

代理重加密 (Proxy Re-Encryption)

Sammy Li

2020-11-18

目录

| | |
|-----------------------------|----------|
| 1 符号定义 | 1 |
| 2 流程 | 1 |
| 2.1 A 和 B 本地生成密钥 | 2 |
| 2.2 A 加密消息并上传到 S | 2 |
| 2.3 A 基于 B 的公钥生成重加密密钥并上传到 S | 2 |
| 2.4 S 加工生成重加密消息 | 2 |
| 2.5 B 执行重解密还原消息 | 2 |
| 3 证明 | 2 |
| 3.1 预备知识 | 2 |
| 3.1.1 双线性映射 | 2 |
| 3.2 解密过程正确性推导 | 3 |
| 参考文献 | 3 |

1 符号定义

表 1: 符号定义

| 符号 | 说明 |
|--|---|
| $\mathbb{G} = \langle G \rangle$ | 椭圆曲线群, 生成元记为 G |
| $e: \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ | 椭圆曲线群 $\mathbb{G}_1 = \langle G_1 \rangle$ 和 $\mathbb{G}_2 = \langle G_2 \rangle$ 到 $\mathbb{G}_T = \langle G_T \rangle$ 的双线性映射 |
| $s \in_R S$ | 表示从集合 S 随机选取一个元素 s |
| p | 群 \mathbb{G}_1 和 \mathbb{G}_2 的阶, 即元素个数 |

往后部分使用的具体椭圆曲线群为 bn256 [1,2]。

2 流程

流程涉及角色如下

- 发送方 A: 负责本地加密消息, 然后上传到代理服务器, 为接收方分配重加密的解密密钥
- 代理服务器 S: 存储 A 的密文, 基于 A 的重加密密钥执行重加密
- 接收方 B: 基于重加密密钥解密密文

2.1 A 和 B 本地生成密钥

- A 本地基于 \mathbb{G}_1 生成公私钥对 $(x_A, X_A = x_A \cdot G_1)$
- B 本地基于 \mathbb{G}_2 生成公私钥对 $(x_B, X_B = x_B \cdot G_2)$

2.2 A 加密消息并上传到 S

1. 将 m 映射为 \mathbb{G}_T 的元素 M
 - 通常情况下, m 用作加密数据的对称密钥, 可先随机生成 M 然后转化为 m , 再用 m 对数据进行对称加密
2. 随机生成 $r \in_R \mathbb{Z}_p$
3. 计算密文分片
 - $C_1 = r \cdot G_T + M \in \mathbb{G}_T$
 - $C_2 = r \cdot X_A \in \mathbb{G}_1$
4. 将 (C_1, C_2) 上传到 S

2.3 A 基于 B 的公钥生成重加密密钥并上传到 S

1. A 计算重加密密钥 $X' = x_A'^{-1} \cdot X_B \in \mathbb{G}_2$
2. 将 X' 上传到 S

2.4 S 加工生成重加密消息

S 计算并保存 $C'_2 = e(X', C_2)$

2.5 B 执行重解密还原消息

1. B 从 S 下载 (C_1, C'_2)
2. 计算 $R = x_B'^{-1} \cdot C'_2$
3. 计算 $M' = C_1 - R$
4. 将 M' 转化为 m' , 即得消息原文 $m = m'$

3 证明

3.1 预备知识

3.1.1 双线性映射

设 \mathbb{G}_1 、 \mathbb{G}_2 和 \mathbb{G}_T 都是阶为 p 的循环群, p 是素数。如果映射 $e: \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ 满足以下性质:

1. **双线性性**: 对于任意 $a, b \in \mathbb{Z}_p$ 和 $X \in \mathbb{G}_1, Y \in \mathbb{G}_2$, 有 $e(a \cdot X, b \cdot Y) = a \cdot b \cdot e(X, Y)$
2. **非退化性**: 存在 $X \in \mathbb{G}_1, Y \in \mathbb{G}_2$, 使得 $e(X, Y) \neq G_T$ 。这里 G_T 代表 \mathbb{G}_T 群的单位元
3. **可计算性**: 存在有效的算法对任意的 $X \in \mathbb{G}_1, Y \in \mathbb{G}_2$, 计算 $e(X, Y)$ 的值

那么称 e 是一个双线性映射。

双线性映射可以通过有域上的超椭圆曲线上的 Tate 对或 Weil 对来构造。

注: $e(X, Y) = e(Y, X)$ 。

3.2 解密过程正确性推导

$$\begin{aligned} M' &= C_1 - R \\ &= r \cdot G_T + M - x_B'^{-1} \cdot C_2' \\ &= r \cdot G_T + M - x_B'^{-1} \cdot e(X', C_2) \\ &= r \cdot G_T + M - x_B'^{-1} \cdot e(x_A'^{-1} \cdot X_B, C_2) \\ &= r \cdot G_T + M - x_B'^{-1} \cdot e(x_A'^{-1} \cdot X_B, r \cdot X_A) \\ &= r \cdot G_T + M - x_B'^{-1} \cdot e(x_A'^{-1} \cdot x_B \cdot G_2, r \cdot x_A \cdot G_1) \\ &= r \cdot G_T + M - e(x_B'^{-1} \cdot x_B \cdot G_2, x_A'^{-1} \cdot r \cdot x_A \cdot G_1) \\ &= r \cdot G_T + M - e(G_2, r \cdot G_1) \\ &= r \cdot G_T + M - r \cdot e(G_2, G_1) \\ &= r \cdot G_T + M - r \cdot G_T \\ &= M \end{aligned}$$

参考文献

- [1] Barreto, Paulo S. L. M. , and M. Naehrig . "Pairing-Friendly Elliptic Curves of Prime Order." (2005).
- [2] Naehrig, Michael , R. Niederhagen , and P. Schwabe . "New Software Speed Records for Cryptographic Pairings." International Conference on Progress in Cryptology-latincrypt Springer-Verlag, 2010.