Reading Notes: Paillier Homomorphic Encryption

July 19, 2023

Paillier 同态加密为公钥加密，基于剩余类困难问题，是一种加法同态加密. 其实现的效果为：对于明文 m_1 和 m_2，$D\left(E\left(m_1\right)\times E\left(m_2\right)\right)=m_1+m_2$. 在加解密过程中使用到 Carmichael 函数和定理，以及剩余类相关知识.

1 预备知识

1.1 Carmichael Function

在数论中，Carmichael 函数定义为使得 $a^m\equiv 1\text{mod n}$ 成立的最小正整数 m, 其中 $(a,n)=1$，将 m 记作 $\lambda(n)$。在抽象代数术语中，$\lambda(n)$ 是模 n 的乘法群的指数。

根据唯一因式分解定理，任何 n>1 的整数都可以用唯一的方式写成

$$n=p_1^{r_1}p_2^{r_2}\ldots p_k^{r_k} \tag{1}$$

其中，$p_1<p_2<\ldots<p_k$ 是由小到大排列的素数，$r_1,r_2,\ldots,r_k$ 是正整数. 那么 $\lambda(n)$ 就是其中每一项的 λ 的最小公倍数，有：

$$\lambda(n)=lcm\left(\lambda\left(p_1^{r_1}\right),\lambda\left(p_2^{r_2}\right),\ldots,\lambda\left(p_k^{r_k}\right)\right) \tag{2}$$

证明过程如下：

首先有对任意与 n 互质的数 a, 其必然也与 p_i 互质，有

$$a^{\lambda\left(p_1^{r_1}\right)}\equiv 1modp_1^{r_1} \tag{3}$$

又因为

$$a^{\lambda(n)}\equiv 1modn \tag{4}$$

于是有

$$a^{\lambda(n)}\equiv 1modp_1^{r_1} \tag{5}$$

因为 $\lambda\left(p_1^{r_1}\right)$ 的最小性可以得到

$$\lambda\left(p_1^{r_1}\right)|\lambda(n) \tag{6}$$

对于其它 p_i 可以推知上式同样成立，所以 $\lambda(n)$ 为 $\lambda\left(p_i^{r_i}\right)$ 的公倍数.

另一方面，当 $\lambda(n)$ 取值为 $lcm\left(\lambda\left(p_1^{r_1}\right), \lambda\left(p_2^{r_2}\right), \ldots, \lambda\left(p_k^{r_k}\right)\right)$ 时，有

$$a^{\lambda(n)} \equiv 1 mod p_i^{r_i} \tag{7}$$

注意到 $p_i^{r_i}$ 两两互质，于是可以得到

$$a^{\lambda(n)} \equiv 1 mod \prod_{i=1}^{k} p_i^{r_i} \tag{8}$$

即为

$$a^{\lambda(n)} \equiv 1 mod n \tag{9}$$

因此式 (2) 得到证明，这也是 Carmichael 函数的计算方式. 在本协议中，我们只需要知道式 (9) 的性质即可.

2 协议流程

2.1 密钥产生

选取两个大素数 p,q, 计算 $n = p * q$ 和 $\lambda = lcm(p-1, q-1)$，注意这里的 λ 计算方式其实就是上文说到的 Carmichael 函数. 接下来我们随机选取 g, $g \in \mathbb{Z}_{n^2}^*$ 且满足 $\mu = \left(L\left(g^{\lambda} mod n^2\right)\right)^{-1}$ 存在，其中函数 $L(x)$ 定义为 $L(x) = \frac{x-1}{n}$, 此时公钥为 (n, g), 私钥为 (λ, μ).

2.2 加密过程

对于明文 m,$m \in \mathbb{Z}_n$, 选择随机数 $r < n$, 加密过程为 $c = g^m r^n (mod n^2)$.

2.3 解密过程

对于密文 c 的解密过程为

$$\begin{aligned} m &= L(c^{\lambda} mod n^2) * \mu mod n & (10) \\ &= \frac{L(c^{\lambda} mod n^2)}{L(g^{\lambda} mod n^2)} & (11) \end{aligned}$$

在上式中，$c^{\lambda} = g^{\lambda m} r^{\lambda n}$, 对于任意的 $a \in \mathbb{Z}_n$, 由于上文 Carmichael 函数的性质有 $a^{\lambda(n)} \equiv 1 mod n$, 因此对于 m 和 r，均可以得到

$$g^{\lambda(n)} \equiv 1 mod n \tag{12}$$

$$r^{\lambda(n)} \equiv 1 mod n \tag{13}$$

因而可以设 $g^{\lambda(n)} = 1 + k_1 n$, $r^{\lambda(n)} = 1 + k_2 n$, 在模 n^2 意义下有:

$$r^{\lambda n} = (1 + k_2 n)^n \equiv 1 + k_2 n * n \equiv 1 (mod n^2) \tag{14}$$

$$g^{\lambda m} = (1 + k_1 n)^m \equiv 1 + k_1 n * m (mod n^2) \tag{15}$$

那么

$$\frac{L(c^{\lambda} mod n^2)}{L(g^{\lambda} mod n^2)} = \frac{\frac{1*(1+k_1 mn)-1}{n}}{\frac{(1+k_1 n)-1}{n}} \tag{16}$$

$$= \frac{k_1 m}{k_1} \tag{17}$$

$$= m \tag{18}$$

数学推导证明如上.