1 MAC Construction

There several ways to construct a MAC, each having its advantages and disadvantages.

1.1 A PRF is a CMA-secure MAC

A PRF, using a key $k$, can be used as a (deterministic) MAC using following steps:

**KeyGen:** $k \leftarrow K$

**MAC:** $\sigma = MAC_k(m) = f_k(m)$. $(m, \sigma)$ is sent to the recipient.

**Verify:** Return $f_k(m) == \sigma$

**Theorem 1 (f-PRF $\Rightarrow$ MAC$_f$-CMA)** If $f$ is a PRF, then MAC scheme using $f$ is CMA-secure.

**Proof.** We will prove the contrapositive, $\neg$MAC$_f$-CMA $\Rightarrow$ $\neg$f-PRF. See Figure 1.1.

$A$ thinks that it is interacting with Signing and Verification oracles of the MAC scheme, where in fact it is communicating with $B$. It sends to $B$ message $m_i$. $B$ sends $m_i$ to the Challenger. The Challenger chooses a world, and returns $MAC_i = g(m_i)$, where $g()$ depends on the world the Challenger chooses. $B$ sends $MAC_i$ to $A$ (this way $B$ simulates the signing oracle to $A$). $A$ produces a possible forgery: a message $M$, and it's corresponding message authentication code $MAC'_{new}$, and sends it to $B$. $B$ sends message $M$ to teh challenger. The challenger takes $M$, and return $MAC' = g(M)$. $B$
Figure 2: \( \neg \text{MAC}_f\text{-CMA} \Rightarrow \neg f\text{-PRF} \)

compares if \( \text{MAC}_{\text{new}} \) equals to \( \text{MAC}' \). If they are equal, then it sends \( d = 1 \) to \( \mathcal{A} \) (this simulates the verification oracle to \( \mathcal{A} \)) and the Challenger, otherwise it sends \( d = 0 \) to \( \mathcal{A} \) and the Challenger.

\[
\text{Adv}_{f}^{\text{PRF}}(\mathcal{B}) = Pr(\text{Exp}_{f}^{\text{PRF}-1}(\mathcal{B}) = 1) - Pr(\text{Exp}_{\text{PRF}-0}(\mathcal{B}) = 1)
\]

\[
= \text{Adv}_{f_k}^{\text{CMA}}(\mathcal{A}) - \frac{1}{2^l}
\]

\[
\Rightarrow \text{Adv}_{f}^{\text{PRF-MAC}}(\mathcal{A}) = \text{Adv}_{f}^{\text{PRF}}(\mathcal{B}) + \frac{1}{2^l} \leq \epsilon + \frac{1}{2^l}
\]

This completes the proof.

**Note:** While this construction of MAC using a PRF is simple, it doesn’t allow authentication of messages larger than \( l \) bits.

### 1.2 CBC-MAC

One can encode longer messages by dividing a message into blocks and chaining them, similar to CBC-DES.

This chaining is different than CBC-DES; there is no IV value (and therefore the MAC is deterministic) and also the output is only one block.
Fact. CBC-MAC can only work with fixed number of blocks.

Proof. We will provide an example where the number of blocks is not fixed, and show that this leads to a forgery.

\( A \) sends Signer/Verifier message block \( m_{11} \), and Signer/Verifier responds with a message authentication code \( MAC_{11} = f_k(m_{11}) \). \( A \) sends message \( (m_{12} \oplus MAC_{11}) \) to Signer/Verifier. \( A \) receive in response \( MAC_{12} = f_k(m_{12} \oplus MAC_{11}) \). \( A \) sends \( ((m_{11}||m_{12}), MAC_{\text{new}}) \) as a forgery to Signer/Verifier, where \( MAC_{\text{new}} = MAC_{12} \). We know this is a valid forgery, because message authentication code of \( (m_{11}||m_{12}) \) will be \( f_k(m_{12} \oplus f_k(m_{11})) \), which is exactly \( MAC_{12} \). See Figure 1.2.

Theorem 2 \((f\text{-PRF} \Rightarrow \text{CBC-MAC-CMA})\) If \( f_k \) is a PRF, then CBC-MAC is CMA secure.

