Pseudo random generator

Wednesday, 22 February 2023 8:32 PM

Let us show that for any one way function f and its hardcore predicate B. $G_{BM} : \{0,1\}^n \to \{0,1\}^m$ is a pseudo Random function that is defined as follows:
for seed s.

for $i = 1$ to m
$h_i = B(s)$
$s = f(s)$

1.) The order of bits does not matter G_{BM} is PRNG then G_{BM} reversed is also PRNG : G^R_{BM}

Now suppose that we have a PPTM Algorithm A such that

$$\Pr\left(A\left(G^R_{BM}(s)|_{1\ldots i}\right) = G^R_{BM}(s)_{i+1}\right] \geq \frac{1}{2} + \epsilon$$

$\therefore$ Now if this is true we can say that Algo A' is such that given $z = f(y)$ where $y = f^{m-i}(s)$

Then

$$G^R_{BM}(s)|_{1\ldots i} = \left[B(f^m(s)), B(f^{m-1}(s)) \ldots B(f^{m-i+1}(s))\right]$$
$$= \left[B(f^i(y)) \ldots B(f(y))\right]$$

Then for a z we output
$\therefore \; A\left(\left[B(f^{i-1}(z)) \ldots B(z)\right]\right)$

Thus

$$\Pr\left[A'(f(y)) = B(y) \,\middle|\, y \leftarrow \{0,1\}^n\right] \geq \frac{1}{2} + \epsilon$$

This is because of the fact that f is permutation hence the distribution of

$\{T_z \mid y \leftarrow \{0,1\}^n, z = f(y)\}$ is the same as $\{G^R_{BM}(s)|_{1\ldots i} \mid s \leftarrow \{0,1\}^n\}$

Thus for our case G is defined as

for $i \in 1 \ldots m$ and seed s
$\to h_i = msb(s)$
$\to s = g^s \bmod p$

Thus our construction is valid PRNG solving which means solving discrete log