HW 1: Symmetric Cryptography – Due date: February 28, 2023 before tutorial

Exercise 1. *PRF implies PRG*

Let $F : \{0,1\}^s \times \{0,1\}^n \to \{0,1\}^m$ be a secure Pseudo-Random Function (PRF). We define the following PRGs $G_d : \{0,1\}^s \to \{0,1\}^{md}$, for $d \leq \mathsf{poly}(m)$ such that:

$$\forall k \in \{0,1\}^s, G_d(k) = F(k,\bar{0})||F(k,\bar{1})||\ldots||F(k,\overline{d-1}),$$

where $||$ denotes the concatenation operator and $\bar{i}$ denotes the binary decomposition of i, written over m bits.

1. Prove that G_d is a secure PRG.

Exercise 2. *PRG implies PRF*

Let $G : \{0,1\}^s \to \{0,1\}^{2s}$ be a secure length-doubling PRG. We have aldready how to get such a PRG from any PRG in the previous tutorials. The Goldreich-Goldwasser-Micali construction shows how to build a secure Pseudo-Random Function for any input size from G.

1. Let us denote $G(k) =: G_0(k)||G_1(k)$ for any $k \in \{0,1\}^s$ where $G_0, G_1 : \{0,1\}^s \to \{0,1\}^s$. Define $F_0 : \{0,1\}^s \times \{0,1\} \to \{0,1\}^s$ such that:

$$\forall k \in \{0,1\}^s, \forall b \in \{0,1\}, F_0(k,b) := G_b(k).$$

   Prove that F_0 is a secure PRF.

We now expand our construction to arbitrary input size n. Define the iterated PRF $F_n : \{0,1\}^s \times \{0,1\}^n \to \{0,1\}^s$ that does the following: on inputs k and $x = x_0x_1\ldots x_{n-1}$, define $k_0 := k$ and compute recursively $k_i := G_{x_{i-1}}(k_{i-1})$ for $i = 1$ to n. Finally output k_n.

Remark: This can be seen as going down a binary tree.

2. Before proving the security of F_n, we prove that the distribution $(G(k_1), G(k_2), \ldots, G(k_Q))$, where $k_i \hookleftarrow U(\{0,1\}^s)$ is indistinguishable from $U(\{0,1\}^{2Qs})$ for any $Q = \mathsf{poly}(s)$, under the security of G.

   We use the hybrid argument by defining the following hybrid distributions:

$$\forall i \in [0,Q], D_i := (G(k_1), \ldots, G(k_i), U(\{0,1\}^{2s(Q-i)}) \text{ where } k_j \hookleftarrow U(\{0,1\}^s) \forall j \leq i.$$

   Notice that D_0 and D_Q correspond to the distributions defined previously.

   Prove that D_0 and D_Q are indistinguishable under the security of G. Estimate the security loss.

We move on to the proof that F_n is secure.

3. To do so, we use the hybrid argument by introducing the following hybrid experiments. Let us first define

$$F_{n,i}^{(R_i)} : (x_0, \ldots, x_{n-1}) \mapsto G_{x_{n-1}}(\ldots(G_{x_i}(R_i(x_0, \ldots x_{i-1})))),$$

   where $R_i : \{0,1\}^i \to \{0,1\}^s$ is a map.

   (a) Prove that $F_{n,0}^{(U(\{\varepsilon\}\to\{0,1\}^s))}(\cdot)$ is actually the distribution $F_n(U(\{0,1\}^s), \cdot)$.

   (b) Prove that $F_{n,n}^{(U(\{0,1\}^n\to\{0,1\}^s))}$ is actually the distribution $U(\{0,1\}^n \to \{0,1\}^s)$.

   (c) We define the hybrid experiment Exp_i for $i \in [1,n]$ as: the challenger flips a coin b and samples R uniformly over $\{0,1\}^{i-b} \to \{0,1\}^n$. The adversary is then given access to an oracle, which on query $x \in \{0,1\}^n$ answers with $F_{n,i-b}^{(R)}(x)$. Eventually, the adversary outputs a guess b' and wins if and only if $b = b'$.

   Prove that the PRF F_n is secure under the security of the PRG G and estimate the advantage loss.

Exercise 3. *Encrypting with a PRF*

Let F be a PRF function from $\{0,1\}^s \times \{0,1\}^n \to \{0,1\}^m$, we define the following encryption scheme: To encrypt a message $M \in \{0,1\}^m$ with a key $k \in \{0,1\}^s$, choose r uniformly in $\{0,1\}^n$ and return $c = (r \| F(k,r) \oplus M)$.

Show that this scheme is secure. More precisely, show if that there exists a PPT adversary $\mathcal{A}$ against the encryption scheme, then there exists a PPT adversary $\mathcal{B}$ against the PRF function F such that:

$$\mathrm{Adv}_{\mathcal{A}}^{CPA}(Enc) \leq 2\mathrm{Adv}_{\mathcal{B}}^{PRF}(F) + Q^2/2^n,$$

where Q is the number of encryptions queried by $\mathcal{A}$.

Exercise 4. *IND-CCA secure symmetric encryption*

Consider the following construction of symmetric encryption, where $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Verify})$ is a MAC.

Gen(1^λ)**:** Choose a random key $K_1 \leftarrow \mathsf{Gen}'(1^\lambda)$ for an IND-CPA secure symmetric encryption scheme $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$. Choose a random key $K_0 \leftarrow \Pi.\mathsf{Gen}(1^\lambda)$ for the MAC Π. The secret key is $K = (K_0, K_1)$.

Enc(K, M)**:** To encrypt M, do the following.

1. Compute $c = \mathsf{Enc}'(K_1, M)$.
2. Compute $t = \Pi.\mathsf{Mac}(K_0, c)$.

Return $C = (t, c)$.

Dec(K, C)**:** Return $\perp$ if $\Pi.\mathsf{Verify}(K_0, c, t) = 0$. Otherwise, return $M = \mathsf{Dec}'(K_1, c)$.

1. Assume that the MAC is weakly unforgeable. Assume however that there exists an algorithm $\mathcal{F}$, which on input a valid message for the MAC and a tag (M, t), outputs a forgery (M, t') such that $t \neq t'$. In particular, the MAC is not strongly unforgeable. Show that the scheme is not IND-CCA secure.

2. We assume that: (i) $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ is IND-CPA-secure; (ii) Π is strongly unforgeable under chosen-message attacks. We will prove in this question the IND-CCA security of the new encryption scheme under these assumptions. Let $\mathcal{A}$ be an adversary against the IND-CCA security of the scheme.

(a) Define the event Valid as the event where $\mathcal{A}$ makes a valid (i.e. accepted by the MAC) decryption query for (c, t) where the ciphertext c was not encrypted by the encryption oracle nor is (c, t) the challenge ciphertext. Prove that if $\Pr(\mathsf{Valid})$ is non-negligible then there exists an adversary with non-negligible advantage against the strong unforgeability of the MAC.

The intuition is that since this event has negligible probability, the decryption oracle is useless to an attacker $\mathcal{A}$.

(b) Prove that if $|\Pr(\mathcal{A} \text{ wins} \wedge \overline{\mathsf{Valid}}) - 1/2|$ is non-negligible, then there exists an efficient adversary against the IND-CPA security of the encryption scheme $(\mathsf{Gen}, \mathsf{Enc}', \mathsf{Dec}')$.

(c) Conclude.