EE 720: Introduction to Number Theory and Cryptography (Autumn 2024)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Quiz 1: 20 points Date: September 4, 2024

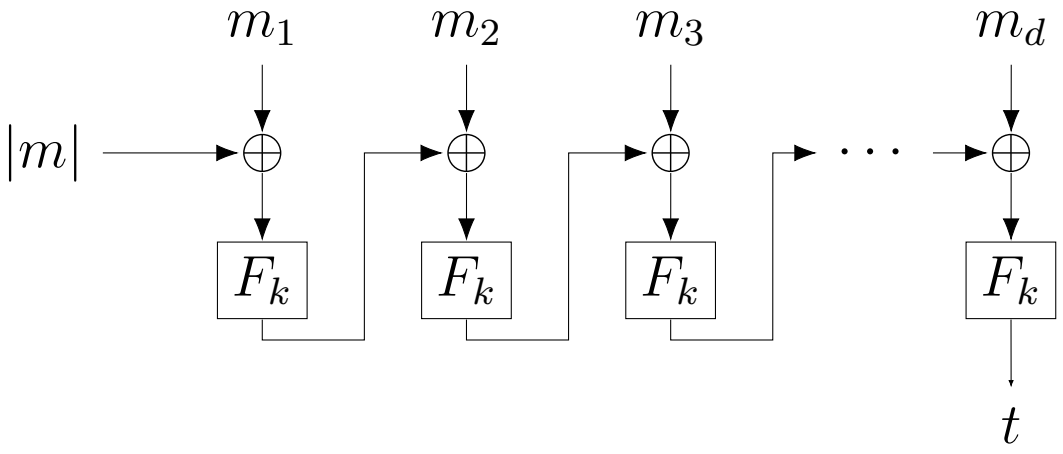
1. [5 points] Let $\Pi = (\texttt{Gen}, \texttt{Enc}, \texttt{Dec})$ be an encryption scheme with message space $\mathcal{M}$ and key space $\mathcal{K}$. Suppose that $\texttt{Enc}$ is a deterministic function of the key $k \in \mathcal{K}$ and message $m \in \mathcal{M}$. Prove that Π is **not CPA-secure**.

2. [10 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:

   - $\texttt{Gen}$: Key k is chosen uniformly from $\{0,1\}^n$.
   - $\texttt{Enc}$: The message space $\mathcal{M} = \{0,1\}^{2n}$. A string r is chosen uniformly from $\{0,1\}^n$ and the ciphertext $c \in \{0,1\}^{3n}$ corresponding to $m = (m_1, m_2) \in \{0,1\}^{2n}$ is given by
   $$c \coloneqq \langle r, m_1 \oplus F_k(r), m_2 \oplus F_k(\neg r) \rangle.$$
   where $\neg r \in \{0,1\}^n$ is the bitwise NOT of r.
   - $\texttt{Dec}$: Given key k and ciphertext $c = \langle r, c_1, c_2 \rangle \in \{0,1\}^{3n}$, the message $m = (m_1, m_2)$ is decrypted using $m_1 = c_1 \oplus F_k(r)$ and $m_2 = c_2 \oplus F_k(\neg r)$.

   Prove that Alice's scheme is **CPA-secure**.

3. [5 points] Consider the modified version of the CBC-MAC for arbitrary-length messages shown in the below figure.



   Let F be a length-preserving pseudorandom function with length n bits. Let $m \in \{0,1\}^{dn}$ be a message where $d > 0$ can vary.

   The tag generation algorithm Mac works as follows::

   1. Parse the message m into d blocks $m_1, \ldots, m_d$ of length n bits each.
   2. Set $t_0 = |m| \in \{0,1\}^n$ where $|m|$ is the length of m in bits. For $i = 1, \ldots, d$, set
   $$t_i = F_k(t_{i-1} \oplus m_i).$$
   3. Output t_d as the tag t.

   The tag verification algorithm Vrfy works as follows: For a message-tag pair (m, t) output 1 if and only if $t = \mathsf{Mac}_k(m)$.

   Prove that this construction is an **insecure** MAC for arbitrary-length messages.