MAD 4471: Cryptography and Coding Theory **Fall 2020**

Lecture 5: Message Authentication Codes (MAC)

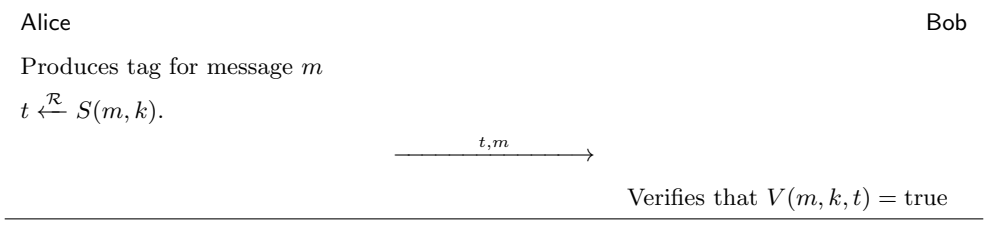
Lecturer: Jean-François Biasse *TA: William Youmans*

5.1 MAC

So far, we have been concerned about encrypting messages. This is not the only task in cryptography. Another important problem is to ensure message integrity.For example, detecting if someone has tampered with data. Here, we do not care about privacy, but it is possible to provide privacy and integrity via "Authenticated encryption" (ex. TSL protocol). To provide integrity, we use a Message Authentication Code (MAC).

Definition 5.1 (Message Authentication Code (MAC)) *A MAC I is made of a signing function $S : \mathcal{M} \times \mathcal{K} \mapsto \mathcal{T}$ and a verification function $V : \mathcal{M} \times \mathcal{K} \times \mathcal{T} \mapsto \{'yes', 'no'\}$ where $\mathcal{T}$ is a tag space (which intuitively has to be large enough to prevent brute force attacks but small enough to allow good performances).*

Figure 5.1: Message Authentication Code



Remark 1 *We need a secret k to ensure integrity. If there is no secret, anyone can authenticate a fake message m.*

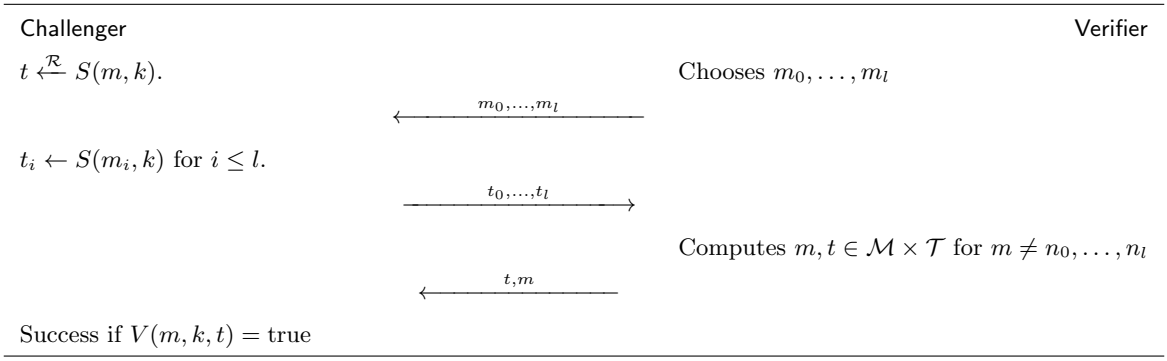
Remark 2 *The security of a MAC relies on the assumption that an adversary cannot forge an authenticated message. We can assume that the adversary has access to pairs (m_i, tag) of valid signatures.*
Here is the game defining the security of a MAC $I = (S, V)$.

Definition 5.2 (Advantage against a MAC) *The advantage is*

$$Adv_{MAC}[A, I] = Pr_{k \leftarrow \mathcal{K}}[\ Adversary\ succeeds].$$

$I = (S, V)$ is secure if for all efficient adversaries, $Adv_{MAC}(A, I)$ is negligible.

Figure 5.2: MAC security game



5.2 The security of a MAC

We want to prove that if we use a MAC with a secure PRF, then it is a secure MAC. This directly derive from the following statement.

Theorem 5.3 *Let $F : X \times \mathcal{K} \mapsto Y$ be a PRF and $I = (S, V)$ be a MAC defined by*

- $S(m,k) = F(m,k)$
- $V(m,h,t) =' yes'$ *if*$\mathcal{A} = F(m,k)$

Then for each efficient adversary $\mathcal{A}$ against F, there is an adversary $\mathcal{B}$ against F such that

$$Adv_{MAC}[\mathcal{A}, I] \leq Adv_{PRF}[\mathcal{B}, F] + \frac{1}{|Y|}$$

Proof: Assume $\mathcal{A}$ is playing the MAC security game against the MAC I_0 defined by F. We call $W_0^{'}$ the event "$\mathcal{A}$ succeeds against I_0".
Assume now that $\mathcal{A}$ is playing the MAC security game where instead of drawing $h \in \mathcal{K}$ and using $F(\cdot, h)$, the challenge draws $f \in Func(X, Y)$ and uses it in a MAC I_1. We call $W_1^{'}$ the event "$\mathcal{A}$ secured against I_1.

