Homework #2

Student name: *Chengqi Liu (1954148), Maitraiyi Dandekar (1990136), Zakariae Jabbour (2039702)*

Course: *Cryptology (2MMC10)* – Professor: *Tanja Lange*
Due date: *September 19th, 2023*

1. (a)

The claim is true.

Prove by contradiction:

Assume that H is not preimage resistant. So, given $\forall y$, the adversary can find m' with non-negligible probability such that $H(k, m') = y$.

Now, given $z = h(k, m)$ as an image, we can just run the same algorithm, consider z as an image of H and find the preimage x_1. So, whe have

$$z = H(k, x_1) = h(k, h(k, x_1))$$

We can just calculate $x_2 = h(k, x_1)$, and get $z = h(k, x_2)$. So, x_2 is a preimage of z. So, h is not preimage resistant. It's a contradiction.

So, If h is preimage resistant, H is preimage resistant.

(b)

The claim is false.

Assume that h_1 is collision resistant but not preimage resistant, and h_2 is not collision resistant.

Because h_2 is not collision resistant, the adversary can find y_1, y_2 such that $h_2(k_2, y_1) = h_2(k_2, y_2)$. Then, because h_1 is not preimage resistant, the adversary can find m_1, m_2 such that $h_1(k_1, m_1) = y_1, h_1(k_1, m_2) = y_2$. In all, the adversary can find m_1, m_2 such that $h_2(k_2, h_1(k_1, m_1)) = h_2(k_2, h_1(k_1, m_2))$, which is $(\langle k_1, k_2 \rangle, m_1) = (\langle k_1, k_2 \rangle, m_2)$. So, the adversary can find a collision of H with non-negligible probability. It's a counterexample. The claim is wrong.

2. (a)

$$\begin{aligned}
s_1 &= r^{-1}(H(m_1) + x(R)a) \mod l \\
s_2 &= r^{-1}(H(m_2) + x(R)a) \mod l \\
\Rightarrow s_1 s_2^{-1} &= (H(m_1) + x(R)a)(H(m_2) + x(R)a)^{-1} \mod l \\
\Rightarrow s_1(H(m_2) + x(R)a) &= s_2(H(m_1) + x(R)a) \mod l
\end{aligned}$$

Notice that a is the only unknown variable in the last equation. So, we can solve the linear equation with one unknown and get

$$a = (s_2 H(m_1) - s_1 H(m_2)) x(R)^{-1} (s_1 - s_2)^{-1} \mod l$$

So, we can just compute $(s_2 H(m_1) - s_1 H(m_2)) x(R)^{-1} (s_1 - s_2)^{-1} \mod l$ to get a.

(b)

$$\begin{aligned}
&R_1 = r_1 P \\
&R_2 = (r_1 + 1) P \\
&s_1 = r_1^{-1} (H(m_1) + x(R_1) a) \mod l \\
&s_2 = (r_1 + 1)^{-1} (H(m_2) + x(R_2) a) \mod l
\end{aligned}$$

Observe the last two equations. There are two unknown variables r_1, a, and there are also two equations. So, we can solve the linear equations with two unknowns and get

$$a = (s_1 H(m_2) - s_2 H(m_1) - s_1 s_2)(s_2 x(R_1) - s_1 x(R_2))^{-1} \mod l$$

So, we can just compute $(s_1 H(m_2) - s_2 H(m_1) - s_1 s_2)(s_2 x(R_1) - s_1 x(R_2))^{-1} \mod l$ to get a.

(C)

First, expand this equation:

$$\begin{aligned}
&w_1 P + w_2 P_A = R \\
\Leftrightarrow &s^{-1} H(m) P + s^{-1} x(R) a P = rP \mod l \\
\Leftrightarrow &s^{-1} (H(m) + x(R) a) P = rP \mod l \\
\Leftrightarrow &s^{-1} (H(m) + x(R) a) = r \mod l
\end{aligned}$$

(Note that we only need to modulo the factor multiplied with P with l. In order to write it beautifully, we wrote $\mod l$ at the end.)

So, for m_1 and m_2, we have

$$\begin{aligned}
&s_1^{-1} (H(m_1) + x(R_1) a) = r \mod l \\
&s_2^{-1} (H(m_2) + x(R_2) a) = r \mod l
\end{aligned}$$

Observe the last two equations. There are two unknown variables r, a, and there are also two equations. So, we can solve the linear equations with two unknowns and get

$$a = (s_1 H(m_2) - s_2 H(m_1))(s_2 x(R_1) - s_1 x(R_2))^{-1} \mod l$$