Here we are trying to prove that PRG is indistinguishable from truly random generator.

If we can distinguish $G(s)$ from truly random string using a distinguisher D, then this distinguisher can be used to construct adversary A which guesses $h(s)$ from $f(s)$ with probability non-negligibly greater than $1/2$.

For one way function f and its hardcore predicate hc, the pseudo-random generator $G(s) = (f(s), hc(s))$ and the PRG has an expansion factor $l(n) = n+1$

Assumption: DLP is a one-way function.

$f(s) = g^s \bmod p$ and it's hcp is $MSB(x)$

$\Rightarrow$ $hc(s) = MSB(s)$

$G(s) = (g^s \bmod p, msb(s))$

proof by contradiction:

Let there exist probabilistic polynomial time distinguisher D and non-negligible function $\varepsilon(n)$ for which

(1) $$|P[D(f(s), hc(s)) = 1 - P[D(r) = 1]| \geq \varepsilon(n)$$

D distinguishes random r and $G(s)$ with probability $\varepsilon(n)$

The first step to build A, Let us show that D can distinguish $(f(s), hc(s))$ from $(f(s), \overline{hc}(s))$ where,

$$\overline{hc}(s) = 1 - hc(s)$$

Consider the random string $(f(s), \beta) \rightarrow \beta$ is equal to $hc(s)$ with probability $1/2$ and equal to $\overline{hc}(s)$ with probability $1/2$.

Thus we write,

$$P[D(f(s), B) = 1] = \frac{1}{2}\left[P[D(f(s), hc(s)) = 1] + \frac{1}{2} P[D(f(s), \overline{hc(s)}) = 1\right]$$

$$s \in \{0,1\}^n, \quad B \in \{0,1\}$$

$$\Rightarrow \left|P[D(f(s), hc(s)) = 1] - P[D(f(s), B) = 1]\right|$$

$$= \left|P[D(f(s), hc(s)) = 1] - \frac{1}{2} P[D(f(s), hc(s)) = 1] \cdot \frac{1}{2} P[D(f(s), \overline{hc}(s)) = 1)\right.$$

$$= \frac{1}{2}\left|P[D(f(s), hc(s)) = 1) - P[D(f(s), \overline{hc}(s)) = 1)\right|$$

for all the expressions,

$s \leftarrow \{0,1\}^n$ and $B \leftarrow \{0,1\}$

By ①,

$$\left| P[D(f(s), hc(s)) = 1] - P[D(f(s), \overline{hc}(s)) = 1] \right|$$

$$= 2 \left| P[D(f(s), hc(s)) = 1] - P[D(r) = 1] \right|$$

$$\Rightarrow P[D(f(s), hc(s)) = 1] \geq P[D(f(s), \overline{hc}(s)) = 1]$$

Construction of the Adversary A.

1. choose $\sigma \leftarrow \{0,1\}$ uniformly
2. Apply the distinguisher for (y, σ)
3. If D returns 1, output σ else output $\bar{\sigma}$.

probability of A succeeding,

$$P[A(f(s)) = hc(s)]$$

$$= \frac{1}{2} [P[A(f(s)) = hc(s) \mid \sigma = hc(s)]$$

$$+ \frac{1}{2} P[A(f(s)) = hc(s) \mid \sigma = \overline{hc}(s)]$$

② $= \frac{1}{2} P[D(f(s), h(s)) = 1] + \frac{1}{2} [D(f(s), \bar{hc}(s) = 0]$

If $\sigma = hc(s)$

→ A invokes D on input $(f(s), \bar{hc}(s))$

→ A outputs $hc(s)$ iff D Output

(similarly, if $\sigma \neq h(s)$

→ A invokes D on input $(f(s), \bar{hc}(s))$

→ A outputs $hc(s)$ iff D outputs C.

from ②,

$P[A(f(s)) = hc(s)]$

$= \frac{1}{2}[P[D(f(s), hc(s)] = 1] + \frac{1}{2}(1 - P[D(f(s), \bar{hc}(s) = 1])$

$= \frac{1}{2} + \frac{1}{2}[P[D(f(s), hc(s)] = 1]$

$- P[D(f(s), \bar{hc}(s)] = 1])$

$$\geq \frac{1}{2} + \frac{1}{2} \cdot 2\varepsilon(n) \quad \geq \frac{1}{2} + \varepsilon(n)$$

↳ non-negligible

which contradicts that hc is a hcp of f.

Hence $\varepsilon(n)$ is negligible.

→ ∴ The construction proposed gives PRG which is indistinguishable from a truly random generator.