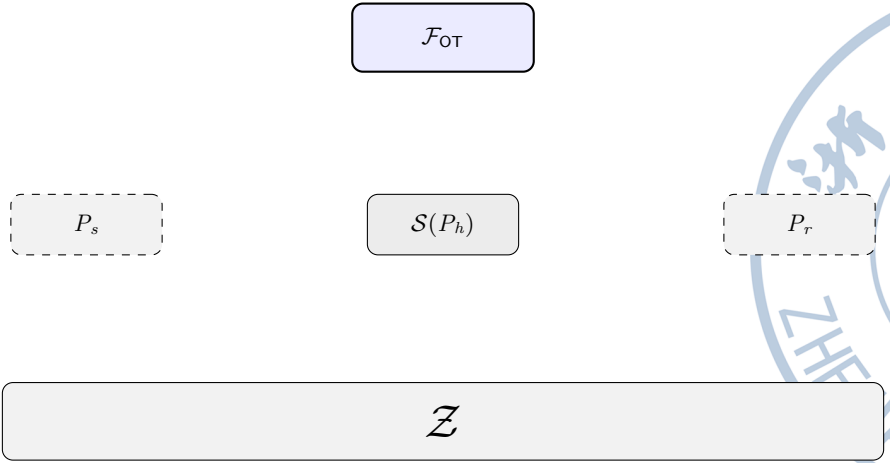
茫然传输理想功能 $\mathcal{F}_{\text{OT}}$



茫然传输理想功能 $\mathcal{F}_{\text{OT}}$

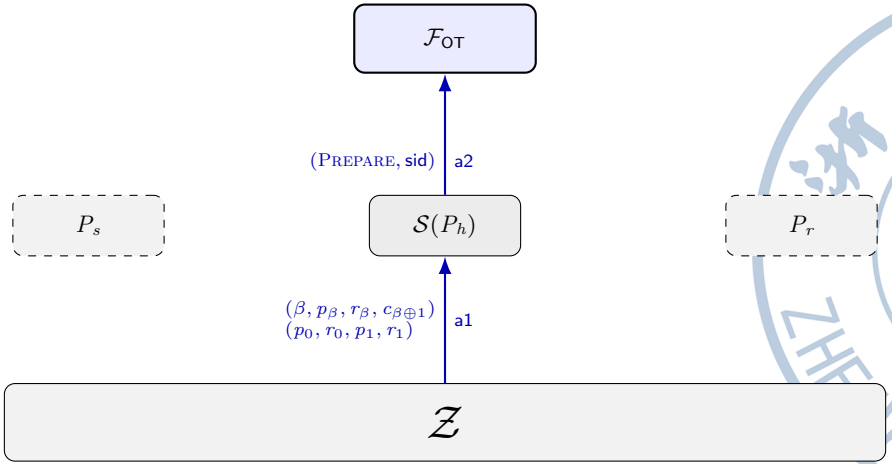


情况 1：协助者 P_h 被攻陷



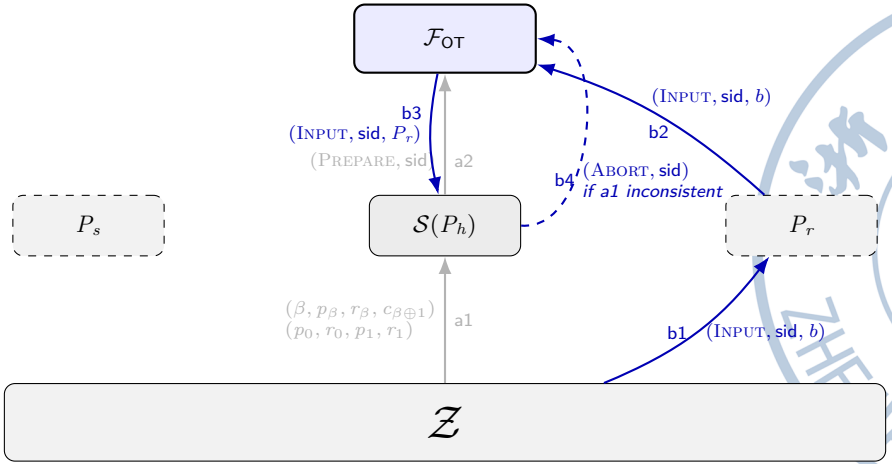
注：模拟器和被攻陷方采用简化表示，省略模拟器实时向环境报告被攻陷方状态的消息.

情况 1：协助者 P_h 被攻陷

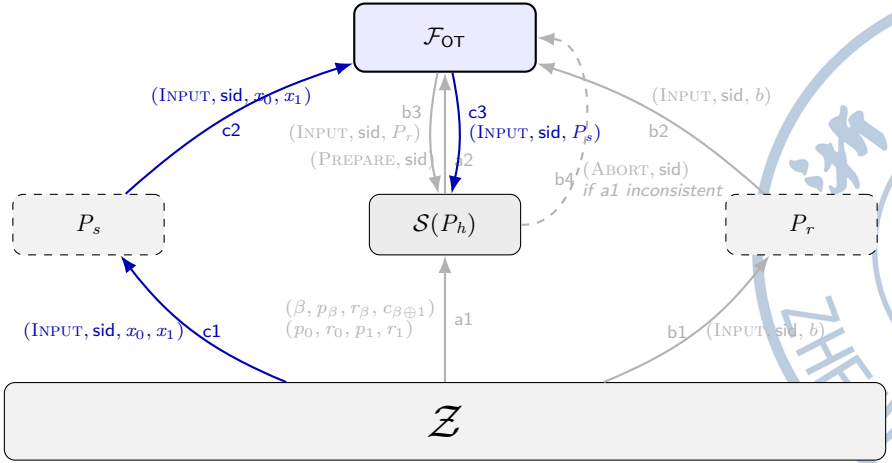


注：这里省略理想功能的回复.

