Introduction to Cryptography 08 February 2018

Lecture 8: Pseudorandomness II

Instructor: Vipul Goyal *Scribe: Brad Denby*

1 Definition of a Pseudorandom Generator

Recall from the Lecture 6 the definition of a pseudorandom generator (PRG).

Definition 1 (Pseudorandom Generator) *A pseudorandom generator is a deterministic function $G : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ with the following properties:*

(i) G is computable in polynomial time

(ii) $\ell(n) > n$

(iii) $\{G(s) | s \xleftarrow{\$} \{0,1\}^n\} \approx_C \{u | u \xleftarrow{\$} \{0,1\}^{\ell(n)}\}$, i.e. $G(U_n)$ and $U_{\ell(n)}$ are computationally indistinguishable.

As a reminder, computational indistinguishability is defined as follows:

Definition 2 (Computational Indistinguishability) *Two ensembles $\{X_n\}$ and $\{Y_n\}$ are computationally indistinguishable, i.e $\{X_n\} \approx_C \{Y_n\}$, when for all adversaries $\mathcal{A}$ there exists a negligible function $\varepsilon_{\mathcal{A}}(n)$ such that $|\mathbb{P}[x \leftarrow X_n : \mathcal{A}(x) = 1] - \mathbb{P}[y \leftarrow Y_n : \mathcal{A}(y) = 1]| \le \varepsilon_{\mathcal{A}}(n)$.*

2 Construction of a PRG

Recall from Lecture 3 that a (strong) one way function (OWF) is (i) "easy" to compute and (ii) "difficult" to invert.

Definition 3 (One Way Function) *A function $f : \{0,1\}^n \to \{0,1\}^m$ is a OWF when*

(i) there exists a PPT algorithm $\mathcal{C}$ s.t. $\forall x \in \{0,1\}^n$ it is the case that $\mathbb{P}[\mathcal{C}(x) = f(x)] = 1$, and

(ii) there exists a negligible function ε such that for every PPT adversary $\mathcal{A}$ and $\forall n \in \mathbb{N}$ it is the case that $\mathbb{P}[x \xleftarrow{\$} \{0,1\}^n, x' \leftarrow \mathcal{A}(f(x)) : f(x) = f('x)] \le \varepsilon(n)$.

Let $f : \{0,1\}^n \to \{0,1\}^m$ be a one way function. A predicate $h : \{0,1\}^m \to \{0,1\}$ is a function with a single bit output. Recall from Lecture 5 that h is a hard core predicate (HCP) for OWF f when (i) h is computable in polynomial time and (ii) for some input x the probability of determining $h(x)$ given $f(x)$ is negligibly more than random chance.

Definition 4 (Hard Core Predicate) *Let $f : \{0,1\}^n \to \{0,1\}^m$ be a OWF. Let $h : \{0,1\}^m \to \{0,1\}$ be a predicate. Then h is a hard core predicate for f when*

(i) h is computable in polynomial time, and

(ii) there exists a negligible function ε such that for every PPT adversary $\mathcal{A}$ and $\forall n \in \mathbb{N}$ it is the case that $\mathbb{P}[x \xleftarrow{\$} \{0,1\}^n : \mathcal{A}(f(x)) = h(x)] \le \varepsilon(n)$.

It seems that, for a OWF f and a HCP h of f, the construction $f(s)||h(s)$ might be a good candidate for a PRG $G(s)$. By definition $h(s)$ is difficult to guess and therefore "uniform." However, $f(s)$ is not necessarily uniform; it is only required to be difficult to invert. Further, $|f(s)| = m$ while $|s| = n$. If $m < n$, then the PRG condition that $\ell(n) > n$ is not satisfied.

To resolve this issue, let f be a one way permutation (OWP) instead of a OWF. A one way permutation is a bijective one way function such that every image has a pre-image that is unique. As a result, the domain and the range for a OWP are equal in magnitude. One way permutations will be explored in more detail during a future lecture. For now, note that a one way permutation $f : \{0,1\}^n \to \{0,1\}^n$ satisfies the condition that $\{f(s)|s \xleftarrow{\$} \{0,1\}^n\} \approx_C \{u|u \xleftarrow{\$} \{0,1\}^n\}$.

