Topic: OWF, UOWHF & CRHF | Date: Nov 7, 2024
Lecturer: Wei-Kai Lin (TA: Arup Sarker) | Scriber: Jinye He, Yanchen Liu

---

In the last lecture, we begin to introduce the Cryptographic hash functions. We start with recapping the universal one-way hash function (UOWHF) and collision resistant hash function (CRHF).

1 UOWHF v.s. CRHF

Definition 1 (Universal One-Way Hash Functions)**.** Let Gen_H be the key generation function and $H = \{H_k(\cdot) : \{0,1\}^{d(n)} \to \{0,1\}^{r(n)}, k \leftarrow Gen_H(1^n)\}$ be a set of functions. The pair (Gen_H, H) is a family of universal one-way hash functions (UOWHF) if:

- Compressing: $d(n) > r(n)$ for all n.
- Efficient: Gen_H is in PPT, H is deterministic PT.
- Security/Second Preimage Collision Resistant: ∀NUPPT A, there exists a negligible function ϵ such that

$$\Pr\left[\begin{array}{l} x \neq x' \\ H_k(x) = H_k(x') \end{array} : \begin{array}{l} k \leftarrow \text{Gen}_H(1^n) \\ (x, st) \leftarrow A(1^n) \\ x' \leftarrow A(st, k) \end{array}\right] \leq \epsilon(n) \quad \forall n \in \mathbb{N}$$

Remark: Because the adversary A chooses both x and x', the key k is necessary to defend against non-uniform adversaries; otherwise, a non-uniform A can just remember a colliding pair (x, x') for every problem size $n \in \mathbb{N}$. Many practical hash functions (such as SHA) are unkeyed and do not satisfy this definition.

Definition 2 (Collision-Resistant Hash Function)**.** Let Gen_H be the key generation function and $H = \{H_k(\cdot) : \{0,1\}^{d(n)} \to \{0,1\}^{r(n)}, k \leftarrow Gen_H(1^n)\}$ be a set of functions. The pair (Gen_H, H) is a family of collision-resistant hash functions (CRHF) if:

- Compressing: $d(n) > r(n)$ for all n.
- Efficient: Gen_H is in PPT, H is deterministic PT.
- Security/Second Preimage Collision Resistant: ∀NUPPT A, there exists a negligible function ϵ such that Let Gen_H be the key generation function and $H = \{H_k(\cdot) : \{0,1\}^{d(n)} \to \{0,1\}^{r(n)}, k \leftarrow Gen_H(1^n)\}$ be a set of functions. The pair (Gen_H, H) is a family of universal one-way hash functions (UOWHF) if:
  - Compressing: $d(n) > r(n)$ for all n.
  - Efficient: Gen_H is in PPT, H is deterministic PT.
  - Security/Second Preimage Collision Resistant: ∀NUPPT A, there exists a negligible function ϵ such that

$$\Pr\left[\begin{array}{l} x \neq x' \\ H_k(x) = H_k(x') \end{array} : \begin{array}{l} k \leftarrow \text{Gen}(1^n) \\ (x, x') \leftarrow A(1^n, k) \end{array}\right] \leq \epsilon(n) \quad \forall n \in \mathbb{N}$$

Remark: The syntax, compression, and efficiency of CRHF are the same as those of UOWHF. The only defference is the secuity definition.

Relationships Between Hash Functions

- CRHF $\Rightarrow$ UOWHF
- CRHF $\Leftarrow$ UOWHF*?* TBD
- UOWHF $\Rightarrow$ OWF
- UOWHF $\Leftarrow$ OWF

Summarily, we have the following relationships now:

$$\text{CRHF} \Longrightarrow \text{UOWHF} \Longleftrightarrow \text{OWF}$$

Remark: UOWHF $\Rightarrow$ OWF[1]. By giving a function $f(\text{rd}, x) := H_{Gen_H(1^n:\text{rd})}(x)$, where rd is a random input. Here $f(rd, x)$ is also an OWF. The key difference between OWF and UOWHF is that the first one needn't key but the later does.

2 Merkle-Damgård Construction

Suppose there is a UOWHF compressing $d = d(n)$ inputs to $r = r(n)$ outputs? Is it possible to use this UOWHF to compress longer input? Fortunately, Merkle-Damgård Construction discribed in the following figure gives a positive answer.

