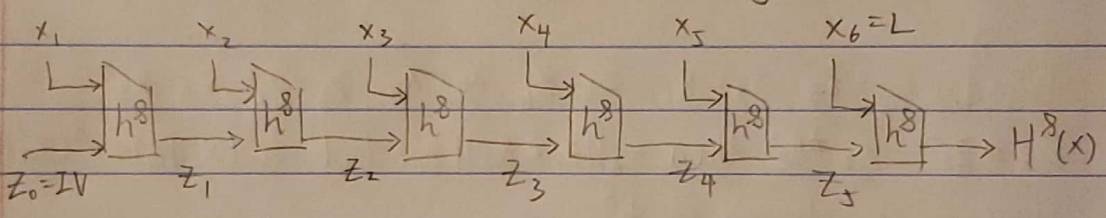
1. $\mathcal{A}$ queries the oracle with $m = m_0 \| m_1$ and $m' = m_0' \| m_1'$ where $m_0 \neq m_0'$ and $m_1 \neq m_1'$ and get two tags $t = t_0 \| t_1$ and $t' = t_0' \| t_1'$ respectively

$\mathcal{A}$ output a message $\tilde{m} = m_0 \| m_1'$ and a tag $\tilde{t} = t_0 \| t_1'$

Clearly $\tilde{t}$ is a correct tag for $\tilde{m}$ and therefore $Vrfy_k(\tilde{m}, \tilde{t}) = 1$

Since $\tilde{m} \in Q$ and $\mathcal{A}$ succeeds with a probability 1, the scheme is not secure

2. Let $x = x_1 x_2 x_3 x_4 x_5$ be a $5n$-bits message, $x_6 = L$ = length of x



Assume h^s is coll-resistant, prove H^s is coll-resistant

Proof by contradiction:

Assume $H^s(x) = H^s(x')$ where $x = x_1 x_2 x_3 x_4 x_5 x_6$, $x' = x_1' x_2' x_3' x_4' x_5' x_6'$ and $x \neq x'$

If $L \neq L'$, $L \| Z_5 \neq L' \| Z_5'$, but we have $H^s(x) = H^s(x') = h^s(L \| Z_5) = h^s(L' \| Z_5')$

There is a collision in h^s

If $L = L'$ and $Z_5 \neq Z_5'$, for the same reason above, there is a collision in h^s

If $L = L'$, $Z_5 = Z_5'$, $X_5 \neq X_5'$, then $X_5 \| Z_4 \neq X_5' \| Z_4'$, but $h^s(X_5 \| Z_4) = h^s(X_5' \| Z_4')$. There is a collision in h^s

If $L = L'$, $Z_5 = Z_5'$, $X_5 = X_5'$, $Z_4 \neq Z_4'$, for the same reason above, there is a collision in h^s

If $L=L'$, $z_5=z_5'$, $x_5=x_5'$, $z_4=z_4'$, $x_4\neq x_4'$, then $x_4||z_3 \neq x_4'||z_3'$, but $h^g(x_4||z_3)=h^g(x_4'||z_3')$, There is a collision in h^g

If $L=L'$, $z_5=z_5'$, $x_5=x_5'$, $z_4=z_4'$, $x_4=x_4'$, $z_3\neq z_3'$, for the same reason above, there is a collision in h^g

If $L=L'$, $z_5=z_5'$, $x_5=x_5'$, $z_4=z_4'$, $x_4=x_4'$, $z_3=z_3'$, $x_3\neq x_3'$, then $x_3||z_2 \neq x_3'||z_2'$, but $h^g(x_3||z_2)=h^g(x_3'||z_2')$. There is a collision in h^g

If $L=L'$, $z_5=z_5'$, $x_5=x_5'$, $z_4=z_4'$, $x_4=x_4'$, $z_3=z_3'$, $x_3=x_3'$, $z_2\neq z_2'$, for the same reason above, there is a collision in h^g

If $L=L'$, $z_5=z_5'$, $x_5=x_5'$, $z_4=z_4'$, $x_4=x_4'$, $z_3=z_3'$, $x_3=x_3'$, $z_2=z_2'$, $x_2\neq x_2'$, then $x_2||z_1 \neq x_2'||z_1'$, but $h^g(x_2||z_1)=h^g(x_2'||z_1')$ There is a collision in h^g