Given these elements, it is now possible to construct a PRG G. Let $f : \{0,1\}^n \to \{0,1\}^n$ be a one way permutation, and let $h : \{0,1\}^n \to \{0,1\}$ be a hard core predicate for f. Construct the pseudorandom generator $G : \{0,1\}^n \to \{0,1\}^{n+1}$ such that $\forall s \in \{0,1\}^n$ it is the case that $G(s) = f(s)||h(s)$.

Construction 1 *Let $f : \{0,1\}^n \to \{0,1\}^n$ be a one way permutation, and let $h : \{0,1\}^n \to \{0,1\}$ be a hard core predicate for f. Construct $G : \{0,1\}^n \to \{0,1\}^{n+1}$ such that $\forall s \in \{0,1\}^n$ it is the case that $G(s) = f(s)||h(s)$.*

Next, it must be shown that Construction 1 satisfies Definition 1 of a pseudorandom generator. This fact is expressed in **Theorem 4**, and it is proven using the following three Lemmas. First, note that $\forall s \in \{0,1\}^n$ it is the case that $G(s)$ is deterministic because $f(s)$, $h(s)$, and concatenation are deterministic. Showing properties (i) and (ii) of Definition 1 is similarly direct.

Lemma 1 *Construction 1 satisfies Definition 1 (i), i.e. G is computable in polynomial time.*

Proof. It is the case that $\forall s \in \{0,1\}^n$ the function G is constructed to be the concatenation of $f(s)$ and $h(s)$, i.e. $G(s) = f(s)||h(s)$. By definition, $\forall s \in \{0,1\}^n$ it is the case that OWP $f(s)$ and HCP $h(s)$ are each computable in polynomial time. For input $|s| = n$, outputs $|f(s)| = n$ and $|h(s)| = 1$. Thus, the concatenation is computable in polynomial time $\forall s \in \{0,1\}^n$. Therefore, G is computable in polynomial time. ■

Lemma 2 *Construction 1 satisfies Definition 1 (ii), i.e. $\ell(n) > n$*

Proof. The function G is constructed to be the concatenation of $f(s)$ and $h(s)$. By definition, $\forall s \in \{0,1\}^n$ it is the case that $|f(s)| = n$ and $|h(s)| = 1$. Thus, $\forall s \in \{0,1\}^n$ it is the case that $|G(s)| = |f(s)||h(s)| = n + 1 > n$. Therefore, $\ell(n) > n$. ■

Property (iii) of Definition 1 requires that $\{G(s)|s \xleftarrow{\$} \{0,1\}^n\} \approx_C \{u|u \xleftarrow{\$} \{0,1\}^{\ell(n)}\}$, i.e. $G(U_n)$ and U_{n+1} are computationally indistinguishable for this construction. Before proceeding to the proof for this property, consider the following insight.

Suppose there exists an adversary $\mathcal{B}$ that distinguishes between $\{G(U_n)\}$ and $\{U_{n+1}\}$. Then it would be possible to construct an adversary $\mathcal{A}$ that calls $\mathcal{B}$ in order to distinguish either $f(s)$ or $h(s)$ from random. By the contrapositive, if there does not exist an adversary $\mathcal{A}$ that can distinguish either $f(s)$ or $h(s)$ from random, then there does not exist an adversary $\mathcal{B}$ that can distinguish between $\{G(U_n)\}$ and $\{U_{n+1}\}$. Due to the properties of OWPs and HCPs, the antecedent is known to be true. Thus, the consequent is true. The remainder of this lecture provides a formalization of this proof sketch.

Lemma 3 *Construction 1 satisfies Definition 1 (iii), i.e.* $\{G(s)|s \xleftarrow{\$} \{0,1\}^n\} \approx_C \{u|u \xleftarrow{\$} \{0,1\}^{\ell(n)}\}$.

