2021201041
Nvss Maneesh Gupta

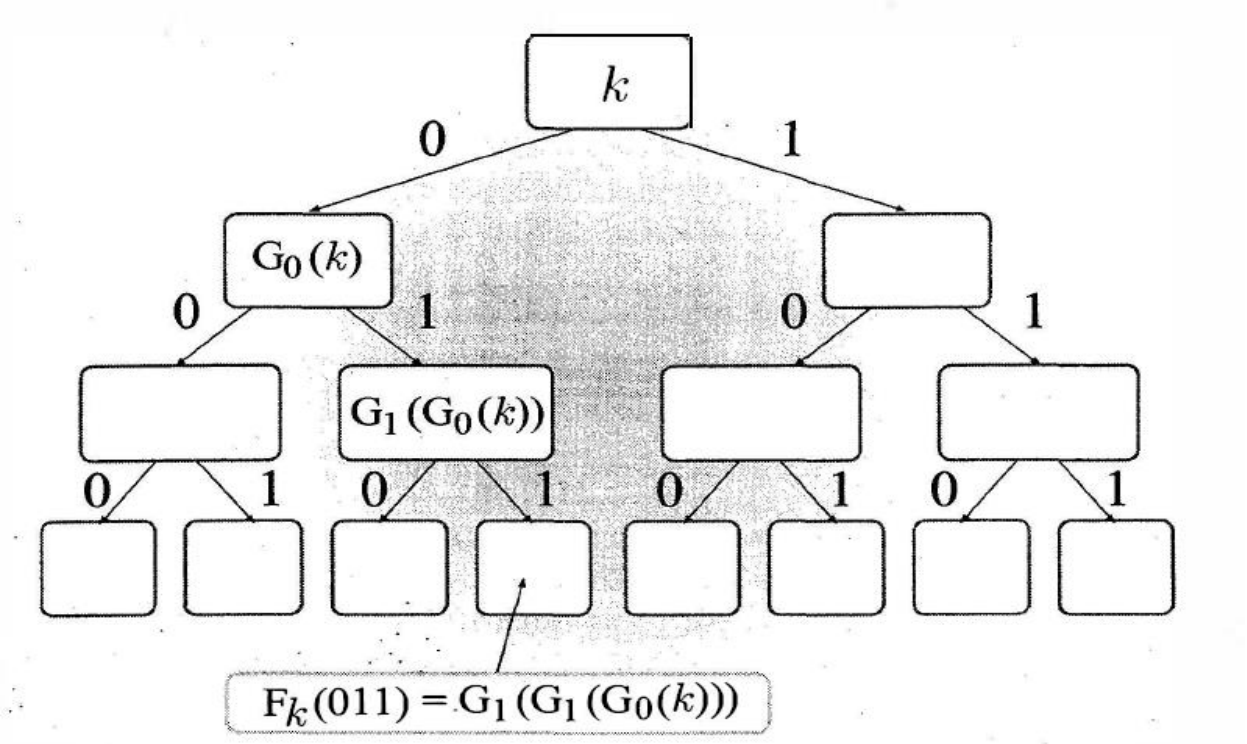
Pseudo Random Function (PRF)

Let $F: \{0,1\}^n \; X \; \{0,1\}^* \rightarrow \{0,1\}^*$ 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:*

$$|\Pr[D^{Fk(.)}(1^n) = 1] - \Pr[D^{f(.)}(1^n) = 1]| \leq negl(n)$$

Construction of PRF from PRG:

Let G be a PRG with an expansion factor $l(n) = 2n$. Denoted by $G_0(k)$ the first half of G's output, and by $G_1(k)$ the second half of G's output. For every $k \in \{0,1\}^n$, define the function $F_k: \{0,1\}^n \rightarrow \{0,1\}^n$ as $F_k(x_1 x_2 \dots x_n) = G_{x_n}(\dots(G_{x_2}(G_{x_1}(k)))\dots)$.



References

[1] J. K. a. Y. Lindell, Introduction to Modern Cryptography.

[2] B. Micali, "Hardcord bits," [Online]. Available: https://crypto.stanford.edu/pbc/notes/crypto/hardcore.html.

[3] Lecture Slide