CipherMamba

1 正确性说明

正确性从算法中可看出是显见的。

2 安全性说明

2.1 安全性定义

首先介绍一个密码学常用概念：

定义（多项式时间不可区分）：设 $\chi_0(n), \chi_1(n)$ 是两族以 n 为规模的概率分布。对多项式时间随机（*Probabilistic Polynomial-Time,* PPT）算法 $\mathcal{A}$，我们作如下试验：

1. 首先，$b \leftarrow \{0,1\}$ 背着 $\mathcal{A}$ 均匀采样；
2. 接着，$x \leftarrow \chi_b(n)$ 背着 $\mathcal{A}$ 取样；
3. 然后，将 x 交付 $\mathcal{A}$，让 $\mathcal{A}$ 输出 $b' \in \{0,1\}$
4. 如果 $b = b'$，输出 1，否则输出 0。

记试验为 $E_{\mathcal{A}}^{\chi_0,\chi_1}(n)$，$\mathsf{output}\big(E_{\mathcal{A}}^{\chi_0,\chi_1}(n)\big)$ 是其输出。称他们是**多项式时间不可区分**（简称，不可区分）的，如果对足够大的 n 以及每个 PPT$-$ 算法 $\mathcal{A}$，都有：

$$P\left[\mathsf{output}\big(E_{\mathcal{A}}^{\chi_0,\chi_1}(n)\big) = 1\right] \leq \frac{1}{2} + \mathsf{negl}(n)$$

我们采用 2-PC 模型下的半诚实场景下安全性定义。

定义（相应于半诚实行为的安全性）[1]：设 $f : (x,y) \mapsto \big(f_0(x,y), f_1(x,y)\big)$ 是确定型可计算函数，π 是一个用来计算 f 的 *2-PC* 协议。记安全参数为 n。定义：

- 第 $j \in \{0,1\}$ 方在输入为 (x,y)、执行协议 π 时的 $\mathsf{view}_j^{\pi}(x,y,n)$ 指如下资料

$$\big(w_j, r_j, m_j^{(1)}, \cdots, m_j^{(t)}\big)$$

其中 $w_0 = x, w_1 = y, r_j$ 是第 j 方的随机纸带，$m_j^{(k)}$ 是第 j 方收到的第 k 份消息；

- 第 $j \in \{0,1\}$ 方在输入为 (x,y)、执行协议 π 时的 $\mathsf{output}_j^\pi(x,y,n)$ 指该方运行协议得到的输出。这个输出应该只依赖于 $\mathsf{view}_j^\pi(x,y,n)$。

如果存在 PPT$-$ 算法 S_0, S_1，使得：

$$\left\{S_0\big(x, f_0(x,y)\big)\right\}_{x,y\in\{0,1\}^n} \text{ 与 } \left\{\mathsf{view}_0^\pi(x,y)\right\}_{x,y\in\{0,1\}^n} \text{ 不可区分}$$

$$\left\{S_1\big(x, f_1(x,y)\big)\right\}_{x,y\in\{0,1\}^n} \text{ 与 } \left\{\mathsf{view}_1^\pi(x,y)\right\}_{x,y\in\{0,1\}^n} \text{ 不可区分}$$

（其中 x,y 取自任意分布）就称 π **相应于半诚实攻击者是安全**的。进一步，如果：

$$\left\{\mathsf{output}_j^\pi(x,y)\right\}_{x,y\in\{0,1\}^n} \text{ 与 } \left\{f(x,y)\right\}_{x,y\in\{0,1\}^n} \text{ 不可区分}$$

就称 π **相应于半诚实攻击者可以安全地计算** f。

这个定义侧重的是：一方手上的输入和输出构成其全部信息来源，在运算过程中收到的所有信息都不真正蕴含有效的信息量。其中，算法 S_0, S_1 被称为 simulator。构建适当的 simulator 就能够证明一个 2-PC 协议的安全性。

2.2 串行模块化复合

一个复杂的 2-PC 可以分解为多步 2-PC 的复合。**串行模块化复合 (Sequential Modular Composition Theorem)** 定理 [2] 给出了一个很好的结果：如果一个 2-PC 协议的运行是靠“安全地”把一些本身安全的 2-PC 协议组合起来，那么它本身也是安全的。这样，验证一个多步骤 2-PC 协议大部分工作就是验证每个子模块的安全性。

定理（SMCT, 2-PC & semi-honest case）：设 π 是一个 *2-PC* 协议。其过程是：

$$\begin{pmatrix} x \\ y \end{pmatrix} \overset{\mathsf{F}_1}{\mapsto} \begin{pmatrix} f_{1,1}(x,y) \triangleq x_1 \\ f_{1,2}(x,y) \triangleq y_1 \end{pmatrix} \overset{\mathsf{F}_2}{\mapsto} \cdots \overset{\mathsf{F}_n}{\mapsto} \begin{pmatrix} f_{n,1}(x_{n-1}, y_{n-1}) \\ f_{n,2}(x_{n-1}, y_{n-1}) \end{pmatrix} = \begin{pmatrix} x_n \\ y_n \end{pmatrix}$$

其中 F_j 是指，双方都将输入发送给一个“可信的第三方”，该“可信的第三方”会准确地（$< \mathsf{negl}(n)$ 的犯错概率）计算出结果，并仅把输出发送还给双方。设 π 相应于半诚实攻击者可以安全地计算 $f_n \circ \cdots \circ f_1$，其中 $f_j : (x_{j-1}, y_{j-1}) \mapsto \big(f_{j,1}(x_{j-1}, y_{j-1}), f_{j,2}(x_{j-1}, y_{j-1})\big)$。

另外，假设 *2-PC* 协议 ρ_j 相应于半诚实攻击者可以安全地计算 f_j，用 $\pi^{\rho_1,\cdots,\rho_n}$ 表示将协议中 F_j 的计算替换为 ρ_j 的调用后所得新的 *2-PC* 协议，那么 $\pi^{\rho_1,\cdots,\rho_n}$ 仍然可以相应于半诚实攻击者安全地计算 $f_n \circ \cdots \circ f_1$。

有时也将 F_j 称为理想函数（ideal functionality）。

2.3 CipherMamba 安全性证明

参考文献

[1] *Efficient Secure Two-Party Protocols*, Carmit Hazay, Yehuda Lindell, Springer-Verlag Berlin Heidelberg 2010. https://doi.org/10.1007/978-3-642-14303-8

[2] Canetti, R. *Security and Composition of Multiparty Cryptographic Protocols*. J. Cryptology 13, 143–202 (2000). https://doi.org/10.1007/s001459910006