Pseudo Random Function (PRF)

Construction

Let G be the PRG, such that

$G: \{0,1\}^n \rightarrow \{0,1\}^{2n}$ (doubles the length)

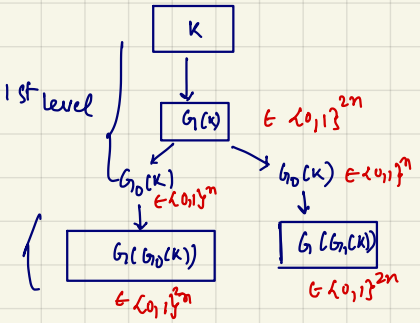
$G_0(x) =$ Left $(G(x))$ [first n-bits]

$G_1(x) =$ Right $(G(x))$ [last n-bits]

$F: \underbrace{\{0,1\}^n}_{k} \times \underbrace{\{0,1\}^n}_{x} \Rightarrow \{0,1\}^n \Rightarrow F(k,x) = F_k(x)$

for a given key k of n-bits, and an input $x = x_1 x_2 \ldots x_n$ (n-bits)

$$F_k(x) = G_{x_n}(\ldots(G_{x_2}(G_{x_1}(k)))\ldots)$$



} General construction of PRF.

Proof: Since the bits x_i of x could either be 0 or 1 with a equal probability $(= 1/2)$ we could say that each step the probability P of choosing $G_0(\cdot)$ or $G_1(\cdot)$ is $= 1/2$ and remains random and indistinguishable.

Proving by Induction

at 1st level → $G_0(k)$ & $G_1(k)$ remains indistinguishable from outputs of truly random functions, assuming output of PRG G (G) is indistinguishable from truly random functions.

at 2nd level → passing the output from the previous levels and passing it to the PRG (G), thus the output generated will be random & can't be distinguished from truly random function.
also, since bits $x_i \in \{0,1\}$, choosing $G_0(k)$ or $G_1(k)$ also, couldn't be distinguished. and thus adds to, indistinguishability.

⇒ Similarly, from induction, we can follow up that, the output at each level will be completely indistinguishable from a truly random sequence.

Let r be a random bit string, $\in \{0,1\}^n$

$$\therefore P[f(x) = r] = \frac{1}{2^n} \quad (1)$$

↓ treat a truly random generator generates string r

for each PRF, at each step we could go either left(0) or right(1)

$$\therefore P[F_k(x) = r] \leq \frac{1}{2^n} + \text{negl}(n)$$

$$\Rightarrow \boxed{P[F_k(x) = r] - P[f(x) = r] \leq \text{negl}(n)}$$

⇒ can't be distinguished & thus is provably secure construction.