PRF is a efficient and deterministic function that is:

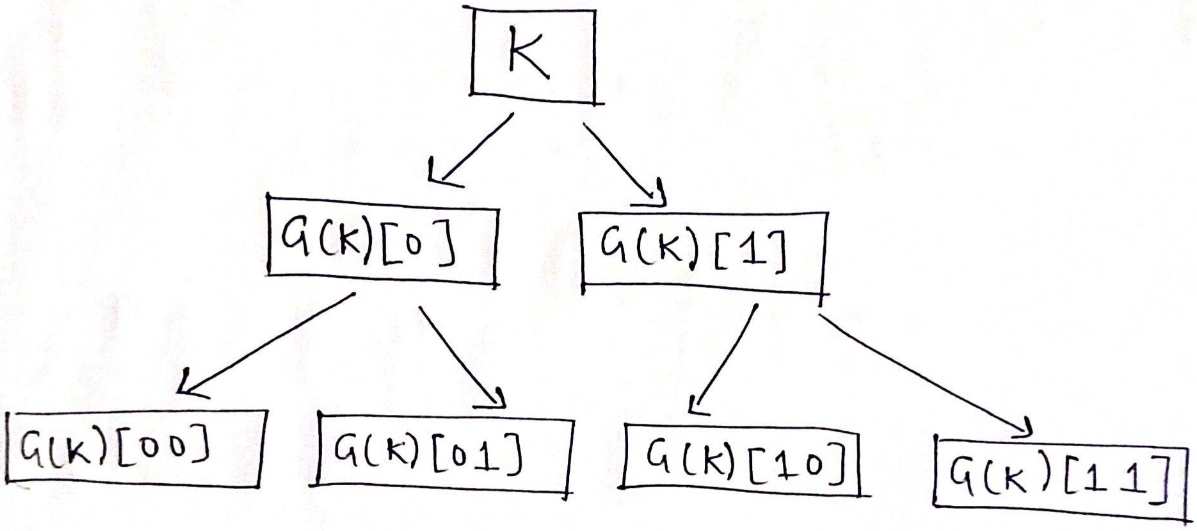
- Easy to compute
- Computationally indistinguishable from a random function

PRF is based on PRG with the only exception that in addition to the internal state they can accept any input data.

Let G be a secure PRG, which on input $\{0,1\}^s$, outputs $\{0,1\}^{2s}$, i.e. double the length of the input. Let G_0 and G_1 be the left and right halves of G, respectively such that $G(x) = G_0(x) \| G_1(x)$. For any K belonging to $\{0,1\}^s$, define F_k: $\{0,1\}^n$ -> $\{0,1\}^s$ by

$$\mathbf{F_K(x_1\ldots x_n) = G_{xn}(G_{xn-1}(\ldots G_{x1}(K)\ldots))}$$

If the PRG G is secure then the function F is also secure.


K
G(K)[0]
G(K)[1]
G(K)[00]
G(K)[01]
G(K)[10]
G(K)[11]