$Adv_{MAC}[\mathcal{A}, I] = Pr(W_0^{'}) = Pr(W_1^{'}) + Pr(W_0^{'}) - Pr(W_1^{'})$

As the adversary cannot do anything against a random function, its probability of success against I_1 is $\frac{1}{|Y|}$ (choice of a tag at random in Y). So $Pr(W_1^{'}) = \frac{1}{|Y|}$.
Now, we can define a PRF adversary $\mathcal{B}$ for F that outputs 0 if $\mathcal{A}$ succeeds and 1 if $\mathcal{A}$ fails.
Then:

$$Adv_{PRF}(\mathcal{B}, F) = |Pr(W_0^{'}) - Pr(W_1^{'})|$$

Finally

$$\begin{aligned} Pr(W_0^{'}) &= |Pr(W_1^{'}) + Pr(W_0^{'}) - Pr(W_1^{'})| \\ &\leq Pr(W_1^{'}) + |Pr(W_0^{'}) - Pr(W_1^{'})| \\ &= \frac{1}{|Y|} + Adv_{PRF}(\mathcal{B}, F) \end{aligned}$$

■

5.3 MAC with a hash function

There is one little problem with the MAC we have described from PRF's. We can only sign messages in X (where the PRF is from $X \times \mathcal{K}$ to Y). X is typically 128 or 256 bits, but messages can be very long!. In HMAC, we use a hash function. It is a function $h : \mathcal{M} \mapsto X$ with $|\mathcal{M}| \gg |X|$.

Question What makes a hash function secure for cryptography? Indeed, there's no key!.
Answer We want to prevent the adversary from finding collisions.

Definition 5.4 (Collision resistance) *h is collision - resistant if there is no efficient algorithm $\mathcal{A}$ that can find $m_0, m_1 \in \mathcal{M}$ such that $h(m_0) = h(m_1)$ with no negligible probability.*

$$Adv_{CR}(\mathcal{A}, h) = Pr(\mathcal{A} \text{ outputs a collision for} h)$$

So, if $I = (S, V)$ is a MAC that authenticates small messages, we can define $I^{'} = (S^{'}, V^{'})$ by

- $S^{'}(m, k) = S(h(m), k)$
- $V^{'}(m, k, t) = V(h(m), k, \mathcal{K})$

Theorem 5.5 *If I is secure and h is collision-resistant, then $I^{'}$ is secure.*

Proof: In assignment ■

5.4 Finding collisions

To ensure the security of HMAC, we must use collision- resistant hash functions. Let $H : \mathcal{M} \to \mathcal{T}$ be a hash function. There is a trivial way to find messages in $\mathcal{M}$ with the same tag in $\mathcal{T}$ (i.e. to find collitions). It consists in drawing elements of $\mathcal{M}$ at random until we find one. It is not very smart, but the expected number of trials before finding a collision is on average significantly less than $N := |\mathcal{T}|$. In the worst case however, one might have to draw $N + 1$ messages in $\mathcal{M}$ before obtaining a collision, but this statistically never happens. This phenomenon is called the "Birthday paradox".

Theorem 5.6 *Let $0 < x < 1$. If we draw $n \geq \sqrt{2 \ln \left(\frac{1}{x}\right)} \sqrt{N}$ elements uniformly at random in $\mathcal{M}$, the probability of finding a collision is at least x.*

Proof: Let us calculate the probability of <u>not</u> finding a collision after trying n times.

$$\begin{aligned} Pr(\text{no collision}) &= (\frac{B-1}{B})(\frac{B-2}{B})....(\frac{B-n+1}{B}) \\ &= \prod_{i=1}^{n-1}(1-\frac{i}{B}) \\ &\leq \prod_{i=1}^{n-1} e^{\frac{-i}{B}} \text{because} 1-x \leq e^{-x} \\ &= e^{\sum_{i=1}^{n-1}\frac{-i}{B}} = e^{\frac{-n^2}{2B}} \end{aligned}$$

Therefore, the probability of finding a collision satisfies:

$$\begin{aligned} Pr(\text{collision}) &= 1 - Pr(\text{no collision}) \\ &\geq 1 - e^{\frac{-n^2}{2B}} \end{aligned}$$

To ensure that this probability be at least $\frac{1}{2}$ we must have

$$\begin{aligned} e^{\frac{-n^2}{2B}} \geq \frac{1}{2} &\iff \frac{-n^2}{2B} \geq \ln(\frac{1}{2}) \\ &\iff n^2 \geq 2\ln(2)\cdot B \\ &\iff n \geq \sqrt{2\ln(2)}\cdot\sqrt{B} \end{aligned}$$

■

Remark 3 *This means that the sign of X must account for the "birthday attack". If we want to make some that an attack take at least 2^{128} operations, $|X|$ must be at least 2^{256}.*