Pseudo-random Function

We devise a pseudo-random function from pseudo-random generator G as follows:

Let $G : \{0,1\}^n \longrightarrow \{0,1\}^{2n}$ be a PRG. Let $r = r_0 r_1 \ldots r_{n-1}$ be a random sequence.

Define G_0 and G_1 as the left and right halves of the output $G(x)$.

$$G_0(x) = \text{Left}(G(x))$$

$$G_1(x) = \text{Right}(G(x))$$

$$\therefore \; G(x) = G_0(x) \,||\, G_1(x)$$

Let $F_k : \{0,1\}^n \longrightarrow \{0,1\}^n$ be defined as follows:

$$F_k(r) = G_{r_{n-1}}(G_{r_{n-2}}(\cdots(G_{r_0}(k))))$$

where k is the key input of length n.

For PPTM adversary, if $F_k(r)$ can be distinguished from a truly random function generated from truly random generator, then the pseudo-random generator G can be distinguished from the truly random generator. This contradicts the definition of pseudo-random generators. Hence, $F_k(r)$ is a pseudo-random function.