Recitation 3 (2/27/2015) Katerina Sotiraki | 6.857

Suggested reading: Katz/Lindell chapter 5.

Theorem: If h is CR, then h is TCR.

proof sketch:
Assume h is not TCR, then given an x, the adversary can find an $x' \neq x$ such that $h(x) = h(x')$.
But, then x, x' form a collision, which is a contradiction since the hypothesis says that h is CR.

Remark: If h is TCR, then h is not necessarily CR

example: $h: \{0,1\}^n \rightarrow \{0,1\}^n$, $h(x) = \begin{cases} 0^n, & \text{if } x = 1^n \\ x, & \text{otherwise} \end{cases}$

then h is TCR since given a uniformly random $x \in \{0,1\}^n$ the probability that we can find an x' such that $h(x) = h(x')$ and $x = x'$ is $\frac{2}{2^n}$ (for $x = 0^n$ and $x = 1^n$).
But, $h(0^n) = h(1^n)$, so h is not CR.

Theorem: h is OW $\not\Leftrightarrow$ h is CR.

proof sketch:
If $h(x) = x$, then h is CR, but h is not OW.
If $h(x) = \begin{cases} 0^n, & \text{if } x = 0^n \\ 0^n, & \text{if } x = 1^n \\ f(x), & \text{otherwise} \end{cases}$ where f is OW,
then h is OW, but $h(0^n) = h(1^n) = 0^n$ so h is not CR.

Why h is OW?
If h was not OW, then it would be "feasible" given $y \in \{0,1\}^n$ such that $y = h(x)$ and $x \xleftarrow{R} \{0,1\}^n$ to find x' such that $h(x) = h(x')$.
But, then f is not OW, since in most of the inputs we have that $h(x) = f(x)$.

Exercise: Assume $h: \{0,1\}^{n+1} \longrightarrow \{0,1\}^n$ and there are exactly two x_1, x_2 such that $h(x_1) = h(x_2)$.
If h is CR, then h is OW.

proof sketch:
Assume h is not OW, then given y such that $y = h(x)$ and $x \leftarrow \{0,1\}^{n+1}$, it is "feasible" to find an x' such that $h(x) = h(x')$
If we prove that with non-negligible propability $x \neq x'$, then it is "feasible" to find collisions, which is a contradiction (since we assume that h is CR).
So, h has to be OW.
What is the probability that $x \neq x'$?
From the hypothesis we know that there are exactly two x_1, x_2 such that $h(x_1) = h(x_2) = y$. Since, $x \xleftarrow{R} \{0,1\}^{n+1}$
$$\Pr(x = x_1) = \Pr(x = x_2) = 1/2$$
$$\text{So, } \Pr(x \neq x') = \Pr(x \neq x' \mid x = x_1) \cdot \Pr(x = x_1) + \Pr(x \neq x' \mid x = x_2) \cdot \Pr(x = x_2)$$
$$= \Pr(x' \neq x_1) \cdot 1/2 + \Pr(x' \neq x_2) \cdot 1/2 =$$
$$= 1/2 \cdot 1 = 1/2$$
(since x' is either x_1 or x_2).

Exercise: (ex. 5.13 Katz/Lindell) Let t be the number of leaves of a Merkle tree, $\mathcal{M}$. Can we find another Merkle tree with $t/2$ leaves that has the same root as $\mathcal{M}$?

Yes, let $(x_1, \dots, x_t)$ be the leaves of $\mathcal{M}$, then if $h(x_{2i-1} \| x_{2i})$, $i = 1, \dots, t-1$ are the $t/2$ leaves of $\mathcal{M}'$ then $\mathcal{M}$ and $\mathcal{M}'$ have the same root.

Theorem: (Th. 5.11 Katz/Lindell) Let h be CR, then $\mathcal{M}T_h$ is CR, where $\mathcal{M}T_h$ is the root of the Merkle tree that uses h, for a fixed t (number of leaves).

proof sketch:
If $\mathcal{M}T_h$ was not collision resistant, then we could find set of leaves $(x_1, \dots, x_t)$, $(x_1', \dots, x_t')$ such that $(x_1, \dots, x_t) \neq (x_1', \dots, x_t')$, but $\mathcal{M}T_h(x_1, \dots, x_t) = \mathcal{M}T_h(x_1', \dots, x_t')$

So, there would be a level i such that the nodes of level i of the two trees will be equal, but the nodes of level $i+1$ will not be equal.
Then, this will give a collision for h, which is a contradiction.

<u>Exercise</u>: Assume h is OW, CR, TCR, PR, non-malleable, ...
Let H be the hash function that we get from Merkle-Damgard construction using h.
Is H non-malleable?

No, H is malleable, because given $H(m)$, we can find (without knowing m) $H(pad(m)\|c)$, where $pad(m)$ is the padded message m and c is a string of our choice.
These attacks are known as "extension attacks".

<u>Exercise</u>: Let h be a length-preserving OW function, is $h'(x) = h(h(x))$ OW?

No. Let $f(x\|y) = h(y)\|0^n$ where $|x|=|y|=n$.
Then, f is a length-preserving OW function, since if we could "invert" f, we could "invert" h as well.
But, $f(f(x,y)) = f(h(y)\|0^n) = h(0^n)\|0^n$, which is not OW.

Why ~~the~~ proving the contrapositive is not possible?
Assume h' is not OW, then from $h(h(x))$ we can get x' such that $h(h(x)) = h(h(x'))$.
But, to prove that h is not OW, we need to be able to recover an x' from $h(x)$ such that $h(x)=h(x')$.
If given $y=h(x)$, we apply h and invert $h(y)=h(h(x))$ then we will get an x' such that $h(h(x))=h(h(x'))=h(y)$.
But, can we argue that $h(x')=y$? No.