Foundation of Cryptography Homework 1

周书予
2000013060@stu.pku.edu.cn

September 13, 2022

Problem 1

For any fixed probability distribution over $\mathcal{M}$, arbitrary message $m \in \mathcal{M}$ and ciphertext $c \in \mathcal{C}$, we have

$$\begin{aligned}\Pr[C = c | M = m] &= \Pr[K \cdot M = c | M = m] = \Pr[K \cdot m = c] \\ &= \Pr\left[K = c \cdot m^{-1}\right] = 1/|\mathcal{G}|\end{aligned}$$

Thus, by using Bayes' Theorem we obtain

$$\begin{aligned}\Pr[M = m_0 | C = c] &= \frac{\Pr[C = c \wedge M = m_0]}{\Pr[C = c]} \\ &= \frac{\Pr[C = c | M = m_0]}{\sum_{m \in \mathcal{M}} \Pr[C = c | M = m] \Pr[M = m]} \Pr[M = m_0] \\ &= \frac{1/|\mathcal{G}|}{\sum_{m \in \mathcal{M}} \Pr[M = m] / |\mathcal{G}|} \Pr[M = m_0] \\ &= \Pr[M = m_0]\end{aligned}$$

as required by the definition of perfect secrecy.

Problem 2

perfect secrecy implies perfect indistinguishability

For any $m_0, m_1 \in \mathcal{M}$, consider a probability distribution over $\mathcal{M}$ with non zero probability on both m_0 and m_1. According to perfect secrecy, for all $c \in \mathcal{C}$, we have

$$\begin{aligned}\Pr[\mathsf{Enc}(K, m_0) = c] &= \Pr[C = c | M = m_0] = \frac{\Pr[M = m_0 | C = c]}{\Pr[M = m_0]} \Pr[C = c] \\ &= \Pr[C = c] = \frac{\Pr[M = m_1 | C = c]}{\Pr[M = m_1]} \Pr[C = c] = \Pr[C = c | M = m_1] = \Pr[\mathsf{Enc}(K, m_1) = c]\end{aligned}$$

perfect indistinguishability implies perfect secrecy

Perfect indistinguishability shows that for any fixed $c \in \mathcal{C}$, $\Pr[C = c | M = m_0] = \Pr[C = c | M = m_1]$ holds for arbitrary $m_0, m_1 \in \mathcal{M}$. Thus, for any probability distribution over $\mathcal{M}$ and arbitrary $m \in \mathcal{M}, c \in \mathcal{C}$, we have

$$\begin{aligned}\Pr[M = m | C = c] &= \frac{\Pr[C = c | M = m] \Pr[M = m]}{\Pr[C = c]} \\ &= \frac{\Pr[C = c | M = m]}{\sum_{m' \in \mathcal{M}} \Pr[C = c | M = m'] \Pr[M = m']} \Pr[M = m] \\ &= \Pr[M = m]\end{aligned}$$

Problem 3

Part C

FSOC we assume $H[K] < \log(|\mathcal{M}|)$. Take the uniform distribution over $\mathcal{M}$ and consider a fixed ciphertext c, according to perfect correctness, we know that $\mathsf{Dec}(k, c) = m$ and Dec is deterministic.

Regard message M, ciphertext C and key K as random variables, we have

$$H[M|C] = H[\mathsf{Dec}(K, C)|C] \leqslant H[K] < \log(|\mathcal{M}|) = H[M]$$

which means that there must be some $m \in \mathcal{M}$ violating the secrecy constraint $\Pr[M = m|C = c] = \Pr[M = m]$, so this scheme is not perfectly secret.

Problem 4

Part A

$|\mathcal{K}| \geqslant |\mathcal{M}|$.

FSOC we assume $|\mathcal{K}| < |\mathcal{M}|$. For a fixed ciphertext $c_0 \in \mathcal{C}$, there must be some message $m_0 \in \mathcal{M}$ which cannot be decrypted from c_0, i.e. for all $k \in \mathcal{K}$, $\mathsf{Dec}(k, c_0) \neq m_0$ (perfect correctness requires Dec to be deterministic). For every probability distribution M over $\mathcal{M}$, we have

$$|\Pr[M = m_0|C = c_0] - \Pr[M = m_0]| = |0 - \Pr[M = m_0]| = \Pr[M = m_0]$$

since M is arbitrary, $\Pr[M = m_0]$ can be arbitrarily large, so the relaxed secrecy requirement cannot be achieved for any fixed $\varepsilon < 1$.

Part B

$|\mathcal{K}| \geqslant (1 - \varepsilon)|\mathcal{M}|$, with the assumption that Enc and Dec are both deterministic.

The relaxed correctness requirement requires the total error rate to be

$$\sum_{m\in\mathcal{M}} \sum_{k\in\mathcal{K}} \Pr[\mathsf{Gen} \to k] \Pr[\mathsf{Dec}(k, \mathsf{Enc}(k, m)) \neq m] \leqslant \varepsilon|\mathcal{M}|$$

by swapping two Σs on the left side of the above inequation we obtain

$$\varepsilon|\mathcal{M}| \geqslant \sum_{k\in\mathcal{K}} \Pr[\mathsf{Gen} \to k] \sum_{m\in\mathcal{M}} \Pr[\mathsf{Dec}(k, \mathsf{Enc}(k, m)) \neq m]$$

Notice that for a fixed k, we have $\sum\limits_{m\in\mathcal{M}} \Pr[\mathsf{Dec}(k, \mathsf{Enc}(k, m)) \neq m] \geqslant |\mathcal{M}| - |\mathcal{C}|$, and $|\mathcal{K}| \geqslant |\mathcal{C}|$ is guaranteed when perfect secrecy condition holds. So eventually we get

$$\varepsilon|\mathcal{M}| \geqslant |\mathcal{M}| - |\mathcal{K}| \Rightarrow |\mathcal{K}| \geqslant (1 - \varepsilon)|\mathcal{M}|$$