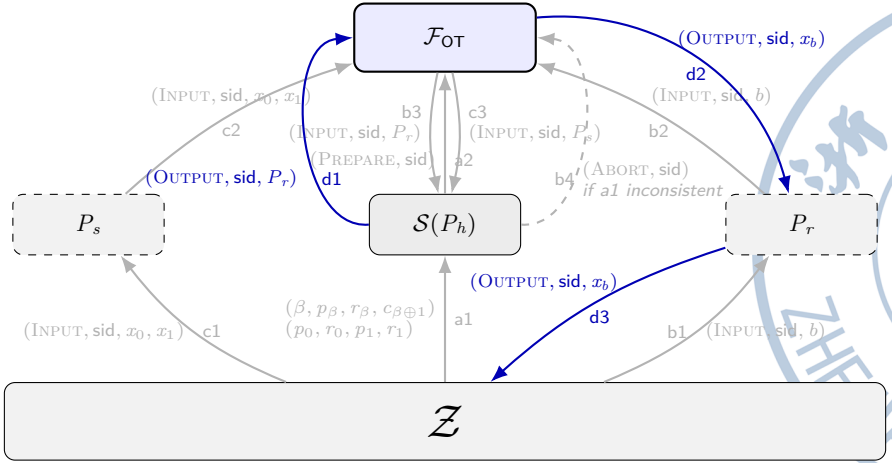
情况 1：协助者 P_h 被攻陷



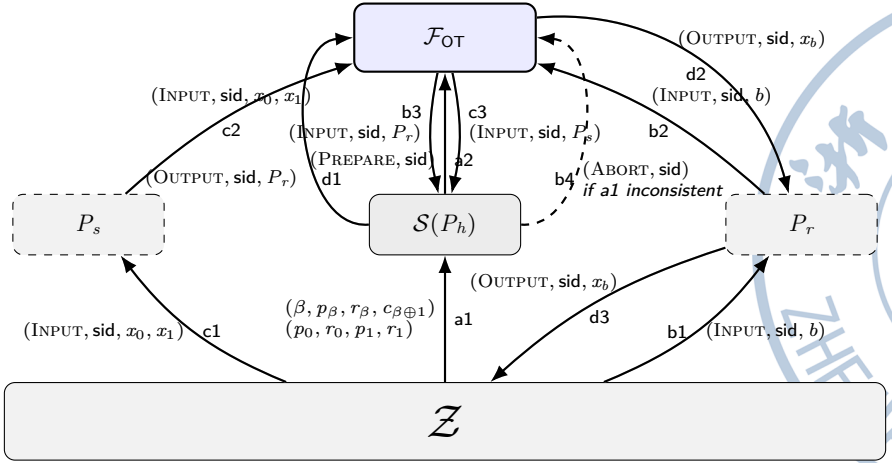
情况 1：协助者 P_h 被攻陷



情况 1：协助者 P_h 被攻陷



情况 1：协助者 P_h 被攻陷



情况 1：安全性分析

Game 0（真实世界）

- P_h 可能向 P_s, P_r 发送不一致消息.
- P_s 无法知晓 P_h 发给 P_r 的内容是否与发给 P_s 的一致，只能检查哈希是否一致.

Game 1（思想实验）

- P_h 可能向 P_s, P_r 发送不一致消息.
- P_s 若发现 P_h 发给 P_r 的内容与发给 P_s 的不一致，强制 P_s 中止协议.

情况 1：安全性分析

Game 0（真实世界）

- P_h 可能向 P_s, P_r 发送不一致消息.
- P_s 无法知晓 P_h 发给 P_r 的内容是否与发给 P_s 的一致，只能检查哈希是否一致.

Game 1（思想实验）

- P_h 可能向 P_s, P_r 发送不一致消息.
- P_s 若发现 P_h 发给 P_r 的内容与发给 P_s 的不一致，强制 P_s 中止协议.

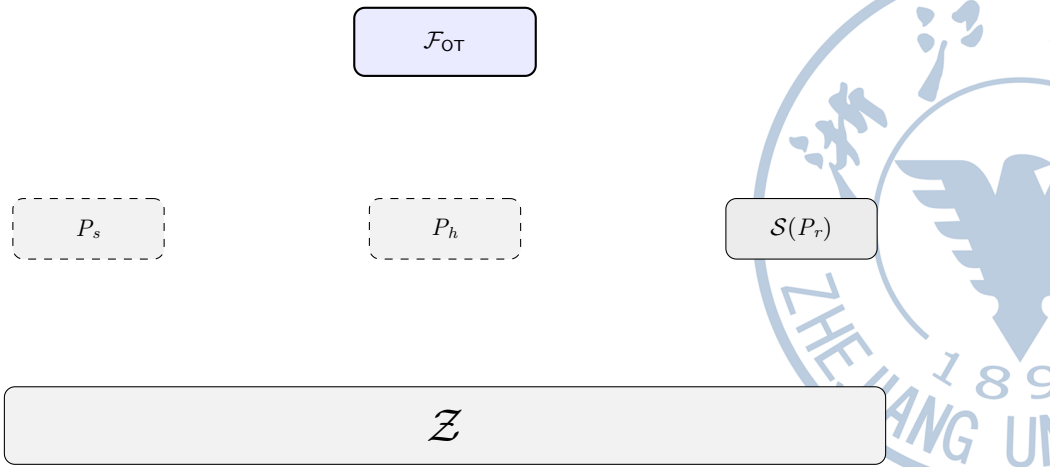
唯一差异

只有在 P_s 与 P_r 收到不同的 (p_β, r_β) 却对应同一哈希时，Game 0 与 Game 1 才会分叉.

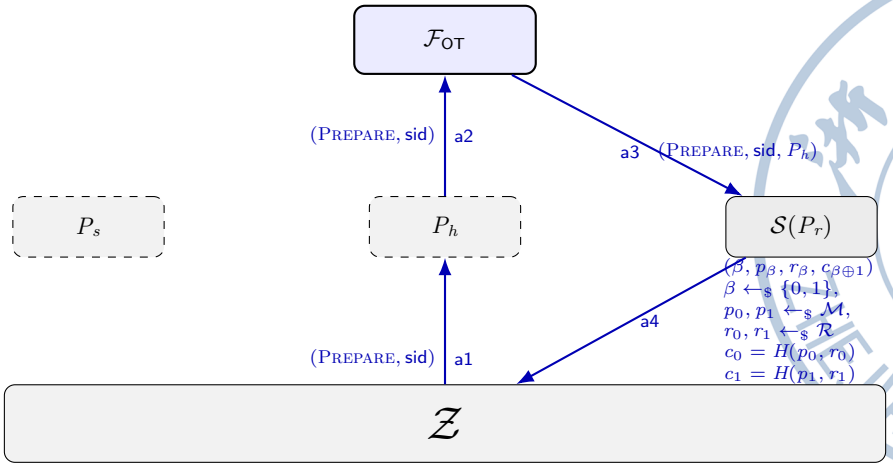
不可区分性

能区分 Game 0/1 等价于找到哈希碰撞，概率可忽略；且 Game 1 与理想世界一致.

