

Pseudo Random Function:

A Pseudo Random function is computationally indistinguishable from a real random function i.e., from domain $\{0,1\}^n$ to $\{0,1\}^n$

We say that the function F is Pseudo Random Function if for all probabilistic polynomial time distinguishers D , there exists a negligible function negl such that

$$\left| \Pr[D^{F_k(\cdot)}(1^n) = 1] - \Pr[D^{f(\cdot)}(1^n) = 1] \right| \leq \text{negl}(n),$$

Where k is chosen uniformly at random and f_n is chosen from the set of functions mapping n -bit strings to n -bit strings.

Construction of PRF using PRG:

Let G be a Pseudo Random Generator with expansion factor being $2n$. Let $G_0(k)$ be the first half of G 's output and $G_1(k)$ be the second half of G 's output. For every k in $\{0,1\}^n$, F is defined as

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

i.e., For each bit ' k ' in the input seed sequence, if k is 0 the first half of PRG's output is considered. If k is 1, the second half of PRG's output is considered.

A PRF F is a two input function $\{0,1\}^* \times \{0,1\}^*$ where the first input is called key and the second input is just the seed. F is a length preserving function i.e., the input and output lengths will be same.

From Mathematical point of view, we define the set Func_n be the set of all such functions. F is a function which maps n -bit strings to n -bit strings. Consider a look up table which has 2^n rows each row corresponding to each bit string of the domain. Each row will have 2^n strings corresponding to codomain. Each such table can be represented using $n \cdot 2^n$ bits. The functions in the set Func_n are in one-one correspondence with these $n \cdot 2^n$ bits. Therefore the size of the set is $2^{(n \cdot 2^n)}$.