# Problem Set 2 Solutions

Definitions or Propositions cited by number below refer to the chapter on Pseudorandom Functions available from the course web page.

---

**Problem 1. [20 points]** Define the family of functions $F$: $\{0,1\}^{128} \times \{0,1\}^{128} \to \{0,1\}^{128}$ by $F(K,M) = \mathsf{AES}(M,K)$. Assuming $\mathsf{AES}$ is a secure PRF, is $F$ a secure PRF? If so, explain why. If not, present the best attack (with analysis) that you can.

$F$ is **not** a secure PRF. The easiest way to see this is to note that it is not even secure against key-recovery: given one input-output example $(M,C)$ of $F_K$, we can recover $K$ via $K \leftarrow \mathsf{AES}_M^{-1}(C)$.

However, this is not enough. The question was whether it is a secure PRF, not whether one can recover the key. To bridge this gap, we can use Proposition 3.14. To this end, first, following Definition 3.12, we formalize the above attack to present the following key-recovery adversary:

**adversary** $B$
Let $M$ be any 128 bit string
$C \leftarrow \mathbf{Fn}(M)$ ; $K \leftarrow \mathsf{AES}_M^{-1}(C)$
Return K

Now, looking at Definition 3.12, we see that $\mathbf{Adv}^{\mathrm{kr}}_F(B) = 1$. Now we can apply Proposition 3.14 to conclude that $F$ is not a secure PRF.

An alternative solution is to demonstrate the insecurity of $F$ as PRF directly, by considering the following adversary $A$ that is given an oracle $\mathbf{Fn}$: $\{0,1\}^{128} \to \{0,1\}^{128}$:

**adversary** $A$
Let $M, N$ be any two distinct 128 bit strings
$C \leftarrow \mathbf{Fn}(M)$ ; $L \leftarrow \mathsf{AES}_M^{-1}(C)$
$D \leftarrow \mathbf{Fn}(N)$
if $(\mathsf{AES}(N,L) = D)$ then return 1 else return 0

We claim that

$$\Pr\left[\mathrm{Real}_F^A \Rightarrow 1\right] \;=\; 1 \quad \text{and} \quad \Pr\left[\mathrm{Rand}_{\{0,1\}^{128}}^A \Rightarrow 1\right] \;=\; 2^{-128}\ .$$

Why? If $\mathbf{Fn} = F_K$ is an instance of $F$ then $C = F(K,M) = \mathsf{AES}(M,K)$, and thus $L = \mathsf{AES}_M^{-1}(C) = K$. Then $D = F(K,N) = \mathsf{AES}(N,K)$, but this equals $\mathsf{AES}(N,L)$, since $L = K$, so $A$ returns 1

with probability one, justifying the first equation above. If **Fn** is a random function, then $D$ is distributed uniformly and independently of $N, L$, and thus the probability that $D = \mathsf{AES}(N, L)$ is $2^{-128}$. Now, subtracting, as per Definition 3.6, we get

$$\begin{aligned} \mathbf{Adv}^{\mathrm{prf}}_{F}(A) &= \Pr\left[\mathrm{Real}^{A}_{F} \Rightarrow 1\right] - \Pr\left[\mathrm{Rand}^{A}_{\{0,1\}^{128}} \Rightarrow 1\right] \\ &= 1 - 2^{-128} \ . \end{aligned}$$

The prf-advantage of our adversary is essentially one. Our adversary is very practical, making just two oracle queries and with running time that of a couple of $\mathsf{AES}$ or $\mathsf{AES}^{-1}$ computations. So we have a highly effective attack, showing that $F$ is very insecure as a PRF.

Note that the design of $A$ is as in the proof of Proposition 3.14 based on the $B$ we presented above.

---

**Problem 2. [60 points]** Let $F$: $\{0,1\}^k \times \{0,1\}^l \to \{0,1\}^L$ be a family of functions where $l, L \geq 128$. Consider the game G of Fig. 1.

Game G

**procedure Initialize**
$K \xleftarrow{\$} \{0,1\}^k$ ; $b \xleftarrow{\$} \{0,1\}$

**procedure LR**$(x_0, x_1)$
Ret $F(K, x_b)$

**procedure Finalize**$(b')$
Ret $(b = b')$

Figure 1: Game G for Problem 2.

