CS152-Homework6

Hongchen Cao 2019533114

2020.10.22

1

1.1

$P = (\frac{M-1}{M})^{Q'}$

1.2

$P = (\frac{M-1}{M})^{Q'Q}$

1.3

$$
\begin{align}
P &= \frac{1}{2} \tag{1}\\
(\frac{M-1}{M})^{Q'Q} &= \frac{1}{2} \tag{2}\\
(\frac{M-1}{M})^{cM} &= \frac{1}{2} \tag{3}\\
((1-\frac{1}{M})^{M})^{c} &= \frac{1}{2} \tag{4}\\
(\frac{1}{e})^{c} &= \frac{1}{2} \tag{5}\\
c &= In(2) \tag{6}
\end{align}
$$

2

$$
\begin{align}
P(CTP) &= \frac{1}{|\mathcal{X}|} \cdot \sum_{x \in \mathcal{X}} P(CTP|x) \tag{7}\\
&= \frac{1}{|\mathcal{X}|} \cdot \sum_{x \in \mathcal{X}} P(OP|h(x)) \frac{\frac{|\mathcal{X}|}{|\mathcal{Y}|} - 1}{\frac{|\mathcal{X}|}{|\mathcal{Y}|}} \tag{8}\\
&= \frac{1}{|\mathcal{X}|} \cdot (1 - \frac{|\mathcal{Y}|}{|\mathcal{X}|}) \cdot \frac{|\mathcal{X}|}{|\mathcal{Y}|} \cdot \sum_{y \in \mathcal{Y}} P(OP|y) \tag{9}\\
&\geq \frac{1}{|\mathcal{Y}|} \cdot (1 - \frac{|\mathcal{Y}|}{|\mathcal{X}|}) \cdot |\mathcal{Y}| \cdot \epsilon \tag{10}\\
&\geq \frac{\epsilon}{2} \tag{11}
\end{align}
$$

3

Suppose we find a collision, so $\exists x \neq x' : h_2(x) = h_2(x')$.

Let $x = x_1 || x_2$ and $x' = x'_1 || x'_2$

Then we have

$$h_1(h_1(x_1)||h_1(x_2)) = h_1(h_1(x'_1)||h_1(x'_2))$$

Let $a = h_1(x_1)||h_1(x_2)$ and $b = h_1(x'_1)||h_1(x'_2)$.

If $a \neq b$, we find collision for h_1, which is impossible.

So $a = b$, then we have $h_1(x_1) = h_1(x'_1)$ and $h_1(x_2) = h_1(x'_2)$.

If $x_1 \neq x'_1$ or $x_2 \neq x'_2$, we find collision for h_1, which is impossible.

So $x_1 = x'_1$ and $x_2 = x'_2$, then we have $x = x'$.

Thus, we get a contradiction.

4

Suppose we find a collision, so $\exists x \neq x' : h(x) = h(x')$.

There exists 2 cases:

1. $|x| = |x'| = tk$
2. $|x| = tk$ and $|x'| = lk$, we can suppose $l > k$

For $case1$:

From $h(x) = h(x')$, we have $\textbf{Compress}(z_k) = \textbf{Compress}(z'_k)$.

Because Compress is collision resistant, we have $z_k = z'_k$.

Then we have $g_{k-1}||x_k = g'_{k-1}||x'_k$ which means that $g_{k-1} = g'_{k-1}$ and $x_k = x'_k$.

Again, because Compress is collision resistant, we have $z_{k-1} = z'_{k-1}$ which means that $g_{k-2} = g'_{k-2}$ and $x_{k-1} = x'_{k-1}$.

Repeat the above steps, and finally we have $x_i = x'_i$ for $i \in [1..k]$ which means that $x = x'$.

Thus, we get a contradiction.

For $case2$:

From $h(x) = h(x')$, we have $\textbf{Compress}(z_k) = \textbf{Compress}(z'_l)$.

Because Compress is collision resistant, we have $z_k = z'_l$.

Then we have $g_{k-1}||x_k = g'_{l-1}||x'_l$ which means that $g_{k-1} = g'_{l-1}$ and $x_k = x'_l$.

Again, because Compress is collision resistant, we have $z_{k-1} = z'_{l-1}$ which means that $g_{k-2} = g'_{l-2}$ and $x_{k-1} = x'_{l-1}$.

Repeat the above steps, and finally we have $z_1 = z'_{l-k+1}$ which means $0^m = g'_{l-k} = \textbf{Compress}(z'_{l-k})$.

However Compress is zero preimage resistant.

Thus, we get a contradiction.

Finally, for both case we get a contradiction so h is collision resistant.