CS403 · Cryptography and Network Security

Assignment 2

Yubin Hu / 11712121

November 2, 2020

1

Since $X_n \approx Y_n$, then for any polynomial-time algorithm A, we have:

$$|Pr[A(X_n) = 1] - Pr[A(Y_n) = 1]| \leq \epsilon(n)$$

For any polynomial-time algorithm A, we also have another algorithm A' since $A'(x) = A(f(x))$, sice f is a polynomial-time computable function, so:

$$|Pr[A'(X_n) = 1] - Pr[A'(Y_n) = 1]| \leq \epsilon(n)$$

$$|Pr[A(f(X_n)) = 1] - Pr[A(f(Y_n)) = 1]| \leq \epsilon(n)$$

therefore this means we have:

$$f(X_n) \approx f(Y_n)$$

2

2.1

We prove it by contraposition. Suppose the negligible function $negl_3$ is not negligible, which means:

$$\forall n,\ \exists p,\ negl_3(n) \geq \frac{1}{p(n)}$$

which p is a polynomial, then,

$$negl_1(n) \geq \frac{1}{2p(n)} \text{ or } negl_2(n) \geq \frac{1}{2p(n)}$$

We assume that $negl_1(n) \geq \frac{1}{2p(n)}$, then assume polynomial $p' = 2p$:

$$negl_1(n) \geq \frac{1}{p(n)}$$

which means $negl_1$ is not negligible function. Therefore it is contraposition, $negl_3$ is a negligible function.

2.2

We prove it by contraposition. Suppose the negligible function $negl_3$ is not negligible, which means:

$$\forall n,\ \exists q,\ negl_4(n) \geq \frac{1}{q(n)}$$

which p, q is a polynomial, then:

$$negl_1(n) \geq \frac{1}{p(n) \times q(n)}$$

then assume polynomial $q'(n) = p(n) \times q(n)$, then we have

$$negl_1(n) \geq \frac{1}{q(n)}$$

which means $negl_1$ is not negligible function. Therefore it is contraposition, $negl_4$ is a negligible function.

3

Suppose $p_{i,j} = Pr[A(E_{U_m}(x_i)) = j]$, we get $p_{i,0} + p_{i,1} + p_{i,2} = 1$. For each $i = 0, 1, 2$, we have $|p_{i,j} - p_{k,j}| \le \epsilon(n)$, where $i, j, k \in 0, 1, 2$, then $p_{k,j} \ge p_{j,i} - \epsilon$ for $k \ne j$. So $3 = \sum_{i=0}^{2} \sum_{j=0}^{2} P_{ij} \ge 3 \sum_{i=0}^{2} p_{i,i} - 3\epsilon(n)$ Thus, $\frac{1}{3} \sum_{i=0}^{2} p_{i,i} \le frac13 + frac13\epsilon(n) < 0.34$

4

4.1

No. We have that $|Pr_{x\leftarrow X_n}[A(x) = 1]| - Pr_{x\leftarrow U_n}[A(x) = 1] \le \epsilon(n)$ for every PPT distinguaisher A. However, there is a distinguaisher A, that output 1 when $x_n = x_1 \oplus x_2 \oplus ... \oplus x_n - 1$. $Pr_{x\leftarrow X_n}[A(x) = 1] = 1$ and $Pr_{x\leftarrow U_n}[A(x) = 1] = \frac{1}{2}$, so X_n is not pseudorandom.

4.2

Yes. With $1-2^{-n/10}$ probability Z_n have a random string, so we have $|Pr_{x\leftarrow Z_n}[A(x) = 1] - Pr_{x\leftarrow U_n}[A(x) = 1]| \le |2^{-n/10} - 2^{-n/10} \times Pr_{x\leftarrow U_n}[A(x) = 1]| \le 2^{-n/10}$. Since $2^{-n/10}$ is a negligible function, Z_n is pseudorandom.

5

5.1

Prove 2 first. Not necessary. We can prove $G'' = G(s_{n/2+1}...s_n)$ is a PRG. Assume G' is a PRG, we have $G'(s) = G''(s_0^{|s|}) = G(0^{|s|})$ is a PRG. By contradicted, it is not necessary.

5.2

Yes. We Suppose l, l' are the expansion factor of G, G'. Therefore $l(n) = |G(s)|$ and $l'(n) = |G(s_1...s_n n/2)| = l(\frac{n}{2})$, for any PPT distinguaisher A we have:

$$|Pr_{x\leftarrow U_n}[A()G'(x) = 1] - Pr_{y\leftarrow U_{l'(n)}}[A(y) = 1]| \le \epsilon(\frac{n}{2})$$

Then we prove $\epsilon'(n) = \epsilon(\frac{n}{2})$. We prove it by contraposition. Therefore, ϵ' is a negligible function and G' is a pseudorandom generator.

6

F_k is not a PRF. We construct a PPT distinguaisher, there are two arbitrary string x_0 and x_1 and $|x_0| = |x_1| = n$. Output 1 when $f(x_0) \oplus f(x_1) = x_0 \oplus x_1$ and outputs 0 otherwise. So the posibility for outputing 1 is 2^{-n} if f is a pseudorandom function. there is 1 when $f = F_k, k \leftarrow 0, 1^n$, so $|1 - 2^{-n}|$ is not a negligible function and F_k is not a PRF.

7

We prove it by contraposition. If G is not a PRG, which means there is a PPT distinguaisher D and a polynomial p.

$$|Pr_{k\leftarrow 0,1^n}[D(F_k(< 1 >)|F_k(< 2 >))|...|F_k(< l >) = 1] - Pr_{y\leftarrow(0,1)^{ln}}[D(y) = 1]| \ge p(n)$$

Then by the definition we have:

$$Pr_{y\leftarrow(0,1)^{ln}}[D(y) = 1] = Pr_{y\leftarrow(0,1)^{ln}}[D(f(< 1 >)|f(< 2 >))|...|f(< l >) = 1]$$

Therefore, there is an PPT distinguaisher D' for given function f' simply output the result of $D(f'(< 1 >)|f'(< 2 >))|...|f'(< l >)$. It is contradicted to distinguaish PRF F_k with the random function f. So G is a PRG.

8

Suppose that IV is a n-bit string, we can construct the adversary A. When query the encryption oracle with $m = 0^{n-1}1$ and we get the ciphertext $< IV, c >$. If IV is odd(last bit 1), output a random bit; If IV is even(last bit 0), output $m_0 = 0^n$ and arbitrary m_1 to be encrypted. Then Receive the challenge ciphertext $< IV + 1, c' >$, and output 0 if $c' = c$, and 1 otherwise.

We claim that this adversary succeeds with probability that is greater than $\frac{1}{2}$ by a nonnegligible function. By guessin randomly, A succeeds with probability $\frac{1}{2}$ if IV is odd, which is $\frac{1}{4}$. If IV is even, $IV+1 = IV \oplus 0^{n-1}$. Therefore, $c = F_k(IV \oplus m_0) = F_k(IV \oplus 0^{n-1}1) = F_k(IV+1) = F_K(IV+1 \oplus 0) = F_K(IV+1 \oplus m_0)$. If m_0 is encrypted, then $c = c'$. That is, whenever IVis even, A decides correctly which message was encrypted. This is $\frac{1}{2}$ cases. In total, A wins $\frac{3}{4}$ cases.