We define

$$\mathbf{Adv}^{\mathrm{lr}}_{F}(B) \ = \ 2 \cdot \Pr\left[\mathrm{G}^{A} \Rightarrow \mathsf{true}\right] - 1 \ .$$

Let $(x_0^1, x_1^1), \ldots, (x_0^q, x_1^q)$ be the queries that $B$ makes to its oracle. (Each query is a pair of $l$-bit strings, and there are $q$ queries in all.) We say that $B$ is *legitimate* if $x_0^1, \ldots, x_0^q$ are all distinct, and also $x_1^1, \ldots, x_1^q$ are all distinct. We say that $F$ is LR-secure if $\mathbf{Adv}^{\mathrm{lr}}_{F}(B)$ is "small" for every legitimate $B$ of "practical" resources.

**1.** **[10 points]** Show that the legitimacy condition is necessary for LR-security to be "interesting" by showing that if $F$ is a block cipher then there is an efficient, illegitimate $B$ such that $\mathbf{Adv}^{\mathrm{lr}}_{F}(B) = 1$. Say how may queries $B$ uses and what is its time-complexity.

Consider the following adversary:

**adversary** $B$
Let $x, y, z$ be any distinct $l$-bit strings
$C_1 \leftarrow \mathbf{LR}(x, y)$ ; $C_2 \leftarrow \mathbf{LR}(z, y)$
If $C_1 = C_2$ then return 1 else return 0

Note $B$ is not legitimate because its queries are of the form $(x_0^1, x_1^1), (x_0^2, x_1^2)$ with $x_1^1 = x_1^2$. Now, if the challenge bit $b = 1$, then $C_1 = F_K(y)$ and $C_2 = F_K(y)$ so $C_1 = C_2$ and $B$ returns 1. (That is, its output $b'$ equals $b$.) On the other hand if $b = 0$ then $C_1 = F_K(x)$ and $C_2 = F_K(z)$. But since $F$ is a block cipher (this is where we use this assumption) the map $F_K$ is a permutation, and thus $C_1 \neq C_2$. So $B$ returns 0. (That is, its output $b$ is again equal to $b$.) So $\Pr[b = b'] = 1$, and thus $\mathbf{Adv}^{\mathrm{lr}}_F(B) = 2 \cdot \Pr[b = b'] - 1 = 1$. Adversary $B$ makes only two oracle queries and has time-complexity $O(l + L + T_F)$ where $T_F$ is the time for one evaluation of $F$. Thus, this is a very practical attack.

**2.** **[25 points]** Let $B$ be a legitimate lr-adversary that makes $q$ oracle queries and has time-complexity $t$. Show that there exists a prf-adversary $A$, also making $q$ oracle queries and having time-complexity close to $t$, such that

$$\mathbf{Adv}^{\mathrm{lr}}_F(B) \;\leq\; 2 \cdot \mathbf{Adv}^{\mathrm{prf}}_F(A)\,. \tag{1}$$

State what is the time-complexity of $A$. Explain why this reduction shows that if $F$ is a secure PRF then it is LR-secure.

This is very similar to several reductions done in class and the notes. Recall that adversary $A$ gets an oracle for a function $\mathbf{Fn}$: $\{0,1\}^l \to \{0,1\}^L$. It works as follows:

| **adversary** $A$ | **procedure** $\mathrm{SIM}(M_0, M_1)$ |
|---|---|
| $b \xleftarrow{\$} \{0,1\}$ | Ret $\mathbf{Fn}(M_b)$ |
| $d \xleftarrow{\$} B^{\mathrm{SIM}(\cdot,\cdot)}$ | |
| If $d = b$ then return 1 else return 0 | |

Our adversary picks at random a bit $b$ to represent the challenge bit in game G. It then defines a subroutine SIM via which it responds to oracle queries made by $B$. Note that SIM uses $b$ and also invokes $A$'s oracle $\mathbf{Fn}$. After learning $B$'s decision $d$, $A$ tests whether it is correct, meaning equals the challenge bit $b$. If so, it declares that its oracle is an instance of $F$, and otherwise it declares its oracle to be random.