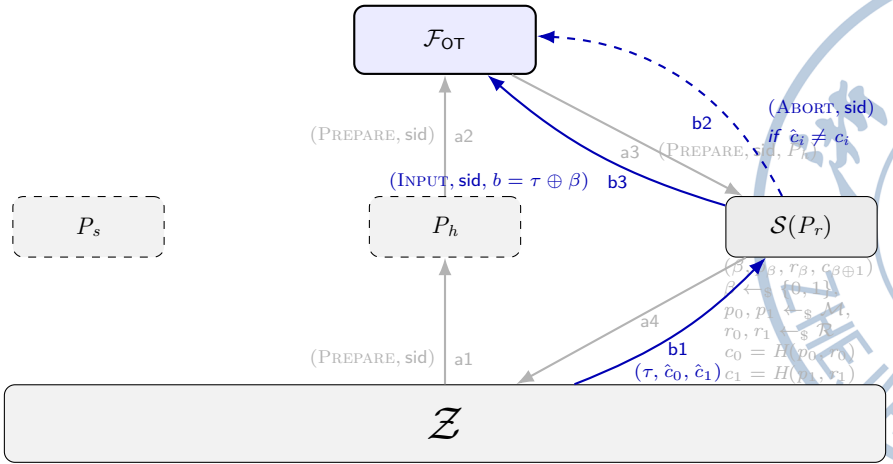
情况 2：接收方 P_r 被攻陷



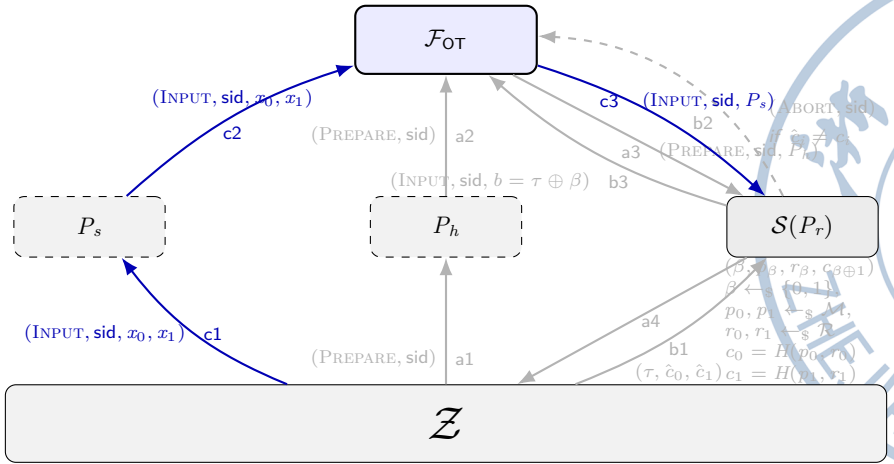
情况 2：接收方 P_r 被攻陷



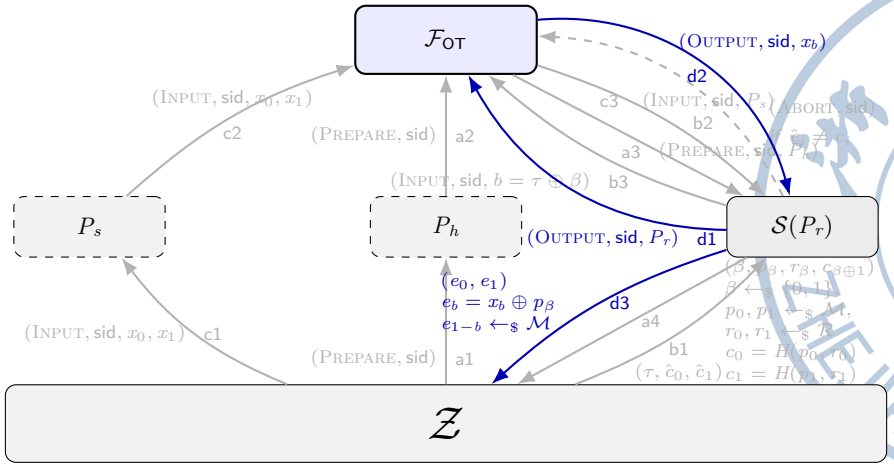
情况 2：接收方 P_r 被攻陷



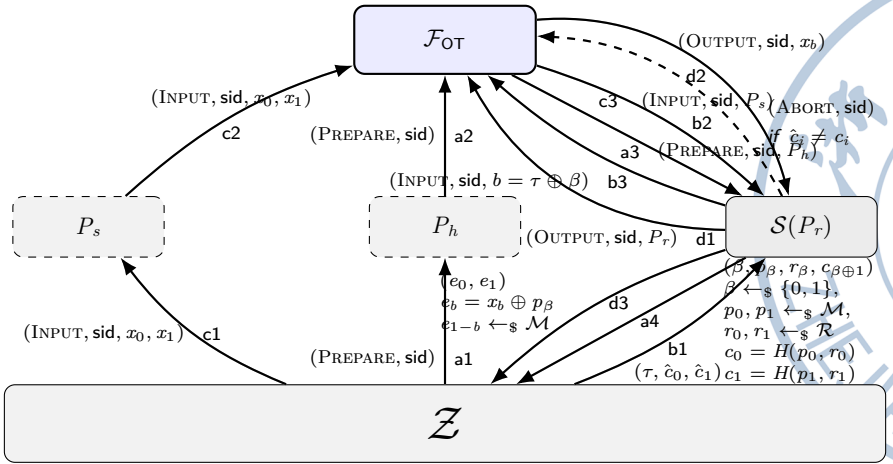
情况 2：接收方 P_r 被攻陷



情况 2：接收方 P_r 被攻陷



情况 2：接收方 P_r 被攻陷



情况 2：安全性分析

Game 0（真实世界）

- $c_{\beta\oplus 1} = H(p_{\beta\oplus 1}, r_{\beta\oplus 1})$.
- $e_{b\oplus 1} = x_{b\oplus 1} \oplus p_{\beta\oplus 1}$.

Game 1

- 仅改动：
  $c_{\beta\oplus 1} = H(p, r_{\beta\oplus 1})$.
- 其中 $p \leftarrow_{\$} \mathcal{M}$ 随机.
- 其余流程与 Game 0 相同.

Game 2

- 直接令 $e_{b\oplus 1} \leftarrow_{\$} \mathcal{M}$.
- 其余流程与 Game 1 相同.

情况 2：安全性分析

Game 0（真实世界）

- $c_{\beta\oplus 1} = H(p_{\beta\oplus 1}, r_{\beta\oplus 1})$.
- $e_{b\oplus 1} = x_{b\oplus 1} \oplus p_{\beta\oplus 1}$.

Game 1

- 仅改动：
  $c_{\beta\oplus 1} = H(p, r_{\beta\oplus 1})$.
- 其中 $p \leftarrow_{\$} \mathcal{M}$ 随机.
- 其余流程与 Game 0 相同.

Game 2

- 直接令 $e_{b\oplus 1} \leftarrow_{\$} \mathcal{M}$.
- 其余流程与 Game 1 相同.

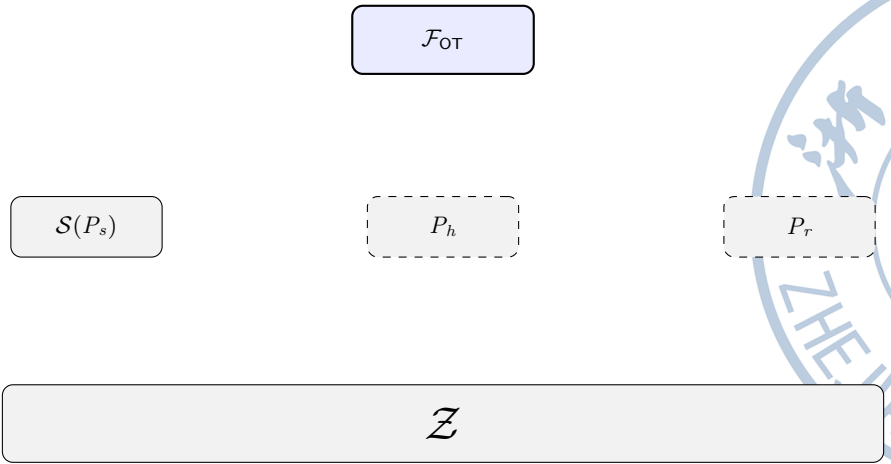
关键差异

Game 0/1 的差异仅在 $c_{\beta\oplus 1}$；Game 1/2 的差异仅在 $e_{b\oplus 1}$.

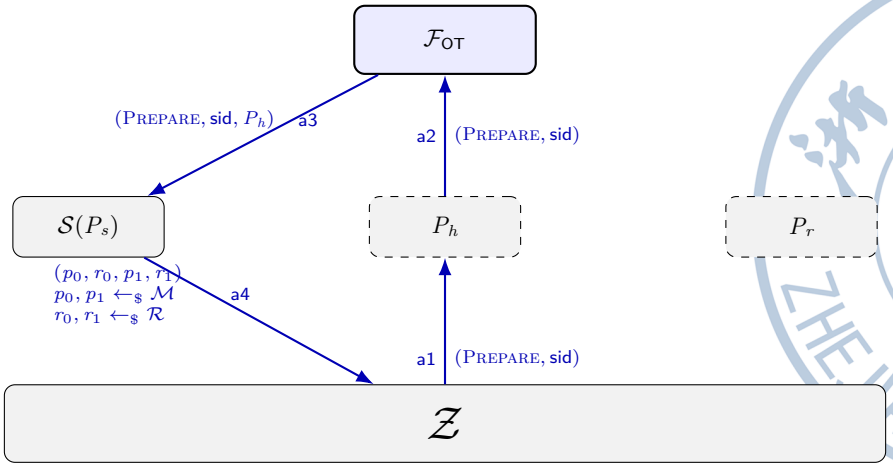
不可区分性

Game 0≈Game 1 由 H 的输入隐藏性；Game 1=Game 2 由一次一密完美隐私性；Game 2 与理想世界一致.

