HIT — Cryptography — Homework 4

September 9, 2014

Problem 1. Prove that if f is a one-way function, then $g(x_1, x_2) = (f(x_1), x_2)$ where $|x_1| = |x_2|$ is also a one-way function. Observe that g fully reveals half of its input bits, but is nevertheless still one-way.

Problem 2. Let f be a one-way function. Is $g(x) = f(f(x))$ necessarily a one-way function? What about $g(x) = (f(x), f(f(x)))$? Prove your answers.

Problem 3. Let G be a pseudorandom generator with expansion factor $\ell(n) = n + 1$. Prove that G is a one-way function.