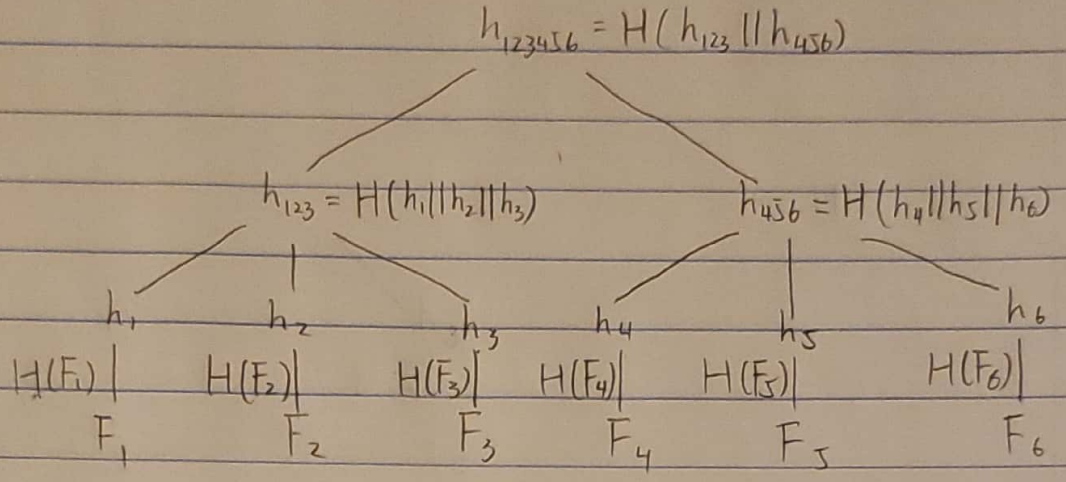
If $L=L'$, $z_5=z_5'$, $x_5=x_5'$, $z_4=z_4'$, $x_4=x_4'$, $z_3=z_3'$, $x_3=x_3'$, $z_2=z_2'$, $x_2=x_2'$ $z_1\neq z_1'$, by the same reason above, there is a collision in h^g

If $L=L'$, $z_5=z_5'$, $x_5=x_5'$, $z_4=z_4'$, $x_4=x_4'$, $z_3=z_3'$, $x_3=x_3'$, $z_2=z_2'$, $x_2=x_2'$, $z_1=z_1'$ $x_1\neq x_1'$, then $x_1||z_0 \neq x_1'||z_0'$, but $h^g(x_1||z_0)=h^g(x_1'||z_0')$, there is a collision in h^g.

$z_0\neq z_0'$ cannot happen, so in conclusion, $x_1=x_1'$, $x_2=x_2'$, $x_3=x_3'$, $x_4=x_4'$, $x_5=x_5'$, $x_6=x_6'$, which contradicts the assumption

Therefore, H^g is coll-resistant

3(a)



3(b) Alice stores the root hash h_{123456} on her computer

4(a) Bob sends h_1', h_2', h_{456}' and F_3' to Alice

Then Alice computes $h_3' = H(F_3')$, $h_{123}' = H(h_1' || h_2' || h_3')$, $h_{123456}' = H(h_{123}' || h_{456}')$ and checks if $h_{123456} = h_{123456}'$

4(b) Suppose Bobs send F_3', h_1', h_2', h_{456}' such that $F_3' \neq F_3$, $h_3' = H(F_3')$, $h_{123}' = H(h_1' || h_2' || h_3')$, $h_{123456}' = H(h_{123}' || h_{456}')$

Since $F_3 \neq F_3'$, H is coll-resistant, it is impossible that $h_3 = h_3'$

Since $h_3 \neq h_3'$, H is coll-resistant, it is impossible that $h_{123} = h_{123}'$

Since $h_3 \neq h_3'$, $h_{123} \neq h_{123}'$, H is coll-resistant, it is impossible that $h_{123456} = h_{123456}'$

Therefore, it's hard to find F_3' such that $F_3' \neq F_3$, $h_{123456} = h_{123456}'$