Homework 4

Casey Bates

3 May 2020

1 $\boldsymbol{h}(x) = y$

(a)

If h takes inputs of 1088 bits and outputs of 256 bits, then we know there must be 2^{1088} possible values of x, and 2^{256} possible values of y.
If h is an n-to-1 map, then n 1088-bit strings are mapped to one 256-bit string. Thus,

$$n = \frac{2^{1088}}{2^{256}} = 2^{832}$$

Therefore. h is a 2^{832}-to-1 map.

(b)

We know that there are 2^{1088} possible values of x, and we know that h is a 2^{832}-to-1 map. The probability, P, of solving the one-to-one propblem is:

$$P = \frac{2^{832}}{2^{1088}} = \frac{1}{2^{256}}$$

Therefore, the probability of solving the one-to-one problem for h is $\frac{1}{2^{256}}$

2 $\boldsymbol{f}\colon X \to Y$

Assume f does not have the one-way property. Thus, given y ϵ Y it is possible to find x ϵ X such that $f(x) = y$.
Suppose we take a random x ϵ X, then compute $f(x) = y$.
Then, we find an x' ϵ X such that $f(x') = y$.
If $x \neq x'$, then there is a collision, and f must not be weakly collision resistant.