CS 202 - Introduction to Applied Cryptography **Fall 2016**

HomeWork 3

October 18, 2016 *Liangjian Chen*

Problem 1 **Solution:**

(a) Expansion rate: $|H(x)| = |G(1|x)| = 2|x| + 2$.
Yes, it is a PRG.
Proof: Suppose, there is a efficient attack A against H. Then we use attack A against G. Assume $p_A = |\Pr[A(H(s)) = 1] - \Pr[A(r) = 1]|$, $p_B = |\Pr[B(G(s)) = 1] - \Pr[B(r) = 1]|$. If the beginning of s is 1, B is same with A. If th beginning of s is 0, B is always incorrect. So $p_B = p_A/2 + 0/2 = p_A/2$ which is still non-negligible. So it violets the assumption that G is a secure PRG. Thus H is a secure PRG.

(b) Expansion rate: $|H(x)| = |G(x_L|x_R)|G(x_R|x_L)| = 4|x|$.
No, it is not a PRG.
Proof: Assume $\ell = 2n$, $\overline{G}$ is a PRG and it is a mapping from $\{0,1\}^{4n}$ to $\{0,1\}^{8n}$. define G as follow, if G has a pattern x_L, x_R, x_R, x_L, which means both first and fourth quarter of bits, and second and third quarter bits are same, G map to 1^{8n}. Otherwise, G is same as $\overline{G}$.

First, G is a PRG, that because, the probability of G map to 1^{8n} is $\frac{2^{2n}}{2^{4n}} = 2^{-2n}$ which is still negligible. However, if you applied G into H, all outputs is 1^{8n}, obviously not a PRG.

(c) Expansion rate: $|H(x)| = |G(z_L)|G(z_R)| = 2|G(x)|/2 * 2 = 4|x|$.
Yes, it is a PRG.
Proof: Suppose, there is a efficient attack A against H. Construct attack B against G as follow:
calculate $G(G(x)_L)|G(G(x)_R)$. Then use A attack it. Since $H(x) = G(z_L)|G(z_R) = G(G(x)_L)|G(G(x)_R)$, B is a efficient attack which contradict with the assumption. Thus H is a secure PRG.

Problem 2 **Solution:**

Problem 3 **Solution:**

Problem 4 **Solution:**