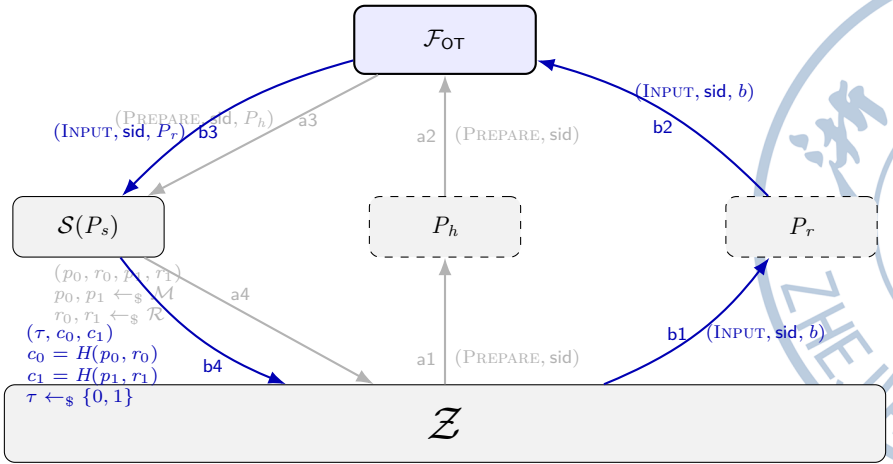
情况 3：发送方 P_s 被攻陷



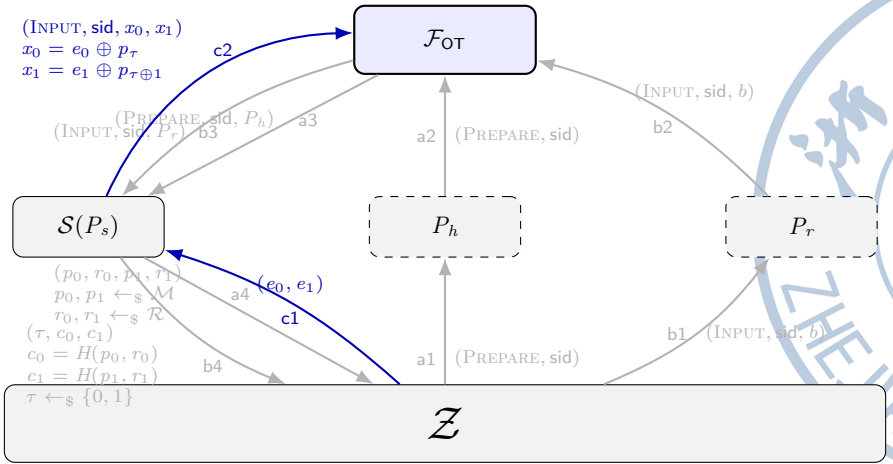
情况 3：发送方 P_s 被攻陷



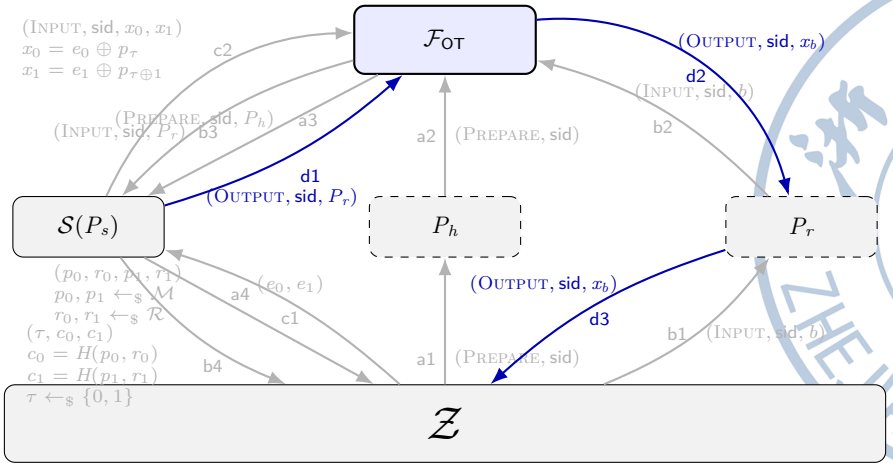
情况 3：发送方 P_s 被攻陷



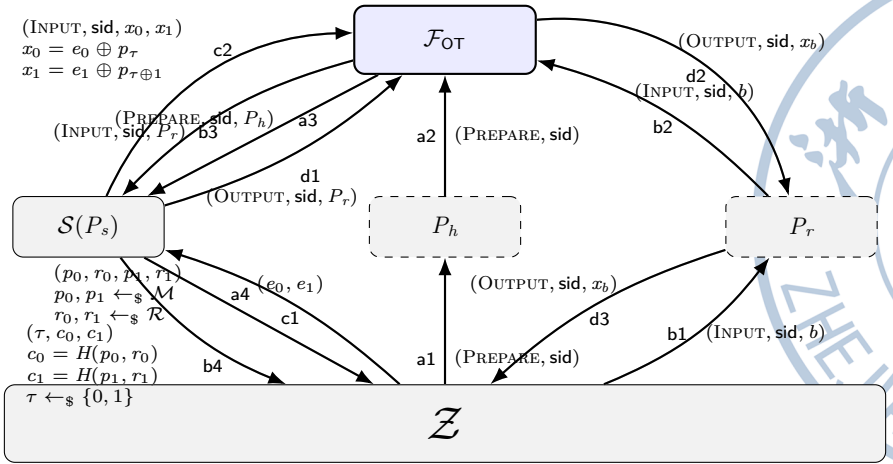
情况 3：发送方 P_s 被攻陷



情况 3：发送方 P_s 被攻陷



情况 3：发送方 P_s 被攻陷



情况 3：安全性分析

真实世界

- P_r 输出为 x_b.
- $\tau = b \oplus \beta$，且 $\beta \leftarrow_{\$} \{0,1\}$.

理想世界

- P_r 输出为 x_b（由 a4,c1,c2 步骤得知）.
- $\tau \leftarrow_{\$} \{0,1\}$.

情况 3：安全性分析

真实世界

- P_r 输出为 x_b.
- $\tau = b \oplus \beta$，且 $\beta \leftarrow_{\$} \{0,1\}$.

理想世界

- P_r 输出为 x_b（由 a4,c1,c2 步骤得知）.
- $\tau \leftarrow_{\$} \{0,1\}$.

唯一差异

仅在 τ 的生成方式上不同.

不可区分性

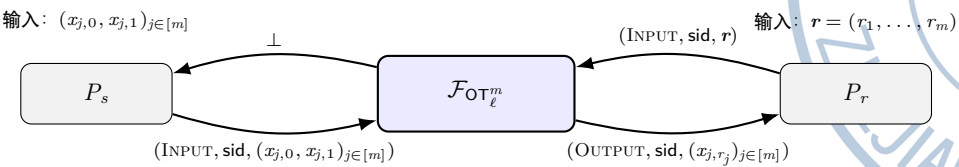
因为 $b \oplus \beta$ 与均匀比特同分布，理想世界与真实世界完美不可区分.

