EE 720: Introduction to Number Theory and Cryptography (Autumn 2023)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Quiz 1: 20 points | Date: September 1, 2023

---

1. [5 points] If (Gen, Enc, Dec) is a perfectly secret encryption scheme with message space $\mathcal{M}$ and key space $\mathcal{K}$, then prove that $|\mathcal{K}| \geq |\mathcal{M}|$.

2. [5 points] Alice has a length-preserving pseudorandom function $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$. She wants to encrypt messages of length $2n$. Let $m \in \{0,1\}^{2n}$ denote the message. Let $m_1 \in \{0,1\}^n$ denote the first $n$ bits of $m$ and let $m_2 \in \{0,1\}^n$ denote the last $n$ bits of $m$. Alice uses the encryption scheme $\Pi = (\texttt{Gen}, \texttt{Enc}, \texttt{Dec})$ where:

   - `Gen`: Key $k$ is chosen uniformly from $\{0,1\}^n$.
   - `Enc`: The message space $\mathcal{M} = \{0,1\}^{2n}$. A string $r$ is chosen uniformly from $\{0,1\}^{n-1}$ and the ciphertext $c \in \{0,1\}^{3n-1}$ corresponding to $m = (m_1, m_2) \in \{0,1\}^{2n}$ is given by

     $$c := \langle r, m_1 \oplus F_k(r\|0), m_2 \oplus F_k(1\|r) \rangle.$$

     Here $\|$ is the string concatenation operator.
   - `Dec`: Given key $k$ and ciphertext $c = \langle r, c_1, c_2 \rangle \in \{0,1\}^{3n-1}$, the message $m = (m_1, m_2)$ is decrypted using $m_1 = c_1 \oplus F_k(r\|0)$ and $m_2 = c_2 \oplus F_k(1\|r)$.

   Prove that Alice's scheme is ~~not~~ **CPA-secure**.

3. [10 points] Let $F$ be a length-preserving pseudorandom permutation having key length, input length, and output length all equal to $n$ bits. Suppose a fixed-length private key encryption scheme $\Pi = (\texttt{Gen}, \texttt{Enc}, \texttt{Dec})$ is defined as follows:

   - `Gen`: Key $k$ is chosen uniformly from $\{0,1\}^n$.
   - `Enc`: The message space $\mathcal{M} = \{0,1\}^{n/2}$. A string $r$ is chosen uniformly from $\{0,1\}^{n/2}$ and the ciphertext $c \in \{0,1\}^n$ corresponding to $m \in \{0,1\}^{n/2}$ is given by

     $$c := F_k(r\|m).$$

     Here $\|$ is the string concatenation operator.
   - `Dec`: Given key $k$ and ciphertext $c \in \{0,1\}^n$, the message $m$ is obtained by taking the last $n/2$ bits of $F_k^{-1}(c)$.

   **Prove that $\Pi$ is CPA-secure for messages of length $n/2$.**