دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری

پاسخنامه تمرین شماره ۳

نگارنده: الهه کوشافر

For any questions contact Elahe Kooshafar via `cyberian.eli@gmail.com`.

Problem 1

Decryption algorithm)
Suppose that s is the n-bit message and $g(s)$ is the $2n$-bit string resulting after replacing each bit “0” of s with bits “01” and each bit “1” with bits “00” or “11” at random. Also, suppose k is the $2n$-bit key used in the encryption algorithm, so the encrypted string c is obtained as $c = g(s) \oplus k$.
The decryption algorithm works as follows:
It first checks that if the length of c is not equal to $2n$, then it returns $\perp$; otherwise, it XORs the string c with the key k and computes g as follows: :

$$g = c \oplus k \ .$$

If c is a valid ciphertext, then g must correspond to a valid enconfing of s under the randomized mapping $g()$. To check validity of g, starting from the first bit, for each pair of consecutive bits of $g = g_1 \dots g_{2n}$, if these two bits are 01, the corresponding bit in s must have been zero; and if these two bits are equal to 00 or 11, the corresponding bit in s must have been one.

$$\begin{cases} g_{2i}g_{2i+1} = 01 \Rightarrow s_i = 0 \\ g_{2i}g_{2i+1} = 00 \Rightarrow s_i = 1 \\ g_{2i}g_{2i+1} = 11 \Rightarrow s_i = 1 \\ g_{2i}g_{2i+1} = 10 \Rightarrow s_i = \perp \end{cases}$$

If for some i, it holds that $g_{2i}g_{2i+1} = \perp$, the decryption algorithm returns $\perp$. Otherwise, it returns the bits resulting as explained above consecutively as the plaintext.

Multi-message security)

We show that this encryption system is not multi-message secure. To do so, we introduce an attacker $\mathcal{A}$ who has significant advantage in the multi-message security experiment against this encryption system. Attacker $\mathcal{A}$ selects the following two sets of messages for the experiment:

$$(x_0, y_0) = (0^n, 0^n),\ (x_1, y_1) = (0^n, 1^n)$$

Then a random bit b is selected by the challenger and messages x_b, y_b are encrypted with a random key k and the set of encrypted texts $c = \{c_0, c_1\}$ is sent back to attacker $\mathcal{A}$. Consider the attacker's $\hat{b}$ selection strategy as follows:

$$\hat{b} = \begin{cases} 0 & c_0 = c_1 \\ 1 & c_0 \neq c_1 \end{cases}$$

Note that the encryption of the message 0^n is deterministic. So if the message 0^n is encrypted twice by a key, two resulting encrypted texts will be exactly the same. On the other hand, if the message 0^n and a non-zero message are encrypted by the same key, the results must be distinct, or otherwise there would be no way to decrypt them and the validity condition would not hold. Consequently, for the attacker $\mathcal{A}$

$$P[\hat{b} = b] = 1$$

will hold. This means that our attacker can pass the multi-message security experiment with advantage 1. Therefore, the system clearly lacks multi-message security.

Problem 2

Multi-message security)
First, we prove that the following encryption system has multi-message security.

$$\mathsf{Enc'}_k(m) = (r, f_k(r) \oplus m, f_k(0^n))$$

We first define $\mathsf{H}_0 := \mathsf{Exp\_Mult}_{\mathcal{A},\mathsf{Enc'}}(n)$, the multi-message security experiment for $\mathsf{Enc'}$. As we know, H_0 is as follows:

1. $k \leftarrow \mathsf{Gen}(1^n)$
2. Then it runs attacker $\mathcal{A}$ and gets two lists of messages $M_0 = (m_{01}, ..., m_{0l})$ and $M_1 = (m_{11}, ..., m_{1l})$ with equal size l, where each two corresponding messages in M_0 and M_1 have the same length.
3. It chooses $b \leftarrow \{0, 1\}$ at random.
4. It chooses l random n-bit strings $r_1, ..., r_l$ and sets $r_0 = 0^n$. .

5. Sends $C = [(r_1, f_k(r_1) \oplus m_{b1}, f_k(r_0)), ..., (r_l, f_k(r_l) \oplus m_{bl}, f_k(r_0))]$ to the attacker $\mathcal{A}$.
6. Eventually, the attacker $\mathcal{A}$ outputs a bit $\hat{b}$. If $\hat{b} = b$, then it outputs 1, and 0 otherwise.

Next, we define 3 hybrid security experiments as follows:

- H_1:= It is like H_0, but a random function $F \leftarrow \mathsf{Func_n}$ is used instead of f_k in step 5.
- H_2: It is like H_1, but in step 5 for $i = 0, 1, ..., l$ a fresh uniformly random $x_i \in \{0,1\}^n$ is used instead of each $F(r_i)$.
- H_3:= It is like H_2, but each m_{bi} is replaced with 0^n in step 5.