OT 扩展 (OT Extension)

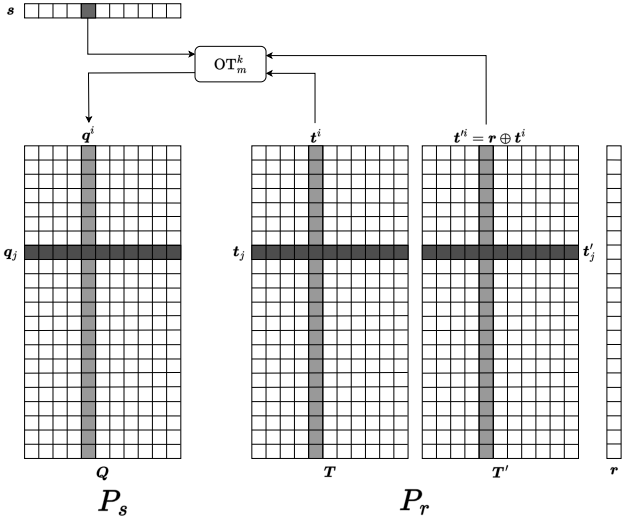
- **动机**: 公钥操作（如 DDH）计算昂贵，难以大规模使用.
- **目标**: 利用少量的 k 个 “基 OT”，扩展为海量 m 个 OT ($m \gg k$).
- **核心技术 (IKNP '03)**:
  - **矩阵转置**: 将 OT 操作方向反转.
  - **随机预言机 (RO)**: 使用哈希函数打破关联.
  - 效率极高：主要运算为 XOR 和 Hash.

OT 扩展 (OT Extension)

- **动机**: 公钥操作（如 DDH）计算昂贵，难以大规模使用.
- **目标**: 利用少量的 k 个 “基 OT”，扩展为海量 m 个 OT ($m \gg k$).
- **核心技术 (IKNP '03)**:
  - **矩阵转置**: 将 OT 操作方向反转.
  - **随机预言机 (RO)**: 使用哈希函数打破关联.
  - 效率极高：主要运算为 XOR 和 Hash.



IKNP 协议示意图



IKNP 协议

输入：$(x_{j,0}, x_{j,1})_{j\in[m]}$

$H : [m] \times \{0,1\}^k \to \{0,1\}^\ell$

输入：$\boldsymbol{r} = (r_1, \ldots, r_m)$

P_s

$\mathcal{F}_{\mathsf{OT}_m^k}$

P_r

IKNP 协议

输入：$(x_{j,0}, x_{j,1})_{j\in[m]}$

$H : [m] \times \{0,1\}^k \to \{0,1\}^\ell$

输入：$\boldsymbol{r} = (r_1, \ldots, r_m)$

P_s

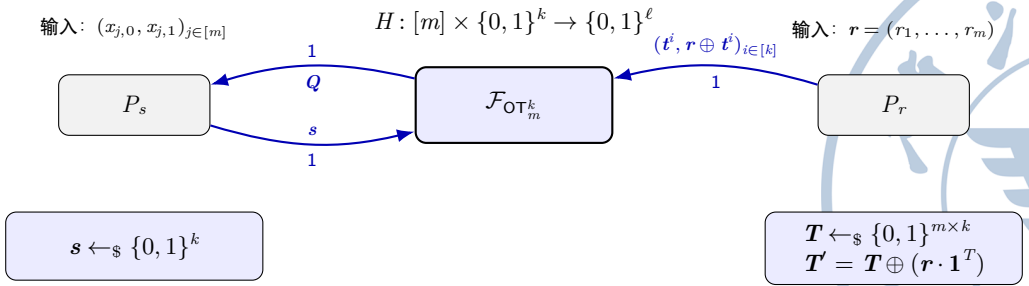
$\mathcal{F}_{\mathsf{OT}_m^k}$

P_r

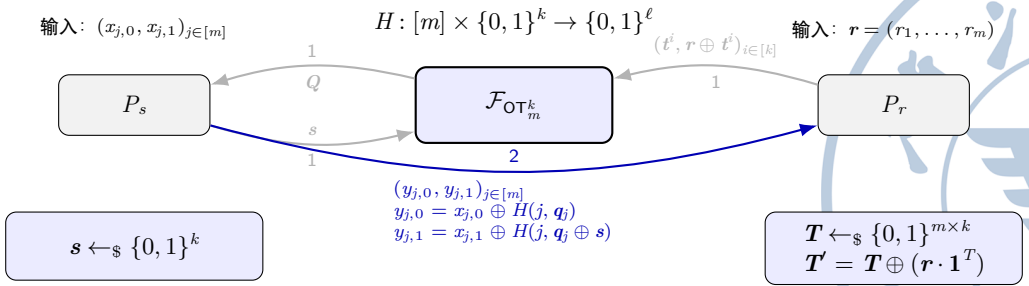
$\boldsymbol{s} \leftarrow_{\$} \{0,1\}^k$

$\boldsymbol{T} \leftarrow_{\$} \{0,1\}^{m\times k}$
$\boldsymbol{T}' = \boldsymbol{T} \oplus (\boldsymbol{r} \cdot \mathbf{1}^T)$

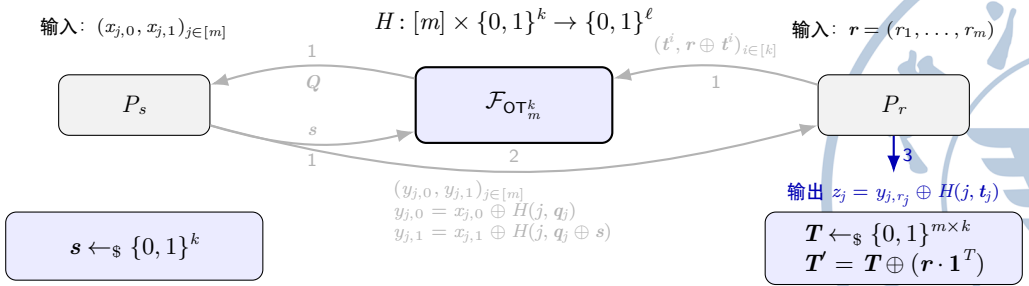
IKNP 协议


输入：$(x_{j,0}, x_{j,1})_{j\in[m]}$
$H : [m] \times \{0,1\}^k \to \{0,1\}^\ell$
输入：$\boldsymbol{r} = (r_1, \ldots, r_m)$
1
$\boldsymbol{Q}$
$(\boldsymbol{t}^i, \boldsymbol{r} \oplus \boldsymbol{t}^i)_{i\in[k]}$
1
P_s
$\mathcal{F}_{\mathsf{OT}^k_m}$
P_r
$\boldsymbol{s}$
1
$\boldsymbol{s} \leftarrow_\$ \{0,1\}^k$
$\boldsymbol{T} \leftarrow_\$ \{0,1\}^{m\times k}$
$\boldsymbol{T}' = \boldsymbol{T} \oplus (\boldsymbol{r} \cdot \boldsymbol{1}^T)$
矩阵 $\boldsymbol{Q}$ 满足
$\boldsymbol{q}^i = (s_i \cdot \boldsymbol{r}) \oplus \boldsymbol{t}^i$
$\boldsymbol{q}_j = (r_j \cdot \boldsymbol{s}) \oplus \boldsymbol{t}_j$

