Solutions

Cryptography--ENEE/CMSC/MATH 456
Class Exercise 2/7/24

Let G be a pseudorandom generator where $|G(s)| = |s| + 1$

1. Define $G'(s) = G(s||\bar{s})$, where $\bar{s}$ is the bit-wise negation of s. Is G' necessarily a pseudorandom generator? No.

   Let G^* be a PRG from inputs of length n to length $2n+1$

   Define G in terms of G^* as follows: $G(s=s_1||s_2) := G^*(s_1 \oplus s_2)$

   G is a PRG from n to $n+1$. G is secure b/c $s_1 \oplus s_2$ is unif. dist.

   Note $G'(s) = G(s||\bar{s}) = G^*(s \oplus \bar{s}) = G^*(1^{n/2}) =$ constant.

   Distinguisher for G':

   $D(w)$:

   If $w == G^*(1^{n/2})$ output 1

   Else output 0

   Need to show $|\Pr[D(r)=1] - \Pr[D(G'(s))=1]|$ is high.

2. Define $G'(s) = G(s)||G(\bar{s})$, where $\bar{s}$ is the bit-wise negation of s. Is G' necessarily a pseudorandom generator? No.

   Let G^* be a PRG from inputs of length n to $n+2$.

   Define G in terms of G^* as follows.

   $G(s = s_1 s')$: [where s_1 is a single bit]

   If $s_1 = 0$, output $G^*(s')$

   If $s_1 = 1$, output $G^*(\bar{s'})$

   G is PRG from n to $n+1$.

   G is secure b/c s', $\bar{s'}$ unif. dis-

   Note $G'(s_1 s') = G(s_1 s')||G(\bar{s}_1 \bar{s'}) = G^*(s)||G^*(s)$

   Distinguisher checks if 1st and 2nd half of w are the same.

   Need to show $\Pr[D(r=1)] - \Pr[D($ is high

3. Define $G'(s) = G(s)_1||G(G(s)_2, \ldots, G(s)_{|s|+1})$, where $G(s)_i$ denotes the i-th output bit of $G(s)$. Is G' necessarily a pseudorandom generator? Yes.

   Use a hybrid argument. Consider 3 distributions H_0, H_1, H_2

   In order to prove $G'(s)$ is a PRG, need to show distinguisher cannot dist. H_0, H_2

   $H_0: G(s)_1||G(G(s)_2 \ldots G(s)_{|s|+1})$ where $s \xleftarrow{R} \{0,1\}^n$

   Indistinguishable due to security of PRG G.

   $H_1: r_1||G(r_2 \ldots r_{|s|+1})$ where $r \xleftarrow{R} \{0,1\}^{n+1}$

   Indistinguishable due to security of PRG G.

   $H_2: r_1||r'_1 \ldots r'_{n+1}$ where $r_1 \xleftarrow{R} \{0,1\}$, $r' \xleftarrow{R} \{0,1\}^{n+1}$

   Note G' has stretch 2. Takes inputs of length n, produces outputs of length $n+2$.