Pseudo-random Function

We devise a pseudo-random function from pseudo-random generator G as follows. Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a PRG. Let $r = r_0 r_1 \dots r_{n-1}$ be a random sequence. Define G_0 and G_1 as the left and right parts of the output of $G(x)$.

$$G_0(x) = Left(G(x))$$

$$G_1(x) = Right(G(x))$$

$$G(x) = G_0(x)||G_1(x)$$

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

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

where k is given key of length n.
If $F_k(r)$ were distinguishable from a truly random function, the PRG G used would be distinguishable from a truly random generator because a truly random generator must give a truly random function following the aforesaid process. Hence, $F_k(r)$ is a pseudo random function.