# Foundations of Cryptography 2021-22

Homework Set No. 1

Date Due: Nov 22nd 2021

0. Consider the distribution where with probability $1/2$ the result is $0^n$ and with probability $1/2$ it is uniform over $\{0,1\}^n$. Compute the Shannon entropy of this distribution.

1. If a function $f\colon \{0,1\}^n \mapsto \{0,1\}^n$ is one-to-one as well as a one-way function then it is a called a *one-way permutation*. Show that if $P = NP \cap Co - NP$ then there are no one-way permutations.

Recall that we showed that inverting (presumed) one-way functions is easy if $P = NP$.

2. If $f\colon \{0,1\}^n \mapsto \{0,1\}^n$ is a one-way function, is $f_L$ where $f_L(x)$ consists of the first half of the bits of $f(x)$ necessarily a one-way function?

3. Show how to use a square-root computing routine to factor, while preserving the probability of success.

Bonus question: suggest a way of using $f$ that is one-way on its iterates to get a more compact one-time signature scheme, by using a larger alphabet. Recall that we saw a method that uses a public key with $2n/\log k$ images. Think of a method that is closer to $n/\log k$ images.