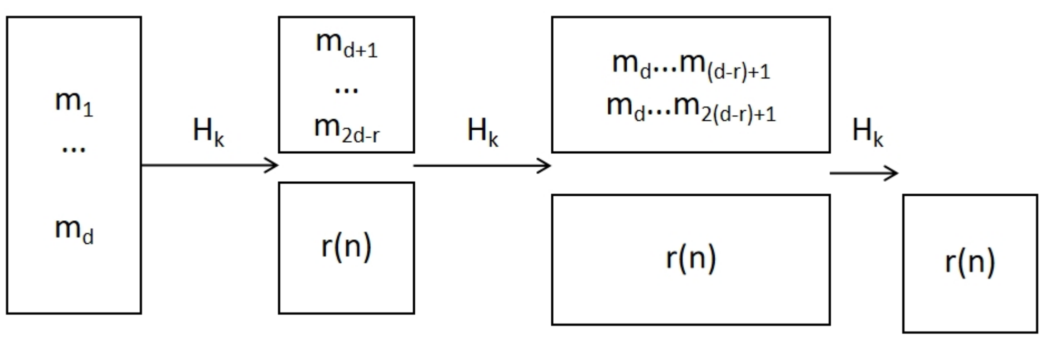

Figure 1: Merkle-Damgård Construction Diagram

What if the shorter output? It is not clear. Consider the attempt $H'_k(x) = H_k(x)[1...r-1]$. Suppose $H'_k(x) = H(x)$ for $x' \neq x$, It is possible x, x' won't collide in H_k.

[1]The other direction is non-trivial. You can find the proof in this lecture note.

3 Hash and MAC

Based on CRHF, we can construct an MAC that can authenticate arbitrarily length of message.

Construction

Let (Gen, Tag, Ver) be an MAC defined in last lecture, and (Gen_H, H) be a CRHF, we define our new MAC'= (Gen', Tag', Ver') as follows:

- Gen'(1^n) :
  - $k \leftarrow \text{Gen}(1^n)$
  - Output k
- Tag'$_k(m)$:
  - $s \leftarrow \text{Gen}_H(1^n)$
  - $v \leftarrow H_s(m)$
  - $\theta \leftarrow \text{Tag}_k(v)$
  - Output $(s, \theta) =: \theta'$
- $\text{Ver}_k(m, \theta' = (s, \theta))$:
  - $v \leftarrow H_s(m)$
  - Output $\text{Ver}_k(v||s, \theta)$

Security Game

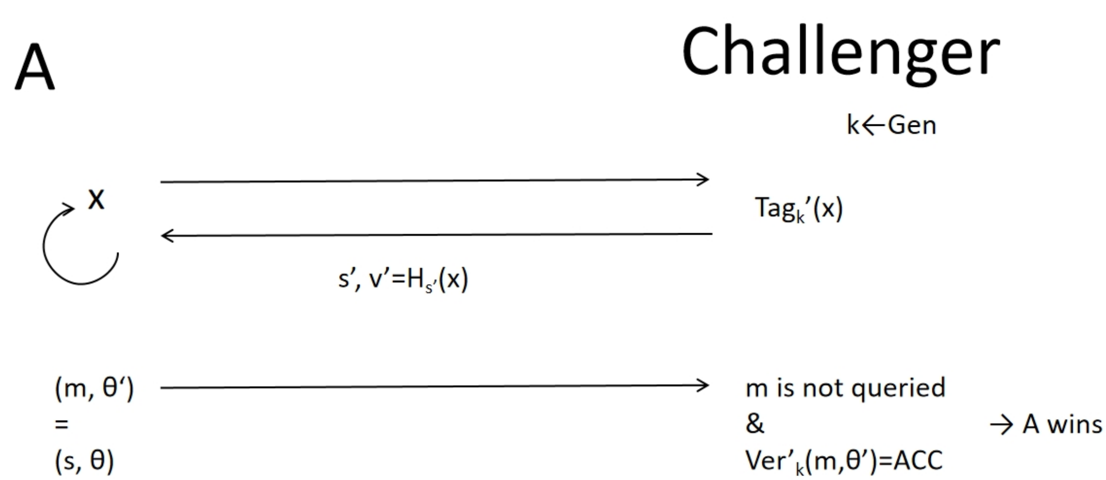

Figure 2: Game Flow

$$\begin{aligned}
\Pr[A \text{ wins}] &= \Pr\left[A \text{ wins} \wedge \text{collision}\right] + \Pr[A \text{ wins} \wedge \neg\text{collision}] \\
&= \Pr\left[A \text{ wins} \wedge \text{collision}\right] + \Pr[A \text{ wins}|\neg\text{collision}] \cdot \Pr[\neg\text{collision}] \\
&\leq \Pr[\text{collision}] + \Pr[A \text{ wins} \mid \neg\text{collision}] \cdot \mathbf{1}
\end{aligned}$$

where the event of collision is $m \neq m' \wedge H_s(m) = H_s(m')$

By the definition of CRHF the first term is negligible and by the security of MAC the second term is also negligible. Therefore, the new MAC' we construct is also secure.