CS 171: Problem Set 7

Due Date: March 18th, 2024 at 8:59pm via Gradescope. No late submissions will be accepted.

1 PRGs Imply OWFs (5 points)

We saw in lecture 12 that one-way functions (OWFs) can be used to construct pseudorandom generators (PRGs). Additionally, it turns out that PRGs can be used to construct OWFs. This means that the assumption that OWFs exist is equally strong as the assumption that PRGs exist.

Question: Let $G : \{0,1\}^{n/2} \to \{0,1\}^n$ be a PRG. Prove that G is also a OWF.

2 A Candidate Key-Exchange Protocol (5 points)

Consider the following proposal for a key exchange protocol:

1. Alice samples $k \leftarrow \{0,1\}^n$ and $r \leftarrow \{0,1\}^n$, and sends Bob the following:
$$s := k \oplus r$$
2. Bob samples $t \leftarrow \{0,1\}^n$, and sends Alice the following:
$$u := s \oplus t$$
3. Alice sends Bob the following:
$$w := u \oplus r$$
4. Alice outputs k and Bob outputs $w \oplus t$.

Questions:

(a) *Correctness:* Show that Alice and Bob will always output the same key k.

(b) *Security:* Does this scheme satisfy key-exchange security[1]? Prove your answer.

[1]Key-exchange security is also known as $\mathsf{KE}^{\mathsf{eav}}_{\mathcal{A},\Pi}$ security. It was defined in lecture 13, slide 26, as well as in Katz & Lindell, 3rd Edition, Definition 11.1.