We define $\mathsf{Adv}_{\mathcal{A},\mathsf{j}}$ for $j = 0, .., 3$ the advantage of the attacker $\mathcal{A}$ in the security experiment $\mathsf{H_j}$.
Since f_k is a pseudo-random function, it is indistinguishable from a random function $F \leftarrow \mathsf{Func_n}$. Therefore, replacing it with a random function F in H_1 would not make any non-negligible difference in the attacker's advantage. Hence

$$|\mathsf{Adv}_{\mathcal{A},0} - \mathsf{Adv}_{\mathcal{A},1}| \leq neg(n)$$

holds. More precisely, one can show that if $|\mathsf{Adv}_{\mathcal{A},0} - \mathsf{Adv}_{\mathcal{A},1}|$ is non-negligible, then f_k is not pseudorandom (we leave it for the students to fill in the details).
Due to the random choice of function $F \leftarrow \mathsf{Func_n}$, each $F(r_i)$ for $i = 0, 1, .., l$ is random. Therefore, if the values of $\{x_0, x_1, \ldots, x_l\}$ were all distinct, the ciphertext C in the step 5 of H_1 and H_2 would be indistinguishable for any attacker. The probability that the values of $\{x_0, x_1, \ldots, x_l\}$ are not all distinct is at most $\binom{l+1}{2}2^{-n}$. Hence

$$|\mathsf{Adv}_{\mathcal{A},1} - \mathsf{Adv}_{\mathcal{A},2}| \leq \binom{l+1}{2}2^{-n}$$

holds.
Since x_i variables are random, then each $x_i \oplus m_{bi}$ in step 5 is completely random, therefore, it has the exact same distribution as $x_i \oplus 0 = x_i$. Hence

$$|\mathsf{Adv}_{\mathcal{A},2} - \mathsf{Adv}_{\mathcal{A},3}| = 0$$

holds. Since the output sent to the adversary has no information about b, then the adversary has no advantage in the H_3 experiment. Hence

$$\mathsf{Adv}_{\mathcal{A},3} = 0$$

holds.

Sum of the equations and equalities above, gives:

$$\mathsf{Adv}_{\mathcal{A},0} \leq neg(n) + \binom{l+1}{2} 2^{-n}$$

Since l is polynomial in n, $neg(n) + \binom{l+1}{2}2^{-n}$ is negligible with respect to n, and the advantage of any efficient $\mathcal{A}$ in expriment H_0 is negligble. Therefore, Enc' has multi-message security.

Now lets prove the encryption system Enc has multi-message security as well. Towards reaching a contradiction, suppose it does not. Then an attacker $\mathcal{A}$ exists with non-negligible advantage $\frac{1}{2} + \mu(n)$ in the multi-message security attack game against Enc. Attacker $\mathcal{A}$ performs as follows, as we know:

- It first sends two lists of messages M_1 and M_2 with equal size l to the challenger, where each two corresponding messages in M_1 and M_2 have equal length.
- Then it receives the ecrypted texts for one of the lists of messages sent earlier (M_b).
- Outputs either 0 or 1, indicating it guesses which list of messages has been encrypted.

The probability that at least one of the messages in the set M_b is equal to $f_k(0^n)$ (lets call it p) is less than $l \times 2^{-n}$. Then with probability $1 - l \times 2^{-n}$ all the messages in set M_b are encrypted as

$$(r, f_k(r) \oplus m, f_k(0^n)).$$

We have earlier proved that in this condition any attacker including $\mathcal{A}$ has negligible advantage $\epsilon(n)$ in the security attack game. Suppose w is the probability that the attacker returns the correct output in the situation that at least one of the messages in the set M_b is equal to $f_k(0^n)$,
The probability that $\mathcal{A}$ returns correctly $= (1-p) \times \epsilon(n) + p \times w \leq \epsilon(n) + l \times 2^{-n}$.

Since l is polynomial with respect to n, the probability written above is negligible. So the advantage of $\mathcal{A}$ is negligible, meaning the assumption was wrong and no such attacker exists. Therefore, Enc has multi-message security.

CPA security)
Attacker $\mathcal{A}$ requests three distinct messages m_0, m_1 and m_2 for encryption to the encryption system. Since at least two of them are not equal to $f_k(0^n)$, last n bits in at least two of the resulting outputs are equal to $f_k(0^n)$. Next, the attacker requests the message $f_k(0^n)$ for encryption to the encryption system and receives the resulting output $(r, f_k(r) \oplus m, k)$, in which the last n bits is the key k. Thereafter, the attacker holds the key and can recognize which message has been encrypted correctly, with probability one. Therefore, this encryption system lacks CPA security.

Problem 3

The statement "if G is secure, then it is unpredictable" is equivalent to "if G is predictable, then it is insecure", so it suffices to show the latter. To do so, we assume that G is predictable and, therefore, there is an efficient attacker $\mathcal{A}$ with non-negligible advantage in the defined predictability attack game. Now we present attacker $\mathcal{A}'$ that distinguishes G from a random generator with non-negligible advantage, which means that G is insecure. Attacker $\mathcal{A}'$ has access to oracle F, which is either G or a random generator, and performs as follows:

- runs attacker $\mathcal{A}$ and gets an index i, with $0 \leq i \leq L-1$, from $\mathcal{A}$
- gets input s from oracle F, sends $s[0, ..., i-1]$ to attacker $\mathcal{A}$
- gets bit b from $\mathcal{A}$. if $b = s[i]$ returns 1, and 0 otherwise.

Now if the oracle F is equal to G, $\mathcal{A}$ outputs the correct bit b with probability $1 + \mu(n)$, therefore $\mathcal{A}'$ returns 1 with the same probability. If F is random, $s[i]$ is totally random and independent from $s[0...i-1]$, therefore $\mathcal{A}$ returns the correct b with probability $\frac{1}{2}$, therefore $\mathcal{A}'$ returns 1 with probability $\frac{1}{2}$ in this case. So, the advantage of $\mathcal{A}'$ is:

$$|Pr[\mathcal{A}'(G(s)) = 1; s \leftarrow S] - Pr[\mathcal{A}'(x) = 1; x \leftarrow U_n]| = |Pr[\mathcal{A}_{wins}] - \frac{1}{2}| = Adv^{\mathsf{Pre}}_{\mathcal{A},G} > \mu(n)$$

Attacker $\mathcal{A}'$ has non-negligible advantage in the security attack game against G, so G is proved to be insecure.