Proof. By Definition 2, $\{G(s)|s \xleftarrow{\$} \{0,1\}^n\} \approx_C \{u|u \xleftarrow{\$} \{0,1\}^{n+1}\}$ requires that for all adversaries $\mathcal{A}$ there exists a negligible function $\varepsilon_{\mathcal{A}}(n)$ such that

$$|\mathbb{P}[s \xleftarrow{\$} \{0,1\}^n : \mathcal{A}(G(s)) = 1] - \mathbb{P}[u \xleftarrow{\$} \{0,1\}^{n+1} : \mathcal{A}(u) = 1]| \leq \varepsilon_{\mathcal{A}}(n).$$

This property will be shown using a hybrid argument. In particular, it will first be shown that $G(s) = f(s)||h(s)$ and $f(s)||b$, where b is an ideally uniform bit, are computationally indistinguishable. It will then be shown that $f(s)||b$ and $u||b$, where u is an ideally uniform string, are computationally indistinguishable. These results together give the conclusion that $G(U_n) \approx_C U_{n+1}$.

Let $\mathcal{B}$ be an adversary, and define the following experiments:

- Let H_0 be an experiment where $\mathcal{B}$ is given input $G(s)$ and $p_0 = \mathbb{P}[s \xleftarrow{\$} \{0,1\}^n : \mathcal{B}(G(s)) = 1]$.
- Let H_1 be an experiment in which $\mathcal{B}$ is given $f(s)||b$ as input, where b is drawn uniformly at random from $\{0,1\}$, and $p_1 = \mathbb{P}[s \xleftarrow{\$} \{0,1\}^n, b \xleftarrow{\$} \{0,1\} : \mathcal{B}(f(s)||b) = 1]$.

Require that $p_0 > p_1$; if not, construct a new $\mathcal{B}$ that outputs the complement of the original $\mathcal{B}$.

Claim: $|p_0 - p_1| \leq \varepsilon_{\mathcal{B}}(n)$
Suppose not, i.e. there exists an adversary $\mathcal{B}$ such that for all negligible functions $\varepsilon(n)$ it is the case that

$$\mathbb{P}[s \xleftarrow{\$} \{0,1\}^n : \mathcal{B}(f(s)||h(s)) = 1] - \mathbb{P}[s \xleftarrow{\$} \{0,1\}^n, b \xleftarrow{\$} \{0,1\} : \mathcal{B}(f(s)||b) = 1] > \varepsilon(n).$$

Note that

$$\mathbb{P}[s \xleftarrow{\$} \{0,1\}^n, b \xleftarrow{\$} \{0,1\} : \mathcal{B}(f(s)||b) = 1] =$$
$$\mathbb{P}[s \xleftarrow{\$} \{0,1\}^n : \mathcal{B}(f(s)||h(s)) = 1]\mathbb{P}[b = h(s)] + \mathbb{P}[s \xleftarrow{\$} \{0,1\}^n : \mathcal{B}(f(s)||\overline{h(s)}) = 1]\mathbb{P}[b = \overline{h(s)}] =$$
$$\frac{1}{2}(\mathbb{P}[s \xleftarrow{\$} \{0,1\}^n : \mathcal{B}(f(s)||h(s)) = 1] + \mathbb{P}[s \xleftarrow{\$} \{0,1\}^n : \mathcal{B}(f(s)||\overline{h(s)}) = 1]).$$

As a result,

$$\mathbb{P}[s \xleftarrow{\$} \{0,1\}^n : \mathcal{B}(f(s)||h(s)) = 1] - \mathbb{P}[s \xleftarrow{\$} \{0,1\}^n : \mathcal{B}(f(s)||\overline{h(s)}) = 1] > 2\varepsilon(n).$$

