1 Pseudorandom Functions

1.1 What are psuedorandom functions?

A psuedorandom function is a function that is indistinguishable from a random function.

Let $F : \{0,1\} \times \{0,1\} \to \{0,1\}^*$ be an efficient, length-preserving, keyed function. We say that F is a pseudorandom function if for all probabilistic polynomial-time distinguishers D, there exists a negligible function negl such that:

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

where $k \leftarrow \{0,1\}^n$ is chosen uniformly at random and f is chosen uniformly at random from the set of functions mapping n-bit strings to n-bit strings.

1.2 Construction of PRF from PRG

Let G be a pseudorandom generator with expansion factor $\ell(n) = 2n$. Denoted by $G_0(k)$ is the first half of G' 's output, and by $G_1(k)$ the second half of G' s output. For every $k \in \{0,1\}^n$, we define the function $F_k : \{0,1\}^n \to \{0,1\}^n$ as:

$$F_k\left(x_1x_2\cdots x_n\right) = G_{x_n}\left(\cdots\left(G_{x_2}\left(G_{x_1}(k)\right)\right)\cdots\right).$$