Pseudo Random Function

Def^n Let G be a pseudorandom generator with expansion factor $l(n) = 2n$. Denote $G_0(k)$ 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

$$F_k : \{0,1\}^n \to \{0,1\}^n \text{ as}$$

$$F_k(x_1, x_2, -- x_n) = G_{x_n}(-- G_{x_2}(G_{x_1}(k))--).$$

Provable Secure :-

Since, we already proved that ~~PRF~~ PRG is provably secure in Q1, so here

$$F_k(x_1, x_2 -- x_n) = G_{x_n}\underbrace{(-- G_{x_2}(G_{x_1}(k)))--)}_{\text{seed}}$$

$$\therefore F_k(x_1, x_2 - x_n) = G_{x_n}(\text{seed})$$

i.e. F itself is an output of PRG.

So it is also provable secure.