TD2: Pseudorandom Generators (corrected version)

Exercise 1. *Bit-flip of a PRG*

Let G a pseudo-random generator (PRG) of input range $\{0,1\}^s$ and output range $\{0,1\}^n$. We define $\bar{G}$ as follows:

$$\forall x \in \{0,1\}^s, \bar{G}(x) := 1^n \oplus G(x),$$

where $\oplus$ denotes the XOR operation. This corresponds to flipping every bit of the output of G.

1. Prove that $\bar{G}$ is secure if and only if G is secure.

☞ Assume that G is secure. We will prove that $\bar{G}$ is secure. Assume by contradiction that there exists an adversary $\mathcal{A}$ that distinguishes between $\bar{G}(U(\{0,1\}^s))$ and $U(\{0,1\}^n$ with non-negligible advantage. We build $\mathcal{A}'$ a distinguisher between $G(U(\{0,1\}^s))$ and $U(\{0,1\}^n)$ the following way: on input a sample y, $\mathcal{A}'$ calls $\mathcal{A}$ on the sample $1^n \oplus y$. It outputs the same value.

Notice the following: if y is uniformly distributed, then so is $1^n \oplus y$. If y follows the distribution $G(U(\{0,1\}^s))$, then $1^n \oplus y$ follows the distribution $\bar{G}(U(\{0,1\}^s))$. Then $\mathcal{A}$'s view is exactly as intended. It guesses from which distribution is sampled $1^n \oplus y$ with non-negligible advantage, and the advantage of $\mathcal{A}'$ is equal to the advantage of $\mathcal{A}$, which contradicts the assumption that G is secure.

Finally, we notice that the flipped version of $\bar{G}$ is G, and the previous proof also shows that $\bar{G}$ secure implies G secure.

Exercise 2. *Variable-length OTP is not secure*

A *variable length one-time pad* is a cipher (E, D), where the keys are bit strings of some fixed length L, while messages and ciphertexts are variable length bit strings, of length at most L. Thus, the cipher (E, D) is defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$, where

$$\mathcal{K} := \{0,1\}^L \text{ and } \mathcal{M} := \mathcal{C} = \{0,1\}^{\leq L}$$

for some parameter L. Here, $\{0,1\}^{\leq L}$ denotes the set of all bit strings of length at most L (including the empty string). For a key $k \in \{0,1\}^L$ and a message $m \in \{0,1\}^{\leq L}$ of length ℓ, the encryption function is defined as follows:

$$E(k, m) := k[0 \mathinner{..} \ell - 1] \oplus m$$

1. Provide a counter-example showing that the variable length OTP is not secure for perfect secrecy.

☞ Suppose that the message distribution contains two messages m_0, m_1 of distinct length, i.e. $|m_0| \neq |m_1|$ in its support. Then given a ciphertext c with $|c| = |m_0|$, we have $\Pr[c = E(k, m_1)] = 0$ while $\Pr_{m \leftarrow \mathcal{M}}[m = m_1] \neq 0$. Hence, the scheme is not perfectly secure.

Exercise 3.

Let $\mathsf{G} : \{0,1\}^n \to \{0,1\}^m$ be a function, with $m > n$.

1. Recall the definition of a PRG from the lecture.

☞ $\mathsf{G} : \{0,1\}^n \to \{0,1\}^m$ is a PRG if there exists no ppt $\mathcal{A} : \{0,1\}^m \to \{0,1\}$ that distinguish with non-negligible probability between $\mathcal{U}(\{0,1\}^m)$ and $G(\mathcal{U}(\{0,1\}^n))$.

Let $\mathsf{Enc} : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}^m$ defined by $\mathsf{Enc}(k, m) = \mathsf{G}(k) \oplus m$.

2. Give the associated decryption algorithm.

☞ Enc = Dec

3. Recall the smCPA security notion from the lecture.

☞ Two experiments, Exp_b for $b \in \{0,1\}$ are defined as follows:

1. The challenger $\mathcal{C}$ chooses k uniformly.
2. The adversary $\mathcal{A}$ chooses m_0, m_1 distinct of identical bitlength.
3. The challenger $\mathcal{C}$ returns $\mathsf{Enc}(k, m_b)$.
4. The adversary $\mathcal{A}$ outputs a guess b'.

This is summed up in the following sketch:

$\mathcal{C}$	$\mathcal{A}$
$k \hookleftarrow U(K)$	
	Choose and send $(m_0, m_1) \in P' := \{(m, m') \in P^2, m \neq m' \wedge \|m\| = \|m'\|\}$
Send $\mathsf{Enc}(k, m_b)$	
	Output $b' \in \{0,1\}$.

