1 Construction of MAC Schemes

There are many ways of constructing MAC Schemes, with each scheme having its own advantage and disadvantage.

1.1 PRF-based MAC

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

**KeyGen**: $K \leftarrow \text{KeysSpace}$

**MAC**: Input $m$

$\mu = F_k(m)$

Output $(m, \mu)$

**Verify**: Input $(m, \mu)$

If $F_k(m) = \mu$

**Theorem 1** ($F_k\text{-PRF} \Rightarrow \text{PRF-MAC-CMA}$) PRF based MAC is CMA secure. If $F_k$ is a PRF, then PRF-MAC is CMA.

**Proof.** We will prove the contrapositive, $\neg\text{PRF-MAC-CMA} \Rightarrow \neg F_k\text{-PRF}$. See Figure 2.
If there exists an adversary \( \mathcal{A} \) who can break PRF-MAC with respect to CMA security then we can construct \( \mathcal{B} \) who can break \( F_k \) with respect to PRF property. The adversary \( \mathcal{A} \) assumes that it is interacting with Signing and Verification oracles of the MAC scheme, where in fact it is communicating with adversary \( \mathcal{B} \). \( \mathcal{A} \) sends message \( m_i \) to \( \mathcal{B} \). \( \mathcal{B} \) forwards \( m_i \) to the Challenger. The Challenger chooses a world, and returns \( MAC_i = g(m_i) \), where \( g() \) depends on the world the Challenger chooses. \( \mathcal{B} \) forwards \( MAC_i \) to \( \mathcal{A} \) (this way \( \mathcal{B} \) simulates the signing oracle to \( \mathcal{A} \)). \( \mathcal{A} \) produces a possible forgery: a message \( M \), and it’s corresponding message authentication code \( MAC_{\text{new}} \), and sends it to \( \mathcal{B} \). \( \mathcal{B} \) sends message \( M \) to the challenger. The challenger takes \( M \), and returns \( MAC' = g(M) \). \( \mathcal{B} \) compares if \( MAC_{\text{new}} \) equals to \( MAC' \). If they are equal, then it sends \( d = 1 \) to \( \mathcal{A} \) (this simulates the verification oracle to \( \mathcal{A} \)) and the Challenger, otherwise sends \( d = 0 \) to \( \mathcal{A} \) and the Challenger.

\[
\text{Adv}_{\text{PRF}}(\mathcal{B}) = Pr(\text{Exp}_{\text{PRF}}^{-1}(\mathcal{B}) = 1) - Pr(\text{Exp}_{\text{PRF}}^{-0}(\mathcal{B}) = 1) \\
= \text{Adv}_{\text{CMA}}^{f_k}(\mathcal{A}) - \frac{1}{2^l} \\
\Rightarrow \text{Adv}_{\text{PRF-MAC}}(\mathcal{A}) = \text{Adv}_{\text{PRF}}(\mathcal{B}) + \frac{1}{2^l} \leq \epsilon + \frac{1}{2^l}
\]

Figure 2: \( \neg \text{PRF-MAC-CMA} \Rightarrow \neg F_k \text{-PRF} \)
Thus we have proved the theorem.

1.2 How to generate MACs on arbitrarily long messages?

Chaining mechanism is used to create MACs on arbitrarily long messages. This cascading effect securely guards against 2 similar blocks of messages. See figure 3.

![Diagram showing the chaining mechanism for generating MACs](image)

Figure 3: Is this CMA secure?

\[ \mu_i = F_k(\mu_i) \ (m_1, m_2, ..., m_n, \mu_1, \mu_2, ..., \mu_n) \]

This scheme is inefficient because of the size of the output. This method is not secure because we can make different permutations of the message blocks: \((m_1, m_2, ..., m_n, \mu_1, \mu_2, ..., \mu_n)\) can be changed to \((m_2, m_1, ..., m_n, \mu_2, \mu_1, ..., \mu_n)\)

1.3 CBC-MAC

One can generate MACs on arbitrarily long messages by dividing the message into blocks and then 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. In CBC-MAC, IV is a sequence of all zeros.

**Theorem 2** (\(F_k\)-PRF \(\Rightarrow\) CBC-MAC-CMA) *If \(F_k\) is a PRF, then CBC-MAC is CMA secure.*
Proof. We’ll prove the contrapositive \( \neg \text{CBC-MAC-CMA} \Rightarrow \neg F_k\text{-PRF} \).

