UConn, School of Computing
Fall 2024
CSE 3400/CSE 5850: Introduction to Computer and Network Security (or Introduction to Cybersecurity)

Practice Problems—PRFs

Instructor: Prof. Ghada Almashaqbeh

PRFs

These are two PRF problems designed to help you better understand the mechanics behind proving whether a given construction or secure and insecure. The process is similar to writing proofs for PRGs, but includes a logical concept called the **oracle**. The oracle contains either the keyed PRF or a truly random function, and a distinguisher is allowed to query it as many times as they wish (of course polynomial number of queries). However, they **do not** know what is contained in the oracle beyond the construction of the PRF (so it does not get to see the key k). In either case for PRFs, the distinguisher will utilize their oracle for cryptanalysis. In the case of a secure PRF, the distinguisher will also make use of a hypothetical secondary attacker that is capable of breaking the construction in question. In the case of an insecure PRF, the distinguisher will query their oracle in a way that allows them to distinguish the PRF with non-negligible probability.

Are the following constructions secure PRFS?

1. Let $F : \{0,1\}^n \times \{0,1\}^{n+1} \to \{0,1\}^{2n}$ be a PRF, construct $F' : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^{4n}$ as
$$F'_k(m) = F_k(m0)||F_k(m1)$$
where $m0$ is m concatenated with 0, and $m1$ is m concatenated with 1.

   Note: The formal proof is just for your own knowledge. For the homework/exams, the convincing informal argument/analysis is enough as a correct answer.

   Solution
   Informally, F' is a secure PRF. For any input m the output will be a pseudorandom string of length $4n$ bits. F is invoked over two different inputs (m is concatenated once with 0 and then with 1), so the output will be different. This will results in having the output of F' as the concatenation of two pseudorandom strings, which is also pseudorandom. Thus, the attacker advantage in distinguishing F' from a true random function will be negligible.

   [This is for your own knowledge] Formally, we can prove security by a proof by reduction (using contrapositive). By demonstrating that if we have an attacker that is capable of breaking F', then we can use it to build an attacker that is capable of breaking F, a secure PRF. This is a contradiction, which means that our assumption that F' is insecure is false.

Suppose there exists a PPT attacker $\mathcal{A}'$ that is capable of distinguishing F' with non-negligible probability. This means we have the following advantage of $\mathcal{A}'$ (where R' is a true random function):

$$\varepsilon^{PRF}_{\mathcal{A}',F'}(n) = \Pr[\mathcal{A}'^{F'_k}(n) = 1] - \Pr[\mathcal{A}'^{R'}(n) = 1] \notin NEGL(n)$$

Now we show how to build a PPT attacker $\mathcal{A}$ that wants to break F. $\mathcal{A}$ has an oracle access to some oracle (denote it as $\mathcal{O}$) that could be either F or some true random function R. $\mathcal{A}$ will use $\mathcal{A}'$ to distinguish what is inside the oracle. Imagine $\mathcal{A}'$ lives inside $\mathcal{A}$, whenever $\mathcal{A}'$ sends a query to its oracle on some input m, $\mathcal{A}$ will answer that query by using his oracle access as follows:

- $\mathcal{A}$ casts m into $m0$ and $m1$ (by just appending 0 or 1 to m).
- $\mathcal{A}$ queries its oracle $\mathcal{O}$ with $m0$ and $m1$, then concatenates the result to create $\mathcal{O}(m0)||\mathcal{O}(m1)$ and then passes that to $\mathcal{A}'$ as the answer. Note that:
  - If $\mathcal{O} = F_k$, then $\mathcal{O}(m0)||\mathcal{O}(m1) = F_k(m0)||F_k(m1) = F'_k$
  - If $\mathcal{O} = R$, then $\mathcal{O}(m0)||\mathcal{O}(m1) = R(m0)||R(m1)$, which is some true random string of length $4n$ bits (say R').
- $\mathcal{A}$ continues to answer $\mathcal{A}'$ queries as above. At the end, $\mathcal{A}$ outputs whatever $\mathcal{A}'$ outputs (1 if $\mathcal{A}'$ thinks his oracle is F' or 0 if $\mathcal{A}'$ thinks his oracle is R').

It is clear that $\mathcal{A}$ is PPT since $\mathcal{A}'$ is PPT. Also, it is clear that both attackers have equal advantages (since $\mathcal{A}$ outputs whatever $\mathcal{A}'$ outputs).

By our assumption, $\mathcal{A}'$ is capable of distinguishing F' with non-negligible advantage. Since $\mathcal{A}$ simply outputs whatever $\mathcal{A}'$ outputs, $\mathcal{A}$ can distinguish F with the same non-negligible advantage. Therefore, $\mathcal{A}$ has successfully broken the PRF security of F. However, this is a contradiction; F is a secure PRF. Thus, our assumption is false, which means that F' is a secure PRF.

2. Let $F : \{0,1\}^n \to \{0,1\}^n$ be a PRF, construct $F' : \{0,1\}^n \to \{0,1\}^{2n}$ as

$$F'_k(m) = F_k(m)||F_k(F_k(m))$$

Solution

This scheme is insecure, we can build an attacker $\mathcal{A}'$ who is able to distinguish F' from a random function (say R') with non-negligible advantage. $\mathcal{A}'$ has an oracle access to an oracle $\mathcal{O}$, which is either F' or R'. Our attacker works as follows:

- $\mathcal{A}'$ queries $\mathcal{O}$ with m to receive $\mathcal{O}(m)$ as an output.
  - Let $x = \mathcal{O}(m)$, and let the first half of x be x_1 and the second half be x_2.
- $\mathcal{A}'$ queries $\mathcal{O}$ again with $m' = x_1$ (recall that if $\mathcal{O} = F'$ then $x_1 = F_k(m)$), receiving $\mathcal{O}(x_1)$ as an output.
  - Let $y = \mathcal{O}(x_1)$, and let the first half of y be y_1 and the second half be y_2.
- If $y_1 = x_2$ then $\mathcal{A}'$ outputs 1 (meaning that he thinks that $\mathcal{O}$ is F'), otherwise, he outputs 0 (meaning that he thinks that $\mathcal{O}$ is R'). Note that if $\mathcal{O} = F'$, then:
  - $\mathcal{O}(m) = F_k(m)||F_k(F_k(m))$

- $\mathcal{O}(x_1) = \mathcal{O}(F_k(m)) = F_k(F_k(m))||F_k(F_k(F_k(m)))$, where $y_1 = F_k(F_k(m))$.

So indeed $x_2 = y_1$ and hence, $\mathcal{A}'$ can distinguish F' with probability 1. However, if $\mathcal{O} = R$, then having these two parts equal happens with negligible probability given by $\frac{1}{2^n}$.

Clearly $\mathcal{A}'$ is a PPT attacker. We can now determine $\mathcal{A}'$s advantage in distinguishing F' as:

$$\begin{aligned}\varepsilon^{PRF}_{\mathcal{A}',F'}(n) &= \Pr[\mathcal{A}'^{F'_k}(n) = 1] - \Pr[\mathcal{A}'^{R'}(n) = 1]\\ &= 1 - \frac{1}{2^n} \notin NEGL(n)\end{aligned}$$

Therefore, *F'* is not a secure PRF.