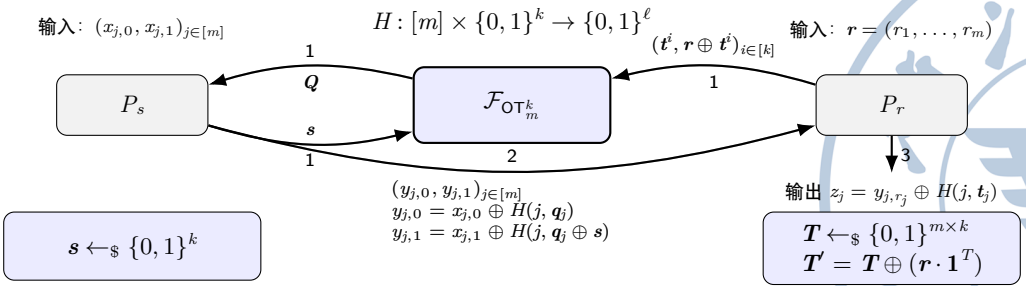
IKNP 协议


输入：$(x_{j,0}, x_{j,1})_{j\in[m]}$
$H : [m] \times \{0,1\}^k \to \{0,1\}^\ell$
输入：$\boldsymbol{r} = (r_1, \ldots, r_m)$
1
Q
$(\boldsymbol{t}^i, \boldsymbol{r} \oplus \boldsymbol{t}^i)_{i\in[k]}$
1
P_s
$\mathcal{F}_{\mathsf{OT}^k_m}$
P_r
s
1
2
$(y_{j,0}, y_{j,1})_{j\in[m]}$
$y_{j,0} = x_{j,0} \oplus H(j, \boldsymbol{q}_j)$
$y_{j,1} = x_{j,1} \oplus H(j, \boldsymbol{q}_j \oplus \boldsymbol{s})$
$\boldsymbol{s} \leftarrow_\$ \{0,1\}^k$
$\boldsymbol{T} \leftarrow_\$ \{0,1\}^{m\times k}$
$\boldsymbol{T}' = \boldsymbol{T} \oplus (\boldsymbol{r} \cdot \boldsymbol{1}^T)$
矩阵 $\boldsymbol{Q}$ 满足
$\boldsymbol{q}^i = (s_i \cdot \boldsymbol{r}) \oplus \boldsymbol{t}^i$
$\boldsymbol{q}_j = (r_j \cdot \boldsymbol{s}) \oplus \boldsymbol{t}_j$

IKNP 协议


输入：$(x_{j,0}, x_{j,1})_{j\in[m]}$
$H : [m] \times \{0,1\}^k \to \{0,1\}^\ell$
输入：$\boldsymbol{r} = (r_1, \ldots, r_m)$
1
Q
$(t^i, \boldsymbol{r} \oplus t^i)_{i\in[k]}$
1
P_s
$\mathcal{F}_{\mathsf{OT}^k_m}$
P_r
s
1
2
3
$(y_{j,0}, y_{j,1})_{j\in[m]}$
$y_{j,0} = x_{j,0} \oplus H(j, \boldsymbol{q}_j)$
$y_{j,1} = x_{j,1} \oplus H(j, \boldsymbol{q}_j \oplus \boldsymbol{s})$
输出 $z_j = y_{j,r_j} \oplus H(j, \boldsymbol{t}_j)$
$\boldsymbol{s} \leftarrow_\$ \{0,1\}^k$
$\boldsymbol{T} \leftarrow_\$ \{0,1\}^{m\times k}$
$\boldsymbol{T}' = \boldsymbol{T} \oplus (\boldsymbol{r} \cdot \mathbf{1}^T)$
矩阵 $\boldsymbol{Q}$ 满足
$\boldsymbol{q}^i = (s_i \cdot \boldsymbol{r}) \oplus \boldsymbol{t}^i$
$\boldsymbol{q}_j = (r_j \cdot \boldsymbol{s}) \oplus \boldsymbol{t}_j$

IKNP 协议



矩阵 $\boldsymbol{Q}$ 满足

$$\boldsymbol{q}^i = (s_i \cdot \boldsymbol{r}) \oplus \boldsymbol{t}^i$$
$$\boldsymbol{q}_j = (r_j \cdot \boldsymbol{s}) \oplus \boldsymbol{t}_j$$

IKNP 协议安全性直观说明（半诚实）

IKNP 协议安全性直观说明（半诚实）

发送方隐私

- P_r 只知道 $\boldsymbol{q}_j$ 与 $\boldsymbol{q}_j \oplus \boldsymbol{s}$ 之一.
- 另一条在 2^k 空间均匀分布，随机谕示机查询成功概率可忽略.

IKNP 协议安全性直观说明（半诚实）

发送方隐私

- P_r 只知道 $\boldsymbol{q}_j$ 与 $\boldsymbol{q}_j \oplus \boldsymbol{s}$ 之一.
- 另一条在 2^k 空间均匀分布，随机谕示机查询成功概率可忽略.

接收方隐私

- 发送方仅见 $\boldsymbol{Q}$.
- 由 $\boldsymbol{T}$ 均匀随机且 $\boldsymbol{Q} = (\boldsymbol{r} \cdot \boldsymbol{s}) \oplus \boldsymbol{T}$，$\boldsymbol{Q}$ 仍均匀随机.
- 因此不泄漏 $\boldsymbol{r}$.

IKNP 协议安全性直观说明（恶意）

IKNP 协议安全性直观说明（恶意）

恶意发送方：安全

- 任意 $(y_{j,0}, y_{j,1})$ 都等价于某些输入 $(x_{j,0}, x_{j,1})$.
- 可视为“输入替换”，协议对恶意发送方仍安全.

IKNP 协议安全性直观说明（恶意）

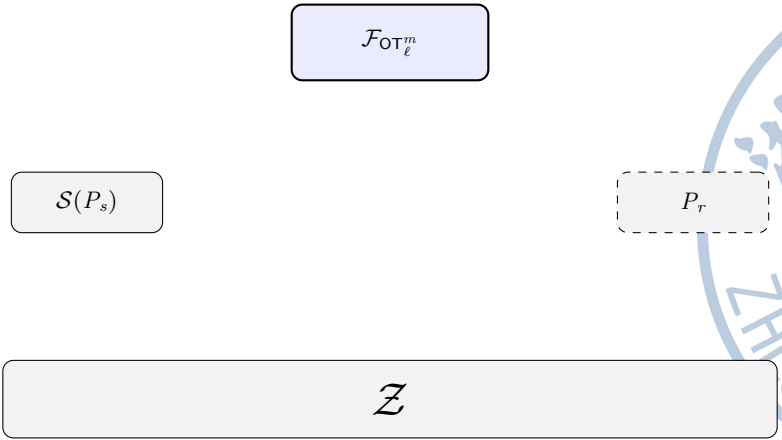
恶意发送方：安全

- 任意 $(y_{j,0}, y_{j,1})$ 都等价于某些输入 $(x_{j,0}, x_{j,1})$.
- 可视为“输入替换”，协议对恶意发送方仍安全.

恶意接收方：不安全

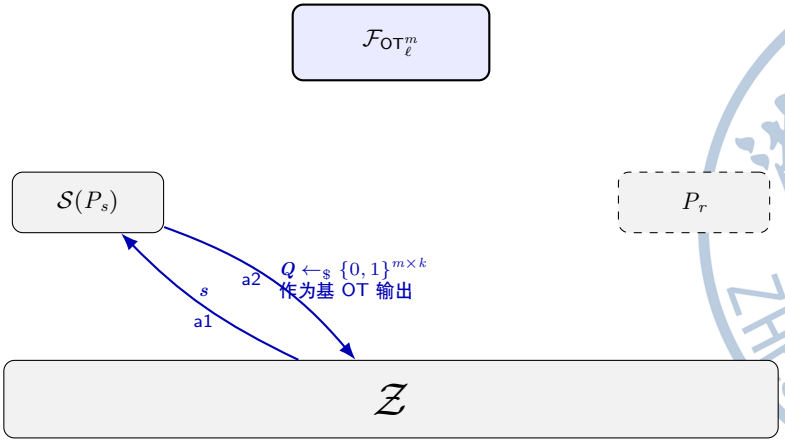
- 伪造 $\boldsymbol{T}, \boldsymbol{T}'$ 使某列仅一位不同，可泄漏 s_i.
- 通过查询 H 恢复 $\boldsymbol{s}$，进而解密两条消息.