If there exists an adversary \( \mathcal{A} \) who can break CBC-MAC with respect to CMA security then we can construct adversary \( \mathcal{B} \) who can break \( F_k \) with respect to PRF property. \( \mathcal{A} \) sends a query message \( m_i \), which is divided into blocks \( m_{i1}, m_{i2}, ..., m_{in} \), to \( \mathcal{B} \). \( \mathcal{B} \) then sends \( m_{i1} \) to the challenger, and repetedly XORs the value received from the challenger with the next block and send it to the challenger. The response corresponding to the last block will be the (simulated) MAC on the message \( m_i \). \( \mathcal{B} \) sends back the MAC to \( \mathcal{A} \). \( \mathcal{A} \) continues to send \( q \) such messages to \( \mathcal{B} \). Eventually, \( \mathcal{A} \) decides it is ready to create a forgery. \( \mathcal{A} \) then sends message \( M \), consisting of \( n \) blocks \( M_{1n}, M_{12}, ..., M_{1n} \), and a message authenticated code \( MAC_{new} \), to \( \mathcal{B} \). \( \mathcal{B} \) forwards the message blocks in the same manner as was done previously queried messages \( m_i \), and finally obtains the corresponding MAC \( MAC' \) on \( M \). If \( MAC_{new} \) equals \( MAC' \), then \( \mathcal{B} \) sends \( d = 1 \) to \( \mathcal{A} \) and the Challenger. Otherwise, it sends \( d = 0 \) to both of them. See figure 5.

\[
\text{Adv}^{\text{PRF}}_g(\mathcal{B}) = Pr(\text{Exp}^{\text{PRF}}_f(\mathcal{B}) = 1) - Pr(\text{Exp}^{\text{PRF}}_0(\mathcal{B}) = 1)
\]

\[
= \text{Adv}^{\text{CMA}}_{\text{CBC-MAC}}(\mathcal{A}) - \Delta
\]

The factor \( \Delta \) above will be determined as follows:

Proof. Adversary \( \mathcal{A} \) recorded \( q \) responses \( (\mu_1, \mu_2, ..., \mu_q) \), 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 \( \mu_i = \mu_j \) (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 \( m_{i,n} \oplus F(m_{i,n-1}) = \)
Figure 5: $F_k$-PRF $\Rightarrow$ 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 $\mu'_i$.

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 $\mu'_i$ 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 $\Delta \leq \frac{q(q-1)}{2^{2l}}$.

Completing the proof:

$$\text{Adv}^{\text{PRF}}_f(B) = Pr(\text{Exp}^{\text{PRF}-1}_f(B) = 1) - Pr(\text{Exp}^{\text{PRF}-0}_f(B))$$
$$\leq \text{Adv}^{\text{CMA}}_{\text{CBC-MAC}}(A) - \frac{q(q-1)}{2^{2l}}$$
$$\implies \text{Adv}^{\text{CMA}}_{\text{CBC-MAC}}(A) \leq \text{Adv}^{\text{PRF}}_f(B) + \frac{q(q-1)}{2^{2l}}$$

**Fact.** CBC-MAC can only work with fixed number of blocks. In other words CBC-MAC can not be used to authenticate arbitrarily long messages of variable lengths.

**Proof.** If the oracle accepted arbitrarily long messages, the adversary $A$ can create a forgery by performing the concatenation $(m_{11}, m_{12}, MAC_{12})$ as shown in the figure 6 (Extension Attack).

Solution to Fixed-Length Restriction on CBC MAC:

To prevent forgery for arbitrarily long messages, we will incorporate the number of message blocks (or the length of the message) into the block computation. The key used for PRF computation can be set to $F_k(l)$ instead of $K$, where $l$ is the number of message blocks. This variant remains CMA secure and it allows to authenticate variable length messages.

From the figure 7, we see that the new authenticator is $\mu = F_{F_k(l)}(m)$ where $l$ is the number of message blocks with equal size.

If the adversary attempts to create a forgery $(m_{11}, m_{12}, MAC_{12})$, the oracle will not accept because the MAC is now computed as $MAC_{12} = F_{F_k(l)}(F_{F_k(l)}(m_{11}) \oplus m_{12})$.  

8-6
Figure 6: Fixed-length restriction on CBC-MAC (Extension Attack)

Figure 7: Solution to fixed-length restriction on CBC-MAC