18-330 Cryptography Notes: Pseudorandomness

Note: This is provided as a resource and is not meant to include all material from lectures or recitations. The proofs shown, however, are good models for your homework and exams.

1 PRF Security

Let function $F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ be a function that satisfies these conditions:

- F is deterministic
- $\forall k \in \mathcal{K}, \forall x \in \mathcal{X}$, $F(k, x)$ can be computed in polynomial time (in $\log |\mathcal{K}|$).

To evaluate whether F is a secure PRF, we must first define what security means. We do so via the following game (or experiment) $Exp_{A,F}$, which is parameterized by the adversary A and the (alleged) PRF F.

1. The experiment takes as input bit $b \in \{0, 1\}$, chosen uniformly at random.
2. If b is 0, then the Challenger samples k from $\mathcal{K}$ uniformly at random and sets $f(x) := F(k, x)$. Note that f remains the same for the rest of the experiment.
3. If b is 1, then the Challenger samples f, uniformly at random, from the space of all functions from $\mathcal{X}$ to $\mathcal{Y}$. Note that f remains the same for the rest of the experiment.
4. The Adversary runs some logic in order to select $x \in \mathcal{X}$.
5. The Adversary sends the chosen x to the Challenger.
6. The Challenger replies with $f(x)$ as defined above (i.e., either the result of applying the PRF with the chosen k, or the result of applying the randomly selected function).
7. Repeat steps 4 through 6 up to some $poly(log|\mathcal{K}|)$ number of times.
8. Finally, the Adversary runs some logic in order to choose $b' \in \{0, 1\}$, which is the output of the experiment.

Definition 1. *The PRF advantage $Adv_{PRF}[A, F, q]$ is defined as:*

$$Adv_{PRF}[A, F] := |Pr[b' = 1 \mid b = 0] - Pr[b' = 1 \mid b = 1]|$$

where A makes at most q queries.

Definition 2. *We say that F is a secure PRF if, for all efficient A, $Adv_{PRF}[A, F, q] < \epsilon$, for some small (negligible) ϵ.*

1.1 PRF Proof of Security

Let $F : \mathcal{K} \times \mathcal{X} \to \{0,1\}^{128}$ be a secure PRF. We show that $G(k,x) = (F(k,x) + 42) \mod 2^{128}$ is also a secure PRF.

Proof. Suppose for sake of contradiction that G is not a secure PRF. Then there must exist an efficient adversary A_G that breaks G. We can then construct an adversary A_F that breaks F. We define A_F as follows:

Algorithm 1: Adversary A_F

Execute A_G
while *Receive query for* $q \in \mathcal{X}$ *from* A_G **do**
    Query $Challenger_F$ with q and receive response r.
    Return $(r + 42) \mod 2^{128}$ to A_G.
end
When A_G outputs a guess b', output b' as the guess for A_F.

We prove that A_F is an efficient adversary that breaks F (i.e., wins the PRF security game with F a non-negligible amount of the time).

First, we argue that our adversary A_F perfectly simulates the challenger for A_G. If A_F is playing in experiment 0 (i.e., A_F is interacting with the PRF), then A_F's response to each of A_G's queries is exactly the definition of G. If A_F is playing in experiment 1 (i.e., A_F is interacting with a truly random function), then the response r it receives is randomly selected. A random value offset by 42 (mod 2^{128}) is still random, so A_F returns a randomly selected value to A_G. Therefore, we have correctly simulated the PRF game in A_F's interactions with A_G.

Now, we calculate the advantage of A_F.

$$Adv_{PRF}[A,F] == |Pr[b'_F = 1 \mid b = 0] - Pr[b'_F = 1 \mid b = 1]| \tag{1}$$

$$Adv_{PRF}[A,F] == |Pr[b'_G = 1 \mid b = 0] - Pr[b'_G = 1 \mid b = 1]| \tag{2}$$

$$Adv_{PRF}[A,F] == Adv_{PRF}[A,G] \tag{3}$$

Where the first step is justified by the reasoning above; namely, the probability that A_F outputs 1 when running in Experiment 0 is exactly that of A_G, and similarly for Experiment 1. The second step is just applying the definition of Adv_{PRF} to G.

Since we assumed G is not a secure PRF, it must be the case that $Adv_{PRF}[A,G]$ is large, which means that $Adv_{PRF}[A,F]$ is large (by Equation 3 above). But that means F is not a secure PRF, and yet we know F is a secure PRF (because that was given in the problem statement), so we have arrived at a contradiction. This means our assumption that G is insecure must be false. Hence G is a secure PRF. □

2 PRP Security

The definition of a secure PRP is nearly identical to that for PRF, except that everywhere we previously mentioned a function, we now work with a permutation. Changes relative to the PRF definition are highlighted below.

Let function $F : \mathcal{K} \times \mathcal{X} \rightarrow \mathcal{X}$ be a function that satisfies these conditions:

- F is deterministic
- $\forall k \in \mathcal{K}, \forall x \in \mathcal{X}$, $F(k, x)$ can be computed in polynomial time.
- $\forall k \in \mathcal{K}$, $F(k, x)$ is a *permutation* (i.e., it is bijective).

To evaluate whether F is a secure PRP, we must first define what security means. We do so via the following game (or experiment) $Exp_{A,F}$, which is parameterized by the adversary A and the (alleged) PRP F.

1. The experiment takes as input bit $b \in \{0, 1\}$, chosen uniformly at random.
2. If b is 0, then the Challenger samples k from $\mathcal{K}$ uniformly at random and sets $f(x) := F(k, x)$. Note that f remains the same for the rest of the experiment.
3. If b is 1, then the Challenger samples f, uniformly at random, from the space of all *permutations* from $\mathcal{X}$ to $\mathcal{X}$. Note that f remains the same for the rest of the experiment.
4. The Adversary runs some logic in order to select $x \in \mathcal{X}$.
5. The Adversary sends the chosen x to the Challenger.
6. The Challenger replies with $f(x)$ as defined above (i.e., either the result of applying the PRP with the chosen k, or the result of applying the randomly selected function).
7. Repeat steps 4 through 6 up to some $poly(log|\mathcal{K}|)$ number of times.
8. Finally, the Adversary runs some logic in order to choose $b' \in \{0, 1\}$, which is the output of the experiment.

Definition 3. *The PRP advantage $Adv_{PRP}[A, F, q]$ is defined as:*

$$Adv_{PRP}[A, F, q] := |Pr[b' = 1 \mid b = 0] - Pr[b' = 1 \mid b = 1]|$$

where A makes at most q queries.

Definition 4. *We say that F is a secure PRP if, for all efficient A, $Adv_{PRP}[A, F, q] < \epsilon$.*