**Pseudo Random Function (PRF)**

Let 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 such that:*

Construction of PRF from PRG:

Let G be a PRG with an expansion factor . Denoted by the first half of G’s output, and by the second half of G’s output. For every , define the function as .



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