Now construct and adversary $\mathcal{A}$ that takes $f(s)$ as input and generates $b' \xleftarrow{\$} \{0,1\}$. Adversary $\mathcal{A}$ calls $\mathcal{B}(f(s)||b')$. Construct $\mathcal{A}$ to return b' when $\mathcal{B}(f(s)||b') = 1$ and to return a randomly sampled bit b'' otherwise. The probability that $\mathcal{A}$ successfully returns the hard core bit $h(s)$ is given by:

$$\mathbb{P}[\mathcal{A} \text{ returns correct } h(s)] =$$
$$\mathbb{P}[b' \text{ correct } \wedge \mathcal{B} = 1] + \mathbb{P}[b'' \text{ correct } \wedge \mathcal{B} = 0] =$$
$$\mathbb{P}[\mathcal{B} = 1|b' \text{ correct}]\mathbb{P}[b' \text{ correct}] + \mathbb{P}[b'' \text{ correct}|\mathcal{B} = 0]\mathbb{P}[\mathcal{B} = 0] =$$
$$\mathbb{P}[\mathcal{B} = 1|b' \text{ correct}]\mathbb{P}[b' \text{ correct}] + \mathbb{P}[b'' \text{ correct}|\mathcal{B} = 0](1 - \mathbb{P}[\mathcal{B} = 1]) >$$
$$\frac{1}{2}p_0 + \frac{1}{2}(1 - p_0 + \varepsilon(n)) = \frac{1}{2} + \varepsilon(n)$$

Thus, for all negligible functions $\varepsilon(n)$ it is the case that $\mathbb{P}[\mathcal{A}$ returns correct $h(s)] > \frac{1}{2}+\varepsilon(n)$, which means that there exists an adversary $\mathcal{A}$ with non-negligible prediction advantage. By the contrapositive, if for all adversaries $\mathcal{A}$ it is the case that the prediction advantage for the HCP $h(s)$ is negligible, then it must be the case that H_0 and H_1 are computationally indistinguishable. The antecedent is known to be true; therefore, the claim $|p_0 - p_1| \leq \varepsilon_{\mathcal{B}}(n)$ for arbitrary $\mathcal{B}$ holds.

Finally, define the following experiment:

- Let H_2 be an experiment in which $\mathcal{B}$ is given $u = u'||b$ as input, where u' is drawn uniformly at random from $\{0,1\}^n$, b is drawn uniformly at random from $\{0,1\}$, and the probability $p_2 = \mathbb{P}[u \xleftarrow{\$} \{0,1\}^{n+1} : \mathcal{B}(u) = 1]$.

Claim: $|p_2 - p_1| = 0$
The key insight supporting this claim is that $f(s)$ is a OWP, and the input s is selected uniformly at random. Thus, the output $f(s)$ is indistinguishable from a string u selected uniformly at random.

Formally, note that $p_2 - p_1$ may be written as:

$$\mathbb{P}[u \xleftarrow{\$} \{0,1\}^{n+1} : \mathcal{B}(u) = 1] - \mathbb{P}[s \xleftarrow{\$} \{0,1\}^n, b \xleftarrow{\$} \{0,1\} : \mathcal{B}(f(s)||b) = 1].$$

Using the law of total probability,

$$\begin{aligned}
&\mathbb{P}[u \xleftarrow{\$} \{0,1\}^{n+1} : \mathcal{B}(u) = 1] - \mathbb{P}[s \xleftarrow{\$} \{0,1\}^n, b \xleftarrow{\$} \{0,1\} : \mathcal{B}(f(s)||b) = 1] = \\
&\sum_{s' \in \{0,1\}^{n+1}} \mathbb{P}[B(u) = 1]\mathbb{P}[u = s'] - \sum_{x' \in \{0,1\}^n, b' \in \{0,1\}} \mathbb{P}[B(y||b) = 1]\mathbb{P}[y = f(x')]\mathbb{P}[b = b'] = \\
&\frac{1}{2^{n+1}} \sum_{s' \in \{0,1\}^{n+1}} \mathbb{P}[B(u) = 1] - \frac{1}{2^n}\frac{1}{2} \sum_{x' \in \{0,1\}^n, b' \in \{0,1\}} \mathbb{P}[B(y||b) = 1]
\end{aligned}$$

To see why, note that the probability of $s' \in \{0,1\}^{n+1}$ matching some $u \in \{0,1\}^{n+1}$ is $1/2^{n+1}$; the probability of $y \in \{0,1\}^n$ matching some output of a OWP is $1/2^n$; and the probability of a single bit b' matching a bit b is $1/2$ for elements selected uniformly at random.

