choose 双向不经意传输.当然,增加的这两个字符串被 R 接收到 1 个还是 2 个,依然由 R 的 cut-and-choose 指示比特 j 来决定.需要注意的是,引入选择比特 σ 会带来以下问题:当 j 为 0 时,R 必须知道 x_0 和 x_1 这两个值应该获得哪一个.如果按照正常顺序 x_0,x_1 发送这两个值,则 R 可以获得 σ 的值,这与 σ 需要保密相矛盾.因此,需要引入一个置换比特 b 来对 x_0 和 x_1 的位置进行随机置换,从而达到隐藏 σ 的目的.这样,R 就可以在不知道 σ 的情况下获得 x_σ.置换比特的引入会对接收方的输出造成影响:当 cut-and-choose 指示比特 j 为 1 时,接收方除了获得被置换位置后的两个字符串 x_b,x_{1-b} 之外,还需要拿到 b 的值,以获得正常顺序的 x_0,x_1;当 cut-and-choose 指示比特 j 为 0 时,接收方除了获得由发送方指定应该获得的 x_σ 之外,实际上也获得了 x_σ 的位置信息 $\sigma\oplus b$,即当获得 x_b,x_{1-b} 中的第 1 个时,说明 $\sigma\oplus b$ 为 0,反之则说明 $\sigma\oplus b$ 为 1.该功能可以由下面的功能函数 $\mathcal{F}_{ccbot}$ 给出.

功能函数 $\mathcal{F}_{ccbot}$.

输入:

--S 输入 $(x_0,x_1,y_0,y_1,b,\sigma)$,其中 $x_0,x_1,y_0,y_1\in\{0,1\}^n,b\in\{0,1\}$ 为置换比特,$\sigma\in\{0,1\}$ 为 S 的选择比特.

--R 输入 (j,τ),其中 $j\in\{0,1\}$ 为 cut-and-choose 指示比特,$\tau\in\{0,1\}$ 为 R 的选择比特.

输出:

--S 输出 $\perp$.

--R 输出 z:

当 j=1 时,z 为 $(x_b,x_{1-b},1-b,y_0,y_1)$;

当 j=0 时,z 为 $(x_\sigma,y_\tau,\sigma\oplus b)$,其中 $\sigma\oplus b$ 指示 x_σ 的位置信息.

2.2 协议构造

Cut-and-choose 双向不经意传输可以基于同态加密构造.主要思想是利用加密方案的同态性,将接收方 cut-and-choose 指示比特的密文与发送方的输入进行特定运算.具体构造请见协议 1.

协议 1. Cut-and-Choose 双向不经意传输协议.

输入:发送方 S 输入 $(x_0,x_1,y_0,y_1,b,\sigma)$;接收方 R 输入 (j,τ).

辅助输入:安全参数 1^n;满足定义 1 的选择明文攻击(CPA)安全的加法同态加密方案 $M=(Gen,Enc,Dec)$.

协议过程:

步骤 1. R 将 τ 编码为两个比特 $\tau_0\tau_1$,其中 $\tau_\tau=1,\tau_{1-\tau}=0$.具体来说,如果 $\tau=1$,则编码为 $\tau_0\tau_1=01$;如果 $\tau=0$,则编码为 $\tau_0\tau_1=10$.另外,R 将 j 编码为两个比特 $j_0j_1=j0$.然后,R 生成一组密钥 $(pk,sk)\leftarrow Gen(1^n)$,公开公钥 pk,并用 pk 对 $(j_0,j_{\tau_0}+\tau_0,j_{\tau_1}+\tau_1)$ 进行加密,将加密后得到的密文三元组 $(Enc_{pk}(j_0),Enc_{pk}(j_{\tau_0}+\tau_0),Enc_{pk}(j_{\tau_1}+\tau_1))$ 发送给 S.

步骤 2. S 将 σ 编码为两个比特 $\sigma_0\sigma_1$,其中 $\sigma_\sigma=1,\sigma_{1-\sigma}=0$.具体来说,如果 $\sigma=1$,则编码为 $\sigma_0\sigma_1=01$;如果 $\sigma=0$,则编码为 $\sigma_0\sigma_1=10$.然后,S 利用 R 的公钥 pk 计算 $(Enc_{pk}(j_1),Enc_{pk}(\sigma_0),Enc_{pk}(\sigma_1),Enc_{pk}(b))$,并计算密文五元组:

$$w_b=(Enc_{pk}(j_{\sigma_b})\cdot Enc_{pk}(\sigma_b))^{x_b},$$

$$w_{1-b}=(Enc_{pk}(j_{\sigma_{1-b}})\cdot Enc_{pk}(\sigma_{1-b}))^{x_{1-b}},$$

$$w_2=(Enc_{pk}(j_b)\cdot Enc_{pk}(b))^{1-b},$$

$$w_3=(Enc_{pk}(j_{\tau_0}+\tau_0))^{y_0},$$

$$w_4=(Enc_{pk}(j_{\tau_1}+\tau_1))^{y_1}.$$

计算完成后,将密文五元组 $(w_b,w_{1-b},w_2,w_3,w_4)$ 发送给 R.

步骤 3. R 用私钥 sk 对接收到的密文五元组进行解密,得到明文五元组 $(u_b,u_{1-b},u_2,u_3,u_4)$:

- 当 j=1 时,令 $(u_b,u_{1-b},u_2,u_3,u_4)=(x_b,x_{1-b},1-b,y_0,y_1)$;
- 当 j=0 时,忽略 u_2 的值,令 u_b,u_{1-b} 中不为 0 的值为 x_σ,即 u_b,u_{1-b} 中的第 $\sigma\oplus b$+1 个;令 u_3,u_4 中的第 τ+1 个为 y_τ,得到输出 $(x_\sigma,y_\tau,\sigma\oplus b)$.