CS 171: Discussion 2 (Jan 29)

1. Equivalence of Definitions

You are given an encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M}$ that satisfies the condition

$$\Pr[M = m | C = c] = \Pr[M = m]$$

for every probability distribution M over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ such that $\Pr[C = c] > 0$. Show that for any two messages $m, m' \in \mathcal{M}$ and for any $c \in \mathcal{C}$,

$$\Pr[\mathsf{Enc}(K, m) = c] = \Pr[\mathsf{Enc}(K, m') = c]$$

Solution Fix any two messages $m, m' \in \mathcal{M}$ and $c \in \mathcal{C}$. Define $\mathcal{M}$ to be the uniform distribution over the set $\{m, m'\}$. Then, from the premise, $\Pr[M = m|C = c] = \Pr[M = m] = 1/2 = \Pr[M = m'|C = c]$.

Now,

$$\begin{aligned} 1/2 = \Pr[M = m|C = c] &= \frac{\Pr[C = c|M = m]\Pr[M = m]}{\Pr[C = c]} \\ &= \frac{\Pr[\mathsf{Enc}(K, m) = c](1/2)}{\Pr[C = c]} \end{aligned}$$

Hence, $\Pr[\mathsf{Enc}(K, m) = c] = \Pr[C = c]$. By an exact similar argument, we can show that $\Pr[\mathsf{Enc}(K, m') = c] = \Pr[C = c]$. Thus, $\Pr[\mathsf{Enc}(K, m) = c] = \Pr[\mathsf{Enc}(K, m') = c]$. ■

2. A Different One-time Pad

Consider the following encryption scheme for the message space $\{0, 1\}$.

- Gen: Choose two random bits $a, b \xleftarrow{\$} \{0, 1\}$.
- $\mathsf{Enc}((a, b), m)$: Choose random $x_1 \xleftarrow{\$} \{0, 1\}$ and compute x_2 such that $a \cdot x_1 + b + x_2 = m$ where $+$ and $\cdot$ are operations over $\mathsf{GF}(2)$.
- $\mathsf{Dec}((a, b), (x_1, x_2))$: Compute $m = a \cdot x_1 + b + x_2$.

Show that this scheme is perfectly secure. *Hint: Use the second (equivalent) definition of perfect secrecy from Q1.*

Solution Fix any two messages $m, m' \in \{0, 1\}$ and a ciphertext $(x_1, x_2) \in \{0, 1\} \times \{0, 1\}$. We will show that

$$\Pr[\mathsf{Enc}(K, m) = c] = \Pr[\mathsf{Enc}(K, m') = c]$$

Let (A, B, X_1) be the uniform random variables over $\{0,1\} \times \{0,1\}$. The random variable denoting the key K is given by (A, B) and the first component of the ciphertext is X_1.

$$\begin{aligned}
\Pr[\mathsf{Enc}(K,m) = c] &= \Pr_{K,X_1}(\mathsf{Enc}(K,m) = c) \\
&= \Pr_{A,B,X_1}(AX_1 + B + x_2 = m \wedge X_1 = x_1) \\
&= (1/2)\Pr_{A,B}(Ax_1 + B = m - x_2) \\
&= (1/2)\sum_{a\in\{0,1\}} \Pr_B[ax_1 + B = m - x_2 | A = a] \Pr_A[A = a] \\
&= (1/2)\sum_{a\in\{0,1\}} \Pr_B[B = m - x_2 - ax_1 | A = a](1/2) \\
&= (1/2)(1/2) = 1/4
\end{aligned}$$

By a similar argument, we can show that $\Pr[\mathsf{Enc}(K, m') = c] = 1/4$. ■

3. Non-Negligible Function

A function $f : \mathbb{Z}^+ \to [0,1]$ is a *negligible function* if $\forall$ polynomials $p(\cdot)$, $\exists N \in \mathbb{Z}^+$ such that $\forall n > N$ we have $f(n) < \frac{1}{p(n)}$.
Define a non-negligible function using the negation of the definition of a negligible function. See `https://en.wikipedia.org/wiki/Universal_quantification`.

Solution A function $f : \mathbb{Z}^+ \to [0,1]$ is a *non-negligible function* if $\exists$ polynomials $p(\cdot)$ such that $\forall N \in \mathbb{Z}^+$, $\exists n > N$ such that we have $f(n) \geq \frac{1}{p(n)}$. ■