CS 600.442 – Modern Cryptography September 14, 2015

Lecture 4: Pseudorandomness - I

Instructor: Abhishek Jain *Scribe: Ivan Solano*

1 Distinguishing vs Prediction

Definition 1 (Prediction Advantage for Adversary A) *The prediction Advantage of an adversary A for ensembles $\{X_n^0\}, \{X_n^1\}$ is defined as*

$$Pr[b \xleftarrow{\$} \{0,1\}, t \leftarrow X_n^b : A(t) = b] - \frac{1}{2}$$

Definition 2 (Prediction Advantage) *For ensembles $\{X_n^0\}, \{X_n^1\}$ and all adversaries A, the prediction advantage is defined as*

$$\max_A Pr[b \xleftarrow{\$} \{0,1\}, t \leftarrow X_n^b : A(t) = b] - \frac{1}{2}$$

Here, a challenger chooses a random bit b. He then samples the corresponding ensemble, and gives the value to the adversary. The adversary then has to guess b. Note that he could always guess with probability $\frac{1}{2}$ just by choosing a random bit.

Compare this definition to Computational Indistinguishability, and try to prove how a negligible prediction advantage is equivalent to computational indistinguishability of $\{X_n^0\}, \{X_n^1\}$.

Lemma 1 (Prediction Lemma) *Let $\{X_n^0\}, \{X_n^1\}$ be ensembles of probability distributions. Let D be a n.u. PPT that $\epsilon(.)$-distinguishes $\{X_n^0\}, \{X_n^1\}$ for infinitely many $n \in \mathbb{N}$. Then, $\exists$ n.u. PPTA s.t.*

$$Pr[b \xleftarrow{\$} \{0,1\}, t \leftarrow X_n^b : A(t) = b] - \frac{1}{2} \geq \frac{\epsilon(n)}{2}$$

for infinitely many $n \in \mathbb{N}$.

Proof. We can construct a $PPTA$ that uses distinguisher D to predict b. The construction is simple, it would just receive input t and feed as input to distinguisher D and output whatever D outputs. The prediction advantage of A will then be

$$\begin{aligned}
&Pr[b \xleftarrow{\$} \{0,1\}, t \leftarrow X_n^b : D(t) = b] - \frac{1}{2} \\
&= \frac{1}{2}(Pr[t \leftarrow X_n^1 : D(t) = 1] + Pr[t \leftarrow X_n^0 : D(t) \neq 1]) - \frac{1}{2} \\
&= \frac{1}{2}(Pr[t \leftarrow X_n^1 : D(t) = 1] + 1 - Pr[t \leftarrow X_n^0 : D(t) = 1]) - \frac{1}{2} \\
&= \frac{1}{2} + \frac{1}{2}(Pr[t \leftarrow X_n^1 : D(t) = 1] - Pr[t \leftarrow X_n^0 : D(t) = 1]) - \frac{1}{2} \geq \frac{\epsilon(n)}{2}
\end{aligned}$$

2 Pseudorandom Distributions

How to test that a string is "random-looking"? Some examples of possible tests include having roughly the same number of 0s and 1s, roughly the same numbers of 00s and 11s. Given any prefix, it should be hard to predict the next bit and sequence. For a pseudorandom string we want one that can pass all possible efficient (polynomial) tests.

Intuition. A distribution is pseudorandom if it "looks like" the uniform distribution to any efficient test. $U_{\ell(n)}$ denotes the uniform distribution over $\{0,1\}^{\ell(n)}$.

Definition 3 (Pseudorandom Ensembles) *An ensemble $\{X_n\}$, where X_n is a distribution over $\{0,1\}^{\ell(n)}$, is said to be pseudorandom if:*

$$\{X_n\} \approx U_{\ell(n)}$$

The main question now is how can we show indistinguishability against all efficient tests? To answer this question, we will identify a "complete" test, namely, next-bit unpredictability.

