PRF

February 22, 2023

We want to prove that for all PPTM Distinguisher given oracle PRF and TRF, it cannot distinguish between PRF and TRF.

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

Let x be the random seed given by the distinguisher to both PRF and TRF oracle.

Firstly, note that G is a provably secure PRG. Therefore, the left/right half bits are also pseudorandom bits. This can be expressed as:

$$[\Pr[G \text{ is a provably secure PRG}] \Rightarrow \Pr[\text{Left/Right half bits are also pseudorandom bits}]]$$

Since x is a random seed given by the distinguisher, moving left or right at each depth in the construction is random. This is because the left/right movement is determined by the output of the pseudorandom function on the left/right half of the input, which in turn is determined by the left/right half bits of x. Since these bits are pseudorandom, the movement is also pseudorandom. This can be expressed as:

$$[\Pr[x \text{ is a random seed}] \Rightarrow \Pr[\text{Moving left or right is random}]]$$

Therefore, the output of the PRF and TRF oracle are indistinguishable, as the distinguisher cannot differentiate between a truly random function and the pseudorandom function generated by G using the pseudorandom bits of x. This can be expressed as:

More formally,

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

This completes the proof.