Pseudo Random Generator

To make a pseudo-random generator, we take the Discrete Logarithm Problem (DLP) as our one-way function, denoted by f.

DLP: Given p, g and $f(x) = g^x \pmod p$,

$\forall$ Probabilistic Polynomial Time Turing Machine A, (PPTM)

it is computationally infeasible for A to find a y such that $f(x) = f(y)$.

$$P\left[A(1^n, f(x)) = y,\ f(x) = f(y)\right] \leq negl(n)$$

where n is the security parameter, $n = |x|$ and $negl(n)$ is the negligible function.

We take the hardcore predicate of DLP as $h(x) = MSB(x)$. In the content of DLP,

$$MSB(x) = \begin{cases} 0 & x < \frac{p-1}{2} \\ 1 & \text{otherwise} \end{cases}$$

From the definition of hardcore predicate,

$\forall$ PPTM A,

$$P\left[A(1^n, f(x)) = h(x)\right] \leq \tfrac{1}{2} + negl(n)$$

This means that the hardcore predicate bit can ~~not~~ be distinguished from a random bit with negligible probability.

Let's define $G: \{0,1\}^n \longrightarrow \{0,1\}^{n+1}$ to be

$G(x) = f(x) \,||\, h(x)$ (DLP output appended to MSB of input)

We can see that G is a pseudo-random generator (PRG) because if $\exists$ PPTM A such that,

$$\left| P\left[A(U_{n+1}) = 1\right] - P\left[A\left[A(G(U_n)) = 1\right]\right] \right| > negl(n)$$

This means that the probability of distinguishing G's output from the output of a truly random generator is greater than $negl(n)$. This implies that probability of finding the MSB(x) is greater than $1/2$.

$$P\left[A(f(x)) = h(x)\right] > 1/2 + negl(n)$$

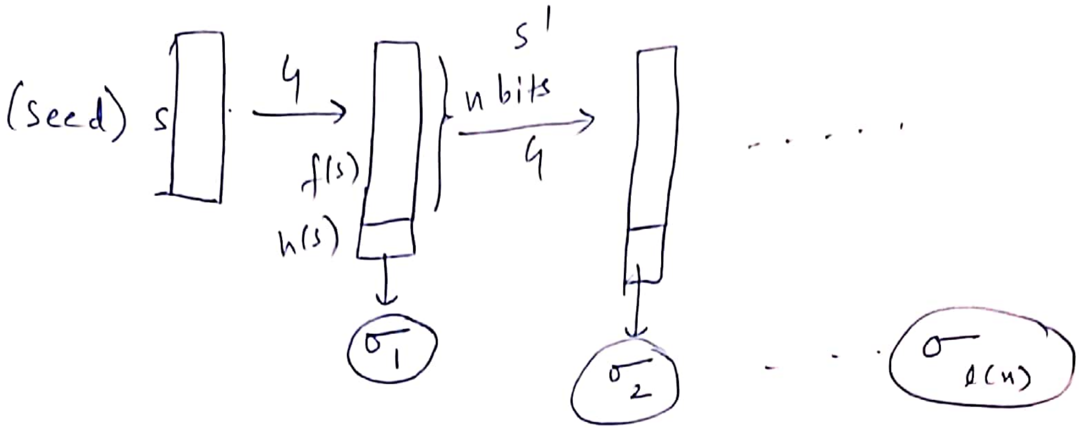
But, $h(x)$ is hardcore predicate and hence $\forall$ PPTM A,

$$P\left[A(f(x)) = h(x)\right] \leq 1/2 + negl(n)$$

leading to a contradiction. Hence, $G(x)$ is a PRG.

We now devise a PRG $H: \{0,1\}^n \longrightarrow \{0,1\}^{l(n)}$ from $G: \{0,1\}^n \longrightarrow \{0,1\}^{n+1}$ for polynomial $l(n)$.

Let us define H as follows:—



$$H(s) = \sigma_1 \sigma_2 \cdots \sigma_{\ell(n)}$$

$$|s| = n$$

If H is not a PRG, a PPTM Adversary would be able to distinguish sequence generated by H from a truly random sequence $r_1 r_2 \cdots r_{\ell(n)}$.

Consider the following sequences:-

$$\sigma_1 \sigma_2 \cdots \sigma_{\ell(n)}$$
$$r_1 \sigma_2 \cdots \sigma_{\ell(n)}$$
$$r_1 r_2 \cdots \sigma_{\ell(n)}$$
$$r_1 r_2 \cdots r_{\ell(n)}$$

Any two consecutive sequences in this list differ by one element. Since we can distinguish between the first and the last sequence, any two consecutive sequences from this list are also distinguishable.

This implies that we can distinguish between r_i and σ_i where $i \in \{1, 2, \dots, \ell(n)\}$. This contradicts the hardcore predicate's property ~~and~~ as well as pseudorandomness of G.

Hence, H is a PRG.