دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری

پاسخنامه تمرین شماره ۴

مدرّس: دکتر شهرام خزائی

- This problem sets include 55 points.
- For any question contact Sara Sarfaraz via sarassm60@gmail.com.

Problem 1

(20 points) Let F be a strong pseudorandom permutation, and define the following fixed-length encryption scheme: On input a message $m \in \{0,1\}^{n/2}$ and key $k \in \{0,1\}^n$, algorithm Enc chooses a uniform $r \in \{0,1\}^{n/2}$ and outputs the ciphertext $c := \mathsf{F}_k(m||r)$. Prove that this scheme is CCA-secure.

Solution We prove the security by contradiction. Assume an adversary $\mathcal{A}$ with non-negligible advantage in CCA-security game. We construct a distinguisher $\mathcal{D}$ to attack F with non-negligible advantage. On any encryption query from $\mathcal{A}$ (like m), the algorithm $\mathcal{D}$ generates a random number r, queries F on $m||r$ and gives the answer to A. On any decryption queries from $\mathcal{A}$ like c, $\mathcal{D}$ queries F^{-1} on c and gives the first half of the output back to $\mathcal{A}$. At the end, on input m_0, m_1 from $\mathcal{A}$, $\mathcal{D}$ chooses a random bit b and returns $\mathsf{F}_k(m_b||r)$ to $\mathcal{A}$. If $\mathcal{A}$ can not guess b correctly, then $\mathcal{D}$ guesses random permutation, otherwise it guesses F_k.
It's clear that the following probabilities are equal:

$$\Pr[\mathcal{D}^{\mathsf{F}_k(.),\mathsf{F}_k^{-1}(.)}(1^n) = 1] = \Pr[\mathsf{PrivK}_{\mathcal{A}}^{\mathsf{CCA}} = 1]$$

so we have:

$$\begin{aligned}\mathsf{Adv}(\mathcal{D}) &= \Pr[\mathcal{D}^{\mathsf{F}_k(.),\mathsf{F}_k^{-1}(.)}(1^n) = 1] - \Pr[\mathcal{D}^{f(.),f^{-1}(.)}(1^n) = 1] \\ &= \Pr[\mathcal{D}^{\mathsf{F}_k(.),\mathsf{F}_k^{-1}(.)}(1^n) = 1] - \frac{1}{2}\end{aligned}$$

so $\mathcal{D}$ has non-negligible advantage which contradicts the assumption about F being a pseudorandom permutation. Therefore, our scheme is CCA-secure.

Problem 2

(20 Points) Let F be a pseudorandom function. In each of the following cases, prove or disprove the security of the given MAC. (In each case Gen outputs a uniform $k \in \{0,1\}^n$. Let $\langle i \rangle$ denote an $n/2$-bit encoding of the integer i.)

(a) To authenticate a message $m = m_1, ..., m_l$, where $m_i \in \{0,1\}^{n/2}$, compute $t := \mathsf{F}_k(\langle 1 \rangle || m_1) \oplus ... \oplus \mathsf{F}_k(\langle l \rangle || m_l)$.

Solution This scheme is not secure. We construct an adversary $\mathcal{A}$ for the MAC. On input 1^n, $\mathcal{A}$ queries $m_0 = 0^n, m_1 = 0^{n/2}1^{n/2}$ and $m_2 = 1^n$. We denote the tags as t_0, t_1 and t_2. Now it holds that

$$t_0 \oplus t_1 \oplus t_2 =$$
$$(\mathsf{F}_k(\langle 1 \rangle || 0^{n/2}) \oplus ((\mathsf{F}_k(\langle 2 \rangle || 0^{n/2}) \oplus (\mathsf{F}_k(\langle 1 \rangle || 0^{n/2}) \oplus ((\mathsf{F}_k(\langle 2 \rangle || 1^{n/2}) \oplus (\mathsf{F}_k(\langle 1 \rangle || 1^{n/2}) \oplus ((\mathsf{F}_k(\langle 2 \rangle || 1^{n/2})$$
$$= (\mathsf{F}_k(\langle 1 \rangle || 1^{n/2}) \oplus ((\mathsf{F}_k(\langle 2 \rangle || 0^{n/2}) = \mathsf{MAC}_k(1^{n/2}0^{n/2})$$

Therefore,$\mathcal{A}$ outputs $(1^{n/2}0^{n/2}, t_0 \oplus t_1 \oplus t_2)$ and wins with probability 1.