Let us now compute $\mathbf{Adv}^{\mathrm{prf}}_F(A)$. First consider $\mathrm{Real}^A_F$, where oracle $\mathbf{Fn}$ is $F_K$ for $K \xleftarrow{\$} \{0,1\}^k$. In this case, the response of $\mathrm{SIM}(M_0, M_1)$ is $F_K(M_b)$, which is exactly $\mathbf{LR}(M_0, M_1)$. This means that

$$\Pr\left[\mathrm{Real}^A_F \Rightarrow 1\right] \;=\; \Pr\left[b = d\right] \;=\; \frac{1}{2} + \frac{1}{2} \cdot \mathbf{Adv}^{\mathrm{lr}}_F(B)\,.$$

Now consider $\mathrm{Rand}^A_{\{0,1\}^L}$, where $\mathbf{Fn}$ implements a random function. In this case, the response of $\mathrm{SIM}(M_0, M_1)$ is the random value returned by $\mathbf{Fn}(M_b)$. The legitimacy of $B$ (this is where we use this assumption) now implies that the sequence of responses to $B$'s oracle queries is distributed identically whether $b = 0$ or $b = 1$, in both cases being a sequence of random and independent $L$ bit strings. Thus $B$ gets no information about $b$ from the oracle. This means that $\Pr[b = d] = 1/2$. Thus

$$\Pr\left[\mathrm{Rand}^A_{\{0,1\}^L} \Rightarrow 1\right] \;=\; \Pr\left[b = d\right] \;=\; \frac{1}{2}\,.$$

Subtracting, we get

$$\mathbf{Adv}^{\mathrm{prf}}_F(A) \;=\; \Pr\left[\mathrm{Real}^A_F \Rightarrow 1\right] - \Pr\left[\mathrm{Rand}^A_{\{0,1\}^L} \Rightarrow 1\right] \;=\; \frac{1}{2} \cdot \mathbf{Adv}^{\mathrm{lr}}_F(B)\,,$$

which implies Equation (1). The time-complexity of $A$ is only $O(1)$ more than that of $B$ given our conventions about measuring time-complexity.

Why does this reduction show that if $F$ is a secure PRF then it is LR-secure? For the usual reason with such reductions. To show that $F$ is LR-secure we need to show that $\mathbf{Adv}^{\mathrm{lr}}_F(B)$ is small for any practical $B$. However, if $B$ is practical, so is $A$, and then the assumption that $F$ is a PRF tells us that $\mathbf{Adv}^{\mathrm{prf}}_F(A)$ is small. Then Equation (1) tells us that $\mathbf{Adv}^{\mathrm{lr}}_F(B)$ is also small, as desired.

**3.** **[25 points]** Is the converse true? Namely, if $F$ is LR-secure, then is it a secure PRF? Answer YES or NO. If you say YES, justify this via a reduction, and, if NO, via a counter-example. (The latter means a particular family of functions $F$ which you can prove is LR-secure but which you can show via an attack is not a PRF.)

The answer is NO. A simple counter-example is a family of functions $F$ in which $F_K$ is a constant function for each $K \in \{0,1\}^k$. To be specific, consider the family $F$ defined by $F(K,x) = 0^L$ for all $K \in \{0,1\}^k$ and $x \in \{0,1\}^l$. Here is an attack showing that $F$ is not a PRF:

**adversary** $A$
If $\mathbf{Fn}(0^l) = 0^L$ then return 1 else return 0

In game $\mathrm{Real}_F$, the oracle $\mathbf{Fn}$ implements $F_K$ for some $K$ and so $\mathbf{Fn}(0^l) = F_K(0^l) = 0^L$. On the other hand, in game $\mathrm{Rand}_{\{0,1\}^L}$ the probability that $\mathbf{Fn}(0^l) = 0^L$ is $2^{-L}$. Thus

$$\Pr\left[\mathrm{Real}_F^A \Rightarrow 1\right] \;=\; 1 \quad \text{and} \quad \Pr\left[\mathrm{Rand}_{\{0,1\}^L}^A \Rightarrow 1\right] \;=\; 2^{-L}\,.$$

Subtracting, we get $\mathbf{Adv}^{\mathrm{prf}}_F(A) = 1 - 2^{-L}$. This is close to 1 (recall the problem assumes $L \geq 128$) and furthermore $A$ is very efficient, so we have shown that $F$ is not a PRF. On the other hand, we claim that $F$ is LR-secure. To see this consider any $B$ with a $\mathbf{LR}(\cdot,\cdot)$ oracle. The response of the oracle to any query is $0^L$. In particular, this is true regardless of the value of $b$, meaning the oracle responses give $B$ no information about $b$. Thus $\Pr[b = d] = 1/2$, where $d$ is the output of $B$, and so $\mathbf{Adv}^{\mathrm{lr}}_F(B) = 0$. So we have shown LR-security in a very strong sense: the advantage of any adversary is 0, regardless of its time-complexity or the number of queries it makes.

We clarify that $F$ above is a family of functions. It is not required to be a block cipher except in part **1.**

---