3 Next-bit Unpredictability

Definition 4 (Next-bit Unpredictability) *An ensemble of distributions $\{X_n\}$ over $\{0,1\}^{\ell(n)}$, is next-bit unpredictable if, for all $0 \leq i, \ell(n)$ and n.u. PPT A, $\exists$ negligible function $v(.)$ s.t.*

$$Pr[t = t_1 t_2 \dots t_{\ell(n)} \leftarrow: A(t_1 t_2 \dots t_i) = t_{i+1}] \leq \frac{1}{2} + v(n)$$

Theorem 2 (Completeness of Next-bit Test) *If $\{X_n\}$ is next-bit unpredictable, then $\{X_n\}$ is pseudorandom.*

Proof. Consider the hybrids

$$H_n^{(i)} := \{x \leftarrow X_n, u \leftarrow U_n : x_1 \dots x_i u_{i+1} \dots u_{\ell(n)}\}$$

- The first hybrid, H_n^0 is the uniform distribution
- The last hybrid, $H_n^{\ell(n)}$ is the distribution X_n

Suppose the distribution is next-bit unpredictable but not pseudorandom. We have that H_n^0 and $H_n^{\ell(n)}$ are distinguishable by an adversary D with a non-negligible probability $\epsilon(n)$. Then by the **hybrid lemma**, $\exists\ i \in [\ell(n) - 1]$ s.t. H_n^i and H_n^{i+1} are $\frac{\epsilon(n)}{\ell(n)}$-distinguishable, which is also non-negligible, and next-bit unpredictability would be violated.

4 Pseudorandom Generator

It would be convenient to be able to generate pseudorandom distributions using only a few random bits. A pseudorandom generator is a function that "stretches" n truly random bits into $\ell(n)$ pseudorandom bits.

Definition 5 (Pseudorandom Generator) *A pseudorandom generator (PRG) $G : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ is an efficiently computable function, where $\ell(.)$ is a suitable polynomial s.t. $\ell(n) > n$, such that:*

$$\{G(U_n)\} \approx U_{\ell(n)}$$

In order to build PRGs, we are going to first introduce the notion of Hardcore predicates.

4.1 Hardcore Predicate

Intuition. $h(.)$ is a hardcore predicate for a **one-way function** f if $h(x)$ is hard to predict even if $f(x)$ is given to the adversary.

Definition 6 (Hardcore Predicate) *The predicate $h : \{0,1\}^n \to \{0,1\}$ is hardcore for $f : \{0,1\}^n \to \{0,1\}^m$ if $\forall n.u.PPT$ adversary A, $\exists$ non-negligible function $\mu(.)$ s.t.*

$$Pr[x \xleftarrow{\$} \{0,1\}^n : A(1^n, f(x)) = h(x)] \leq \frac{1}{2} + \mu(n)$$

Now that we have defined hardcore predicates, we can use them to construct PRGs.

4.2 Construction of PRGs

The construction of a PRG from a hardcore predicate can be done in three steps. In this lecture we will only cover in detail steps 2 and 3.

- Step 1: OWF (OWP) $\Longrightarrow$ Hardcore Predicate for OWF (OWP)
- Step 2: Hardcore Predicate for OWF (OWP) $\Longrightarrow$ one-bit stretch PRG
- Step 3: One-bit stretch PRG $\Longrightarrow$ Poly-stretch PRG

4.3 Step 2: One-bit Stretch PRG from OWP

Given a one-way permutation $f : \{0,1\}^n \to \{0,1\}^n$ and a hardcore predicate $h : \{0,1\}^n \to \{0,1\}$, to perform a one-bit stretch G it suffices to append the hardcore predicate to the result of the permutation.

$$G(s) = f(s) \,||\, h(s)$$

Here, s is a random string with uniform distribution. Since f is a one-way permutation $f(s)$ also has uniform distribution, therefore an adversary cannot predict any digit of $f(s)$. Now $h(s)$ cannot be predicted given the first n bits by the definition of hardcore predicate, so it maintains next-bit unpredictability. Thus the one-bit stretch is still pseudorandom.

4.4 Step 3: Poly-stretch PRG from One-bit stretch PRG

Intuition. To build a poly-stretch PRG, we iterate a one-bit stretch PRG poly number of times.

Construction of $G_{poly} : \{0,1\}^n \to \{0,1\}^{\ell(n)}$:

- Let $G_1 : \{0,1\}^n \to \{0,1\}^{n+1}$ be a one-bit stretch
- Let $X_0 = s$
- $X_1 \,||b_1 \leftarrow G_1(X_0)$
- $X_2 \,||b_2 \leftarrow G_1(X_1)$
- $X_3 \,||b_3 \leftarrow G_1(X_2)$
- $X_i \,||b_i \leftarrow G_1(X_{i-1})$
- $G_{poly}(s) := b_1 b_2 \ldots b_{\ell(n)}$

For the proof, use the hybrid lemma to show next-bit unpredictability.