Proof. We’ll prove the contrapositive \( \neg\text{CBC-MAC-CMA} \Rightarrow \neg f\text{-PRF} \).

\( A \) sends a query message \( m_i \), which is divided into blocks \( m_{i1}, m_{i2}, ..., m_{in} \), to \( B \). \( B \) then sends \( m_{i1} \) to the challenger, and repetedly XORs the value received from the challenger with teh next block and send it to the challenger. The response corresponding to the last block will be the (simulated) MAC on the message \( m_i \). \( B \) sends back the MAC to \( A \). \( A \) continues to send \( q \) such messages to \( B \). Eventually, \( A \) decides it is ready to create a forgery. \( A \) then sends message \( M \), consisting of \( n \) blocks \( M_{11}, M_{12}, ..., M_{1n} \), and a message authenticated code \( MAC_{\text{new}} \), to \( B \). \( B \) forwards the message blocks in the same manner as was done was previously quieried messages \( m_i \), and finally obtains the corresponding MAC \( MAC' \) on \( M \). If \( MAC_{\text{new}} \) equals \( MAC' \), then \( B \) sends \( A \), and the Challenger, \( d = 1 \). Otherwise, it sends \( A \), and the Challenger, \( d = 0 \).

\[
\text{Adv}^\text{PRF}_{g}(B) = Pr(\text{Exp}^\text{PRF-1}_{f}(B) = 1) - Pr(\text{Exp}^\text{PRF-0}_{f}(B))
\]
The factor $\triangle$ above will be determined using the following Lemma.

Lemma: Birthday Attack on CBC-MAC instantiated with a random function.

Proof. Adversary $A$ recorded $q$ responses $(\sigma_1, \sigma_2, ..., \sigma_q)$, when it queried the signing oracle on messages $m_1, m_2, ..., m_q$.

Note that we are concerned with the case when the challenger was in World 0, i.e., when $g$ was set to be a random function denoted by $F$.

If any of the two responses collide, i.e., if $\sigma_i = \sigma_j$ (for some $i, j$), then

$$F(m_{i,n} \oplus F(m_{i,n-1})) = F(m_{j,n} \oplus F(m_{j,n-1}))$$

Since $F$ is a random, the above equality will hold if and only if $m_{i,n} \oplus F(m_{i,n-1}) = m_{j,n} \oplus F(m_{j,n-1})$.
Figure 5: f-PRF ⇒ CBC-MAC-CMA
Then, for any binary string $B$ of length $l$-bits, we have $m_{i,n} \oplus B \oplus F(m_{i,n-1}) = m_{j,n} \oplus B \oplus F(m_{j,n-1})$

The adversary can make another query $m_{i,1}, m_{i,2}, ..., m_{i,n} \oplus B$, and receive in return MAC $\sigma'_i$

And then the adversary can create a forgery by sending $m_{j,1}, m_{j,2}, ..., m_{j,n} \oplus B \oplus B$ as the message and $\sigma'_i$ as the corresponding MAC.

Therefore, if the responses of any two previously queried $q$ messages collide, then the adversary can produce a valid forgery. This means that the probability that the adversary wins even when it is fed the responses of a random function is $\Delta \leq \frac{q(q-1)}{2^l}$ (from the upper bound of the birthday attack).

Completing the proof:

$$Adv_{g}^{PRF}(B) = Pr(Exp_{f}^{PRF-1}(B) = 1) - Pr(Exp_{f}^{PRF-0}(B))$$

$$\leq Adv_{CBC-MAC}^{CMA}(A) - \frac{q(q-1)}{2^l}$$

$$\Rightarrow Adv_{CBC-MAC}^{CMA}(A) \leq Adv_{f}^{PRF}(B) + \frac{q(q-1)}{2^l}$$

### 1.3 HMAC: MAC construction based on Hash Functions

HMAC is derived from NMAC (Nested MAC)

$$NMAC_{k_1, k_2}(x) = h^*_k(H^*_k(x))$$

![Figure 6: $H^*_k(x)$](image)
Theorem 3  If $h_{k_1}^*$ is a CMA-secure MAC, and given that $H_{k_2}^*$ is collision resistant, then NMAC is CMA-secure.

In the next lecture, we will prove this theorem.