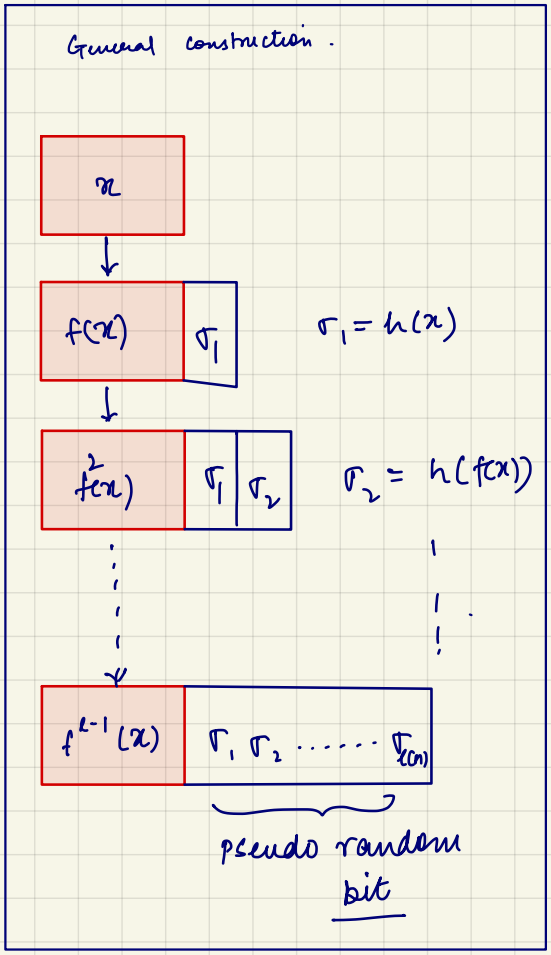
PRG (Pseudo-Random Generator)

Definations: $G: \{0,1\}^n \rightarrow \{0,1\}^{l(n)}$, $l(n)$ → expansion factor, n → security parameter

here, $f(x) = g^x \bmod p$ (DLP) } one-way function

$$h(x) = \begin{cases} 0 & x < \frac{p-1}{2} \\ 1 & \text{otherwise.} \end{cases}$$ } hard-core predicate function

$$G(x,l) = \underbrace{h(x)}_{h_1} \| \underbrace{h(f(x))}_{h_2} \| \underbrace{h(f^2(x))}_{h_3} \| \ldots \| \underbrace{h(f^{l-1}(x))}_{h_l}$$



Proof of security:

By definition of hcp, we know that, $\forall$ PPTM D,

$$P[D(h(x)) = 1 \mid f(x)] \leq \tfrac{1}{2} + \text{negl}(n)$$

⇒ similarly,

$$P[D(h(f(x))) = 1 \mid f(f(x))] \leq \tfrac{1}{2} + \text{negl}(n)$$

$$P[D(h(f^2(x))) = 1 \mid f^3(x)] \leq \tfrac{1}{2} + \text{negl}(n)$$

$$\vdots$$

$$P[D(h(f^{l-1}(x))) = 1 \mid f^l(x)] \leq \tfrac{1}{2} + \text{negl}(n)$$

$\because \forall$ PPTM D, the probability of guessing $h_1 h_2 h_3 \ldots h_l$

$$P(\text{determining } h_1 h_2 \ldots h_n) \leq \left(\tfrac{1}{2} + \text{negl}(n)\right)^l$$

$$\leq \frac{1}{2^l} + \text{negl}(n) \quad -(1)$$

Also, for any random string $r \in \{0,1\}^l$

$$P(D(r) = 1) = \frac{1}{2^l} \quad -(2)$$

(here, for any string x, $D(x) = 1$ ⇒ if D could correctly guess x; $= 0$ ⇒ otherwise)

from (1) & (2) we have,

$$P[D(h_1 h_2 \ldots h_l) = 1] - P[D(r) = 1] \leq \text{negl}(n)$$

$\because$ completes the proof

(since, the PPTM adversary D, could distinguish b/w a completely random string and PRG generated string with negligible probability).

Karmanjot Singh
2022101062