The advantage of $\mathcal{A}$ is defined as $\mathsf{Adv}(\mathcal{A}) := |\Pr\left(\mathcal{A} \xrightarrow{\mathsf{Exp}_0} 1\right) - \Pr\left(\mathcal{A} \xrightarrow{\mathsf{Exp}_1} 1\right)|$. Then $(\mathsf{Enc}, \mathsf{Dec})$ is said smCPA-secure if no efficient adversary has non-negligible advantage.

Let $m_1, m_2 \in \{0,1\}^m$ be arbitrary messages.

4. What is the statistical distance between the distributions $\mathcal{U}_1 = m_1 \oplus \mathcal{U}(\{0,1\}^m)$ and $\mathcal{U}_2 = m_2 \oplus \mathcal{U}(\{0,1\}^m)$?

☞ They are the same distributions, so 0.

We proved in class that G PRG $\Rightarrow$ $(\mathsf{Enc}, \mathsf{Dec})$ smCPA-secure. We are going to prove $(\mathsf{Enc}, \mathsf{Dec})$ not smCPA-secure $\Rightarrow$ G not PRG.

5. Let $\mathcal{A}$ be an distinguisher between two games G_0 and G_1. We say that $\mathcal{A}$ wins if it output 0 (resp 1) during the game G_0 (resp G_1). Show that

$$\mathsf{Adv}_{\mathcal{A}}(G_0, G_1) = 2 \cdot \left| \Pr_{b \sim \mathcal{U}(\{0,1\})}(\mathcal{A} \text{ wins in } G_b) - \frac{1}{2} \right|$$

☞

$$\Pr_{b \sim \mathcal{U}(\{0,1\})}(\mathcal{A} \text{ wins in } G_b) = \frac{1}{2} \cdot \Pr_{G_0}(\mathcal{A} \to 0) + \frac{1}{2} \cdot \Pr_{G_1}(\mathcal{A} \to 1) = \frac{1}{2}\left(\Pr_{G_0}(\mathcal{A} \to 0) + 1 - \Pr_{G_1}(\mathcal{A} \to 0)\right)$$

Hence the result.

6. Assume that $\mathcal{A}$ is an adversary with non-negligible advantage ε against the smCPA-security of $(\mathsf{Enc}, \mathsf{Dec})$. Construct an explicit distinguisher between $\mathcal{U}(\{0,1\}^m)$ and $G(\mathcal{U}(\{0,1\}^n))$ and compute its advantage.

☞ We define the $\mathcal{A}'$ to be the following:

1. Get k from the distribution $G = G(\mathcal{U}(\{0,1\}^n))$ or $\mathcal{U}(\{0,1\}^m)$.
2. Get m_1, m_2 from $\mathcal{A}$.
3. Sample b from $\mathcal{U}(\{0,1\})$.
4. Send $k \oplus m_b$ to $\mathcal{A}$ and get the output b'.
5. If $b = b'$, output "G" else output "$\mathcal{U}$".

The advantage of $\mathcal{A}'$ is $|\Pr_{k \sim G}(\mathcal{A}' \to G) - \Pr_{k \sim \mathcal{U}}(\mathcal{A}' \to G)|$.

Assume $k \sim \mathcal{U}$ and define Y_0 the game played when $b = 0$ and Y_1 the game played when $b = 1$. Since $k \sim \mathcal{U}$, we have that $m_b \oplus k$ is independent from m_b, hence $\Pr_{m_0,k}(\mathcal{A}(m_0 \oplus k) \to 1) = \Pr_{m_1,k}(\mathcal{A}(m_1 \oplus k) \to 1)$ and hence the advantage of $\mathcal{A}$ between Y_0 and Y_1 is 0. By the previous question we have $\Pr_{b \sim \mathcal{U}(\{0,1\}),k}(\mathcal{A} \text{ wins when given } m_b \oplus k) = 1/2$.

Assume $k \sim G$ and define Y'_0 the game played when $b = 0$ and Y'_1 the game played when $b = 1$. We have $\Pr_{k \sim G}(\mathcal{A}' \to G) = \Pr_b(\mathcal{A} \text{ wins } Y'_b)$.

Finaly, $\mathsf{Adv}_{\mathcal{A}'} = |\Pr_{k \sim G}(\mathcal{A}' \to G) - \Pr_{k \sim \mathcal{U}}(\mathcal{A}' \to G)| = |\Pr_b(\mathcal{A} \text{ wins } Y'_b) - 1/2| = \varepsilon/2$.