Assignment - 1

2020111013

PRG

~~Q~~

① Construction of PRG

For a given input x ~~and~~, expansion factor l & security parameter n, PRG G is defined as

$$G : \{0,1\}^n \to \{0,1\}^{l(n)}$$

For a hard-core predicate $hc(x)$, and a probabilistic polynomial time algorithm A, then there exists a negligible function such that

$$Pr[A(f(x)) = hc(x)] \leq \frac{1}{2} + negl(n) \quad - ①$$

~~PRG~~ PRG G is defined as (here $f(x)$ is the one-way function, in this case, DLP)

$$G(x, l) = h(x) \| h(f(x)) \| h(f^2(x)) \| \cdots \| h(f^{l-1}(x))$$

The PRG is defined as the concatenation of the hard-core predicates of ~~all~~ the repeated output of the one-way function.

Proof of Security

From ①,

$$Pr[\underbrace{A(f(x)) = hc(x)}_{\text{Determining } hc(x) \text{ is } D(x)}] \leq \frac{1}{2} + negl(n)$$

$$\Rightarrow Pr[A(f(f(x))) = hc(f(x))] \leq \frac{1}{2} + negl(n)$$

$$\Rightarrow Pr[A(f^3(x)) = hc(f^2(x))] \leq \frac{1}{2} + negl(n)$$

$$\vdots$$

$$Pr[A(f^l(x)) = hc(f^{l-1}(x))] \leq \frac{1}{2} + negl(n)$$

Multiplying all the equations,

$$Pr[D(x) \cdot D(f(x)) \cdot D(f^2(x)) \cdots D(f^{l-1}(x))] \leq \left(\frac{1}{2} + negl(n)\right)^l$$

$$\Rightarrow Pr[\underbrace{D(x) \cdot D(f(x)) \cdots D(f^{l-1}(x))}_{\text{Probability of determining PRG}}] \leq \underbrace{\frac{1}{2^l}}_{\text{Probability of determining random string}} + negl(n) \quad -②$$

From ②

$$Pr[\text{Determining PRG}] - Pr[\text{Determining random string}] \leq negl(n)$$

$\therefore$ Given ~~PRG~~ construction is a valid PRG