(b) To authenticate a message $m = m_1, ..., m_l$, where $m_i \in \{0,1\}^{n/2}$, choose uniform $r \leftarrow \{0,1\}^n$, compute $t := \mathsf{F}_k(r) \oplus \mathsf{F}_k(\langle 1 \rangle || m_1) \oplus ... \oplus \mathsf{F}_k(\langle l \rangle || m_l)$, and let the tag be the pair of $\langle r, t \rangle$.

Solution This schemes in not secure. We construct an adversary $\mathcal{A}$ for the MAC. Let $m \in \{0,1\}^{n/2}$ be an arbitrary message. Then $\mathcal{A}$ outputs $(m, (\langle 1 \rangle || m, 0^n))$. This is a valid message-tag pair as MAC could choose $r = \langle 1 \rangle || m$ and output $t = (r, \mathsf{F}_k(r) \oplus \mathsf{F}_k(\langle 1 \rangle || m)) = (r, 0^n)$
Consequently, $\mathcal{A}$ wins with probability 1.

Problem 3

(15 points) Show that the CBC mode of encryption does not yield CCA-secure encryption.
Solution We construct an adversary $\mathcal{A}$ with non-negligible advantage in attacking the system. The adversary queries the challenger on $m_0 = 0^{2n}, m_1 = 1^{2n}$ and recieves (c_0, c_1, c_2) which is the encryption of m_b. Then, $\mathcal{A}$ queries the decryption oracle on (c_0, c_1, c_3) such that $c_3 \neq c_2$ to get the plaintext (m'_0, m'_1). We can easily see that:

$$m'_0 = \mathsf{E}_k^{-1}(c_1) \oplus c_0$$

So $\mathcal{A}$ outputs $b' = 1$ if $m'_0 = 1^n$ and otherwise $b' = 0$ and wins the game with probability 1.

Problem 4 (Optional)

(20 points) Let (S, V) be a secure MAC defined over (K, M, T) where $T = \{0,1\}^n$. Define a new MAC (S_2, V_2) as follows:
$S_2(k, m)$ is the same as $S(k, m)$, except that the last eight bits of theoutput tag t are truncated. That is, S_2 outputs tags in $\{0,1\}^{n-8}$. Algorithm $V_2(k, m, t')$ accepts if there is some $b \in \{0,1\}^8$ for which $V(k, m, t'||b)$ accepts. Is (S_2, V_2) a secure MAC? Give an attack or argue security.

Solution Let Π denote the system (S, V) and Π' denote (S_2, V_2). We prove the security of Π' by contradiction.
Let $\mathcal{A}'$ be an adversary for Π' with a non-negligible advantage. We construct an adversay $\mathcal{A}$ for Π. On each query from $\mathcal{A}'$, the adversary $\mathcal{A}$ queries its challenger on the same text and returns the output except the last 8 bits of it to $\mathcal{A}'$. Then, when $\mathcal{A}'$ outputs the (m, t) pair, $\mathcal{A}$ generates 8 random bits and concat them to the end of the output tag to obtain t'. At the end, $\mathcal{A}$ outputs (m, t'). considering that the probability of the random 8 bits to be exactly as the same as the last 8 bits of the correct tag is $\frac{1}{2^8}$, we have:

$$\mathsf{Adv}(\mathcal{A}) = \Pr[\mathsf{MacForge}_{\mathcal{A},\Pi} = 1)] = \frac{1}{2^8} \Pr[\mathsf{MacForge}_{\mathcal{A}',\Pi'} = 1)] = \frac{1}{2^8}\mathsf{Adv}(\mathcal{A}')$$

which is non-negligible and contradicts our assumption on the security of Π. Therefore, Π' is also a secure scheme.