情况 1：发送方 P_s 被攻陷（恶意）



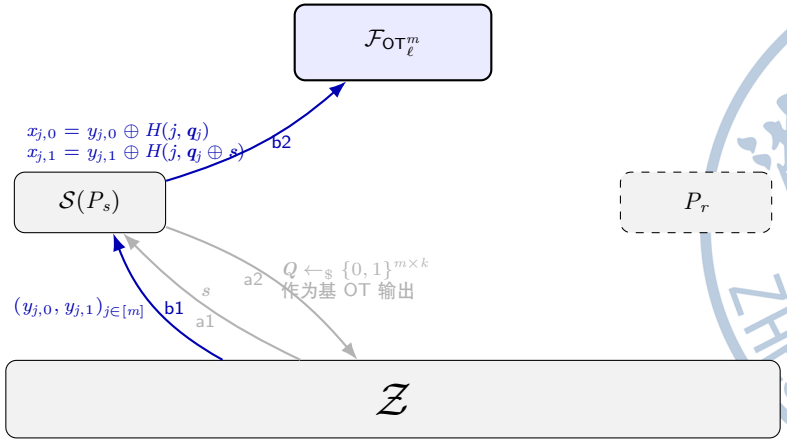
注：这里采用简化消息表示，仅介绍模拟器的工作方式.

情况 1：发送方 P_s 被攻陷（恶意）



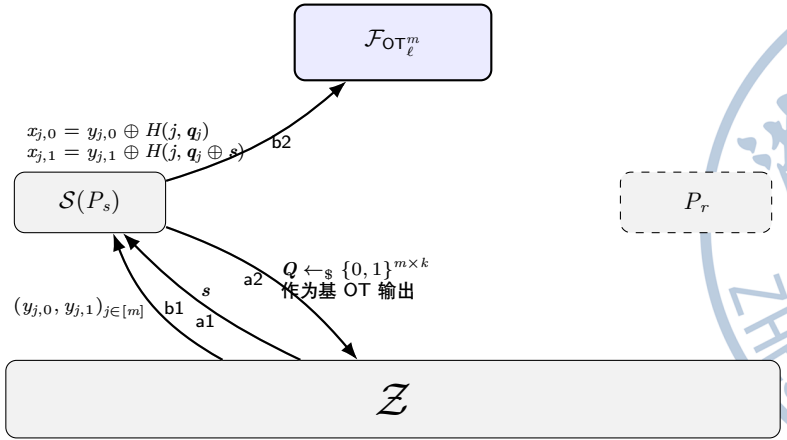
注：这里采用简化消息表示，仅介绍模拟器的工作方式.

情况 1：发送方 P_s 被攻陷（恶意）



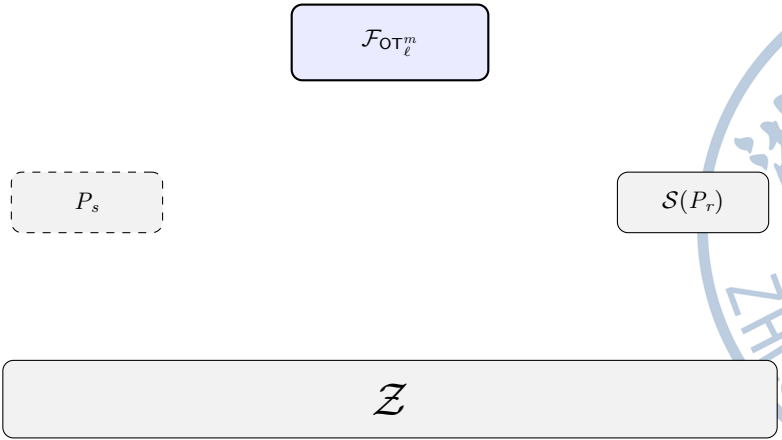
注：这里采用简化消息表示，仅介绍模拟器的工作方式.

情况 1：发送方 P_s 被攻陷（恶意）



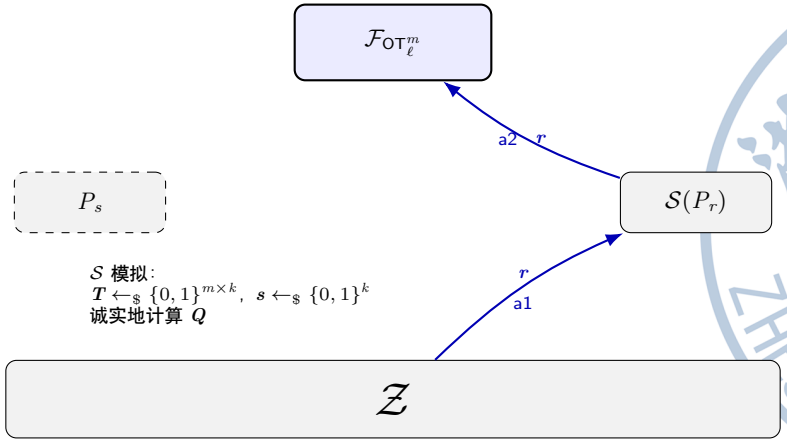
注：这里采用简化消息表示，仅介绍模拟器的工作方式.

情况 2：接收 P_r 被攻陷（半诚实）



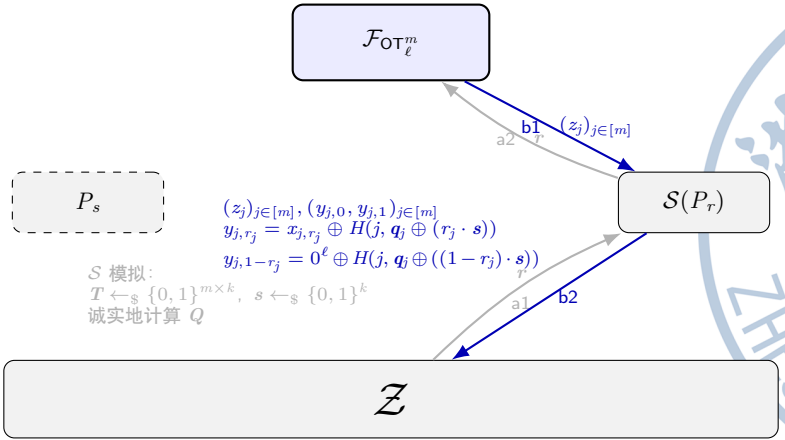
注：这里采用简化消息表示，仅介绍模拟器的工作方式.

