6 Bonus: One Way Functions

Let us assume we have access to a secure one way function $h : \{0,1\}^{2k} \rightarrow \{0,1\}^k$

Consider the following construction of $f : \{0,1\}^{2k} \rightarrow \{0,1\}^{k+1}$:

$$f(s) = \begin{cases} 0 \mid\mid x & \text{if } s = 0^k \mid\mid x \\ 1 \mid\mid h(s) & \text{otherwise} \end{cases} \tag{1}$$

Thus, $g : \{0,1\}^{2k} \rightarrow \{0,1\}^k$ is defined as follows:

$$g(s) = \begin{cases} x & \text{if } s = 0^k \mid\mid x \\ h(s) & \text{otherwise} \end{cases} \tag{2}$$

Clearly, an attacker can break one-wayness of g by return $0^n x$ as a possible input given an output x.

Claim 6.1. f is a OWF

We will show that breaking one-wayness of f implies an attack on onewayness of h. The idea is that the first bit of the output being 0 occurs with probability $\frac{1}{2^k}$. In this case an attacker can break one-wayness of f with probability 1. However, this case occurs with negligible probability. In the rest of the cases, the attacker has to break one-wayness of h in order to break one-wayness of f.

If an attacker breaks one-wayness of f with probability of ϵ, then the same attacker has probability of at least $\epsilon \cdot (1 - \frac{1}{2^k}) - \frac{1}{2^k}$ of breaking h. If ϵ is non-negligible then so is this probability. Thus, we show that one-wayness of h implies one-wayness of f.