现代密码学第二次作业

2050249 徐正扬

2024 年 6 月 23 日

2.3

1. 证明仿射密码具有完善保密性，如果每个密钥的概率都是 $\frac{1}{312}$。
2. 更一般地，假设在下面的集合上给定一个概率分布

$$\{a \in \mathbb{Z}_{26} \mid \gcd(a, 26) = 1\}$$

假设仿射密码的每个密钥 (a, b) 的概率是 $\frac{\Pr[a]}{26}$。证明当这个概率分布定义在密钥空间上时，仿射密码具有完善保密性。

- 我们先证明第二问。

首先证明 $\forall a, b \in \mathbb{Z}_{26}, \gcd(a, 26) = 1$，我们都有 $a^{-1}(y - b)$ 构成一个模 26 的完全剩余系。

反证法，假设对于一对 (a, b)，有不同的 $y_0, y_1 \in \mathbb{Z}_{26}$ 满足 $a^{-1}(y_0 - b) \equiv a^{-1}(y_1 - b) \mod 26$，
那么 $a^{-1}(y_0 - y_1) \equiv 0 \mod 26$，而 $\gcd(a, 26) = 1$，也即 $\gcd(a^{-1}, 26) = 1$，
则 $y_0 - y_1 \equiv 0 \mod 26$，即 $y_0 = y_1$，矛盾。

因此，$\forall a, b, \gcd(a, 26) = 1$，我们都有 $d(y)$ 是一个 $\mathbb{Z}_{26}$ 的一个置换。
同理，$e(x)$ 也是一个 $\mathbb{Z}_{26}$ 的一个置换。

接下来证明 $\forall x \in \mathcal{P}, y \in \mathcal{C}$，都有 $\Pr[x \mid y] = \Pr[x]$。

首先，对于给定的 y，$d(y)$ 是一个 $\mathbb{Z}_{26}$ 的一个置换，那么

$$\Pr[\mathbf{x} = d(y)] = \Pr[\mathbf{x} = x] = \frac{1}{26}$$

因此

$$\begin{aligned}
\Pr[y] &= \sum_{a \in \mathbb{Z}_{26}} \frac{\Pr[a]}{26} \Pr[d(y)] \\
&= \frac{1}{26} \cdot \sum_{a \in \mathbb{Z}_{26}} \frac{\Pr[a]}{26} \\
&= \frac{1}{26}
\end{aligned}$$

其次，对于给定的 x, y, a，存在唯一的 b，使得 $y \equiv ax + b \mod 26$，即

$$\Pr[y \mid x, a] = \frac{1}{26}$$

因此，由全概率公式，

$$\begin{aligned}
\Pr[y \mid x] &= \sum_{a \in \mathbb{Z}_{26}} \Pr[a] \Pr[y \mid x, a] \\
&= \frac{1}{26} \sum_{a \in \mathbb{Z}_{26}} \Pr[a] \\
&= \frac{1}{26}
\end{aligned}$$

因此，由 Bayes 定理，

$$\begin{aligned}\Pr[x \mid y] &= \frac{\Pr[x] \cdot \Pr[y \mid x]}{\Pr[y]} \\ &= \frac{\Pr[x] \cdot \dfrac{1}{26}}{\dfrac{1}{26}} \\ &= \Pr[x]\end{aligned}$$

证毕。 $\square$

- 再证明第一小问。

  由于 $\phi(26) = 26(1 - \frac{1}{2})(1 - \frac{1}{13}) = 12$，因此只要等概率分别取 a, b （由于 $\frac{1}{12} \cdot \frac{1}{13} = \frac{1}{312}$），同上得证。 $\square$