情况 2：接收 P_r 被攻陷（半诚实）



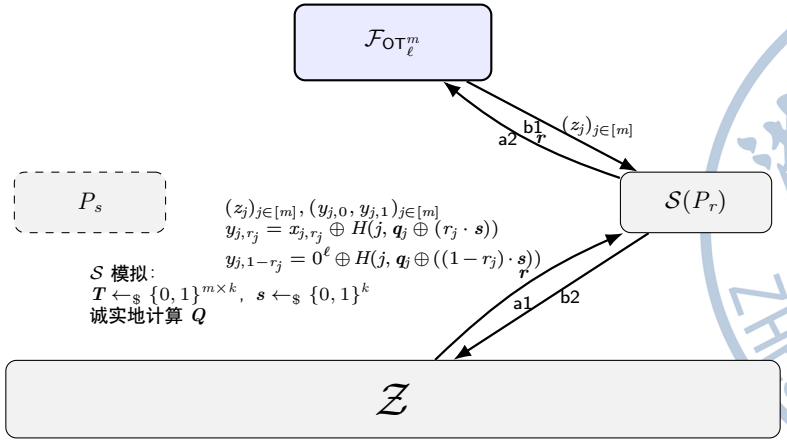
注：这里采用简化消息表示，仅介绍模拟器的工作方式.

情况 2：接收 P_r 被攻陷（半诚实）



注：这里采用简化消息表示，仅介绍模拟器的工作方式.

情况 2：接收 P_r 被攻陷（半诚实）



注：这里采用简化消息表示，仅介绍模拟器的工作方式.

不可区分性分析

P_s 被攻陷时（恶意），理想世界与真实世界完美不可区分：

不可区分性分析

P_s 被攻陷时（恶意），理想世界与真实世界完美不可区分：

- 矩阵 $\boldsymbol{Q}$ 满足 $\boldsymbol{q}_j = (r_j \cdot \boldsymbol{s}) \oplus \boldsymbol{t}_j$，协议正确性成立.

不可区分性分析

P_s 被攻陷时（恶意），理想世界与真实世界完美不可区分：

- 矩阵 $\boldsymbol{Q}$ 满足 $\boldsymbol{q}_j = (r_j \cdot \boldsymbol{s}) \oplus \boldsymbol{t}_j$，协议正确性成立.
- 由 $\mathcal{S}$ 提取 $(x_{j,0}, x_{j,1})$ 的方式，P_r 在理想/真实世界输出一致.

不可区分性分析

P_s 被攻陷时（恶意），理想世界与真实世界完美不可区分：

- 矩阵 $\boldsymbol{Q}$ 满足 $\boldsymbol{q}_j = (r_j \cdot \boldsymbol{s}) \oplus \boldsymbol{t}_j$，协议正确性成立.
- 由 $\mathcal{S}$ 提取 $(x_{j,0}, x_{j,1})$ 的方式，P_r 在理想/真实世界输出一致.
- 敌手视角下 $\boldsymbol{Q}$ 在理想/真实世界均为均匀随机矩阵.

不可区分性分析

P_s 被攻陷时（恶意），理想世界与真实世界完美不可区分：

- 矩阵 $\boldsymbol{Q}$ 满足 $\boldsymbol{q}_j = (r_j \cdot \boldsymbol{s}) \oplus \boldsymbol{t}_j$，协议正确性成立.
- 由 $\mathcal{S}$ 提取 $(x_{j,0}, x_{j,1})$ 的方式，P_r 在理想/真实世界输出一致.
- 敌手视角下 $\boldsymbol{Q}$ 在理想/真实世界均为均匀随机矩阵.

P_r 被攻陷时（半诚实），区分优势不超过 $(t+1) \cdot 2^{-k}$：

不可区分性分析

P_s 被攻陷时（恶意），理想世界与真实世界完美不可区分：

- 矩阵 $\boldsymbol{Q}$ 满足 $\boldsymbol{q}_j = (r_j \cdot \boldsymbol{s}) \oplus \boldsymbol{t}_j$，协议正确性成立.
- 由 $\mathcal{S}$ 提取 $(x_{j,0}, x_{j,1})$ 的方式，P_r 在理想/真实世界输出一致.
- 敌手视角下 $\boldsymbol{Q}$ 在理想/真实世界均为均匀随机矩阵.

P_r 被攻陷时（半诚实），区分优势不超过 $(t+1) \cdot 2^{-k}$：

- 当 $\boldsymbol{s} \neq 0$ 时，理想/真实世界的 $(y_{j,0}, y_{j,1})$ 分布相同.

不可区分性分析

P_s 被攻陷时（恶意），理想世界与真实世界完美不可区分：

- 矩阵 $\boldsymbol{Q}$ 满足 $\boldsymbol{q}_j = (r_j \cdot \boldsymbol{s}) \oplus \boldsymbol{t}_j$，协议正确性成立.
- 由 $\mathcal{S}$ 提取 $(x_{j,0}, x_{j,1})$ 的方式，P_r 在理想/真实世界输出一致.
- 敌手视角下 $\boldsymbol{Q}$ 在理想/真实世界均为均匀随机矩阵.

P_r 被攻陷时（半诚实），区分优势不超过 $(t+1) \cdot 2^{-k}$：

- 当 $\boldsymbol{s} \neq 0$ 时，理想/真实世界的 $(y_{j,0}, y_{j,1})$ 分布相同.
- 坏事件 B：$\boldsymbol{s} = 0$ 或敌手请求 $H(j, \boldsymbol{t}_j \oplus \boldsymbol{s})$.

不可区分性分析

P_s 被攻陷时（恶意），理想世界与真实世界完美不可区分：

- 矩阵 $\boldsymbol{Q}$ 满足 $\boldsymbol{q}_j = (r_j \cdot \boldsymbol{s}) \oplus \boldsymbol{t}_j$，协议正确性成立.
- 由 $\mathcal{S}$ 提取 $(x_{j,0}, x_{j,1})$ 的方式，P_r 在理想/真实世界输出一致.
- 敌手视角下 $\boldsymbol{Q}$ 在理想/真实世界均为均匀随机矩阵.

P_r 被攻陷时（半诚实），区分优势不超过 $(t+1) \cdot 2^{-k}$：

- 当 $\boldsymbol{s} \neq 0$ 时，理想/真实世界的 $(y_{j,0}, y_{j,1})$ 分布相同.
- 坏事件 B：$\boldsymbol{s} = 0$ 或敌手请求 $H(j, \boldsymbol{t}_j \oplus \boldsymbol{s})$.
- 由于 $\boldsymbol{t}_j \oplus \boldsymbol{s}$ 在 2^k 空间均匀，$\Pr[B] \leq (t+1) \cdot 2^{-k}$.

本章总结

本章总结

1. **理论基础**: 不存在信息论安全的两方 OT.

本章总结

1. **理论基础**: 不存在信息论安全的两方 OT.
2. **半诚实协议**: DDH-OT 简单高效，通过“公钥盲化”实现隐私.

本章总结

1. **理论基础**：不存在信息论安全的两方 OT.
2. **半诚实协议**：DDH-OT 简单高效，通过“公钥盲化”实现隐私.
3. **恶意安全**：引入第三方协助防止接收方双密钥.

本章总结

1. **理论基础**: 不存在信息论安全的两方 OT.
2. **半诚实协议**: DDH-OT 简单高效，通过“公钥盲化”实现隐私.
3. **恶意安全**: 引入第三方协助防止接收方双密钥.
4. **协议扩展**: IKNP OT 使用少量“贵的”OT 实现大量“便宜的”OT.

思考题

1. 虽然无法以黑盒的方式利用一般性的公钥加密来构造 OT 协议，我们是否可以利用一些具有特殊性质的公钥加密算法来构造 OT 协议呢？
2. IKNP OT 扩展协议的安全性证明中使用了随机谕示机（Random Oracle）？如果替换为具体的哈希函数，安全性会受到哪些影响？我们需要具有什么特性的哈希函数？
3. OT 协议被证明是安全多方计算的完备原语．请思考一下如何利用 OT 构造一个安全的二方承诺协议.

Q & A