Cryptography: Homework 3

(Deadline: 10am, 2021/10/29)

1. (20 points) Prove that if f is a one-way function, then the function g defined by $g(x_1, x_2) = (f(x_1), x_2)$, where $|x_1| = |x_2|$, is also a one-way function.

2. (30 points) Let F be a length-preserving pseudorandom function. Let $F' : \{0,1\}^n \times \{0,1\}^{n-1} \to \{0,1\}^{2n}$ be a keyed function such that $F'_k(x) = F_k(0\|x)\|F_k(x\|1)$. State whether F' is a pseudorandom function. If yes, prove it; if not, show an attack.