A0216695U Ng Jong Ray, Edward

2

Question 1
The output of $G(s) = l(n)$ where n is the security parameter. For $G\ l(n) = n$.
Based on the *Definition 3.14*, the expansion condition requires for $l(n) > n$ and since the expansion condition does not hold and therefore $G(s)$ is not a PRG. ▮

3

Question 2
The function $G'(s)$ will output a pseudorandom string using the PRG G with the of s' of length $n - 1$ by removing the most significant bit of s. The length of G', $l(n) = 2(n - 1)$
Let us define a randomly generated string r of length $l(n)$.
Suppose that G' is not a PRG and we can define a PPT Distinguisher D which when given a string, can efficiently and correctly determine if the given string is an output of $G'(s)$. D can do so as $Pr[D(G'(s)) = 1] \geq \frac{1}{2} + negl(n)$. Since G' is constructed using G, this implies that $G(s')$ is not a PRG which contradicts that G is a PRG. This therefore proves that G' is also a PRG. ▮

0

Question 3
$2^4 \times 2^4 = 256$

Question 4
Using direct proof:

4

Suppose that G is not a PRG, this means that we can create a Distinguisher D which run in PPT, is able to differentiate G from r, a truly random string, with a probability of more than negligible.

The distinguisher D: Given an input string w of size $l(n)$,

$Pr[D(G(s)) = 1] \geq \frac{1}{2} + negl(n)$ and $Pr[D(r) = 1] \leq \frac{1}{2} + negl(n)$

Thus, $Pr[D(G(s)) = 1] - Pr[D(r) = 1] \geq negl(n)$

In the Construction 3.17,
We now define an PPT adversary A that is able to use D as a subroutine in the game $PrivK^{eav}_{A,\pi}(n, b)$.
The adversary A can choose 2 messages, m_0 and m_1 to as input for the game. The adversary would be able to choose $m_0 = \{0\}^n$ and $m_1 = \{0, 1\}^n$. The challenger that randomly chooses to encrypt either m_0 or m_1 and that choice will be $b = \{0, 1\}$. The adversary receiving back the ciphertext, $c = m_b \otimes G(s)$ will then use $D(c)$. If m_0 is chosen, $D(c) = D(m_0 \otimes G(s)) = D(G(s))$. Since the encrypted m_0 would just be reduced G, $Pr[D(G(s)) = 1] \geq \frac{1}{2} + negl(n)$.
Meanwhile, if m_1 is chosen, $D(c) = D(m_1 \otimes G(s))$ and $Pr[D(m_1 \otimes G(s)) = 1] \leq \frac{1}{2} + negl(n)$ as the distinguisher would not not be able to tell efficiently that it the ciphertext is from $G(s)$.
Therefore, $Pr[PrivK^{eav}_{A,\pi}(n, 0) = 1] - Pr[PrivK^{eav}_{A,\pi}(n, 1) = 1]$
$= Pr[D(G(s)) = 1] - Pr[D(m_1 \otimes G(s)) = 1] \geq negl(n)$ indicating if G is not a PRG that the adversary would be able to win the eavesdropper security game with a probability greater than negligible, thus it cannot be EAV-secure. ▮

4

Question 5

Let $F: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ as a length preserving PRF.

Let $G: \{0,1\}^n \rightarrow \{0,1\}^{2n}$ and $G(s) \stackrel{\text{def}}{=} F(s,0)||F(s,1)$.

As G is a length doubling PRG, $l(n) = 2n > n$, it passes the expansion condition required for a PRG.

Let us define a PPT Distinguisher D which is efficiently determine if a given string of length $l(n)$ is either a truly random string r or $G(s)$. G and by extension $F(s,0) \,||\, F(s,1)$ is created from the PRF F. Individually, $F(s,0)$ and $F(s,1)$ are indistinguishable from a random string and concatenating them together will still maintain that property of indistinguishability. Hence,

$|Pr[D(G(s)) = 1] - Pr[D(r) = 1]| \leq negl(n)$