第三次作业

Log Creative

2023 年 10 月 12 日

1. **解** 在挑战阶段，已经得到 m_b^*（b 从 $\{0,1\}$ 中随机选取）的密文 c^*。在 El Gammal 加密中，该密文具有这种形式：$c^* = (c_1^*, c_2^*)$。在检测阶段，不允许直接对 c^* 进行解密。为了能够得到 m_b^*，将要求对新构造的 $c = (c_1^*, c_1^* \cdot c_2^*)$ 进行解密，得到 m 后，就可以得到 $m_b^* = (c_1^*)^{-1} \cdot m$，此时与 m_0 与 m_1 进行对比就可以确定 b，概率会显著大于 $1/2$，也就意味着 El Gammal 加密不是 CCA 安全的。

   证明如下：根据 El Gammal 加密的定义，对于公钥 $pk = (G, q, g, h)$，私钥 $sk = (x)$，其中 $h = g^x$，对于消息 $m_b \in G$ 有密文 $c^* = (c_1^*, c_2^*) = (g^y, m_b \cdot h^y)$。根据群的封闭性，$c_1^* \in G, c_2^* \in G, c_1^* \cdot c_2^* \in G$，故构造的密文 $c = (c_1^*, c_1^* \cdot c_2^*) \in G^2$ 合法。解密时，有

$$m = c_1^* \cdot c_2^* \cdot (c_1^{*x})^{-1} = c_1^* \cdot m_b \cdot h^y \cdot (g^{xy})^{-1} = c_1^* \cdot m_b \cdot h^y \cdot (h^y)^{-1} = c_1^* \cdot m_b$$

   则等式两边与 $(c_1^*)^{-1}$ 进行左侧二元运算，有

$$(c_1^*)^{-1} \cdot m = (c_1^*)^{-1} \cdot c_1^* \cdot m_b = m_b$$

   可以认为 $(c_1^*)^{-1} = (c_1^*)^{q-1}$ 是可求的，证毕。

2. **证明** (a) 一个散列函数是碰撞抵抗的 $\Rightarrow$ 目标碰撞抵抗的：所有的多项式算法中，已知碰撞抵抗，即对于 $\forall (x, x') \in \{0,1\}^{*2}$ 且 $x \neq x'$，此处认为序列对 (x, x') 是有序的输出，即 $(x, x') \neq (x', x)$，都有

$$P\left(H(x) = H(x')\right) \leq \text{negl}(n) \tag{1}$$

   记 $P(H(x_i) = H(x'))$ 为固定一个定义域中的 $x_i \in \{0,1\}^*$，选取 $x' \in \{0,1\}^*$ 且 $x' \neq x_i$ 使得散列结果相同的概率，有下面的关系

$$P\left(H(x) = H(x')\right) = \sum_i P(H(x_i) = H(x')) \tag{2}$$

   结合式 (1) 和式 (2)，以及概率的定义 $0 \leq P \leq 1$，有

$$P(H(x_i) = H(x')) \leq \text{negl}(n) \tag{3}$$

   也就是它也是目标碰撞抵抗的。

   (b) 一个散列函数是目标碰撞抵抗的 $\Rightarrow$ 原像抵抗的：反证法。假设所有的多项式算法中，对于固定的原像 $y \in \{0,1\}^{l(n)}$，找到 $x \in \{0,1\}^*$ 使得 $H(x) = y$ 的概率不再是可忽略的，即

$$P(H(x) = y) > \text{negl}(n) \tag{4}$$

由于值域空间是小于定义域空间的，$|\{0,1\}^{l(n)}| < |\{0,1\}^*|$，实际上后者是一个无穷大的空间，所以对于一个原像 y，存在定义域中的另一个解 $x' \in \{0,1\}^*$ 且 $x' \neq x$，使得 $y = H(x')$。就原像抵抗的试验而言，x 和 x' 的地位是等价的、不可区分的，所以记

$$p = P(H(x') = y) = P(H(x) = y) > \mathrm{negl}(n) \tag{5}$$

现在做两次原像抵抗试验，假设第一次试验成功得到 x 使得 $H(x) = y$；第二次试验也成功，得到 x' 使得 $H(x') = y$，有两种情形：

i. $x' = x$，第二次与第一次取到的值相同；
ii. $x' \neq x$，第二次与第一次取到的值不相同。

显然

$$P(x' = x) + P(x' \neq x) = 1 \tag{6}$$

以目标碰撞抵抗的视角而言，可以视作第一次试验得到的 x 是固定的，即在 $H(x) = y$ 的条件下，第二次试验成功的概率被分解为

$$P(H(x') = y) = P(x' = x)P\left(H(x') = y | x' = x\right) + P(x' \neq x)P\left(H(x') = y | x' \neq x\right) \tag{7}$$

注意到因为定义域空间 $|\{0,1\}^*|$ 是无穷大的，第二次取值直接为第一次取值的概率极限为 0，结合式 (6) 有

$$\begin{aligned} &P(x' = x) = 0 \\ &P(x' \neq x) = 1 - P(x' = x) = 1 \end{aligned}$$

那么式 (7) 就变为

$$P(H(x') = y) = P(H(x') = y | x' \neq x) \tag{8}$$

结合式 (5) 有

$$P(H(x') = y | x' \neq x) = p > \mathrm{negl}(n) \tag{9}$$

式 (9) 左边正是在 $x' \neq x$ 的条件下，目标碰撞抵抗 $H(x') = y$ 成功的概率，该式表明这个概率是不可忽略的。这与目标碰撞抵抗成功的概率可忽略的前提是矛盾的。 ■