Since $\mathbb{P}[B(u) = 1]$ and $\mathbb{P}[B(y||b) = 1]$ are conceptually equivalent, then

$$\begin{aligned}
&\frac{1}{2^{n+1}} \sum_{s' \in \{0,1\}^{n+1}} \mathbb{P}[B(u) = 1] - \frac{1}{2^n}\frac{1}{2} \sum_{x' \in \{0,1\}^n, b' \in \{0,1\}} \mathbb{P}[B(y||b) = 1] = \\
&\frac{1}{2^{n+1}} \sum_{s' \in \{0,1\}^{n+1}} \mathbb{P}[B(u) = 1] - \frac{1}{2^{n+1}} \sum_{x' \in \{0,1\}^n, b' \in \{0,1\}} \mathbb{P}[B(y||b) = 1] = 0
\end{aligned}$$

Thus, the claim $|p_2 - p_1| = 0$ holds.

Combining these claims in the form of a hybrid argument gives the desired result. Specifically, $|p_0 - p_1| \leq \varepsilon(n)$ and $|p_2 - p_1| = 0$ implies that H_0 and H_2 are computationally indistinguishable. Therefore, $\{G(s) | s \xleftarrow{\$} \{0,1\}^n\} \approx_C \{u | u \xleftarrow{\$} \{0,1\}^{n+1}\}$. ■

In summary, Lemma 1 has shown that Construction 1 satisfies Definition 1 (i); Lemma 2 has shown that Construction 1 satisfies Definition 1 (ii); and Lemma 3 has shown that Construction 1 satisfies Definition 1 (iii). With these Lemmas, it is now possible to show that Construction 1 satisfies the entire definition of a pseudorandom generator.

Theorem 4 *Construction 1 satisfies the definition of a pseudorandom generator.*

Proof. Let $f : \{0,1\}^n \to \{0,1\}^n$ be a one way permutation, and let $h : \{0,1\}^n \to \{0,1\}$ be a hard core predicate for f. Construct $G : \{0,1\}^n \to \{0,1\}^{n+1}$ such that $\forall s \in \{0,1\}^n$ it is the case that $G(s) = f(s)||h(s)$. Recall from before that $\forall s \in \{0,1\}^n$ it is the case that $G(s)$ is deterministic because $f(s)$, $h(s)$, and concatenation are deterministic. By Lemma 1, G is computable in polynomial time. By Lemma 2, the magnitude of the range is strictly larger than the magnitude of the domain. By Lemma 3, the output of G is computationally indistinguishable from uniformly random samples. Therefore, $G(s) = f(s)||h(s)$ is a pseudorandom generator. ■

3 Looking Ahead

Given a construction of a PRG that stretches the domain by one bit, it would be nice to build PRGs with much longer outputs for the same input length. For an input length of n, it is desirable to construct PRGs with an output length of $n+2$, $n+3$, or even n^{100} for example. Intuitively, such constructions should be possible by iteratively applying Construction 1.

Construction 2 *Let $G : \{0,1\}^n \to \{0,1\}^{n+1}$ be a pseudorandom generator. The pseudorandom generator $G' : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ may be constructed as follows. Select a seed $s_n \in \{0,1\}^n$ and apply $G_n(s_n)$ in order to obtain s_{n+1}. Apply the one bit stretch PRG to this output, i.e. calculate $G_{n+1}(s_{n+1})$. Continue this process until $G_n(s_{\ell(n)})$.*

One danger of this construction lies with the initial seed s_n; this seed must be kept private. Additionally, this construction is not necessarily the most efficient way to produce a pseudorandom generator that stretches the input by more than one bit. A proof for this construction is deferred to Lecture 8.