Cryptography 101: Message Authentication Codes

ComComX • 3 May 2026

Definition 1 (MAC). *A MAC scheme is a triple of algorithm* $(\mathsf{Gen}, \mathsf{MAC}, \mathsf{Verify})$ *that perform the following:*

- $\mathsf{Gen}(1^\lambda)$*: generates a key* k
- $\mathsf{MAC}(1^\lambda, k, m)$*: given* k *and a message* m*, generate a tag* t
- $\mathsf{Verify}(1^\lambda, k, m, t)$*: given* k, m, t*, decides to accept or reject.*

The idea of verifying message integrity is similar to the use of checksum. However, checksum only offers protection against random errors/modifications of message but not against an adversarial tempering.

Definition 2 (Correctness). *A MAC scheme is correct if, for any message* m*,*

$$\Pr_{k \leftarrow \mathsf{KeyGen}(1^\lambda), t \leftarrow \mathsf{MAC}(1^\lambda, k, m)}[\mathsf{Verify}(1^\lambda, k, m, t)] = 1.$$

There are three kinds of attacks, from strongest to weakest:

- **Total break**: adversary can reconstruct key k
- **Universal forgery**: adversary can construct a valid tag t for *every* message m
- **Existential forgery**: adversary can construct a valid tag t for *some* message m

Here we define a security notion that not only renders existential forgery impossible, but does so even the adversary can access to the MAC function to create valid pairs of message-tag (m, t), on the condition that (m, t) no longer counts as a successful existential forgery.

Let define a security game:

EUF-CMA(λ): (Existential unforgeability under chosen message attack)

1. Cha sample $k \leftarrow \mathsf{Gen}(1^\lambda)$
2. for some $i = 1, \ldots, \mathrm{poly}(\lambda)$:
   - Adv chooses m_i and sends to Cha
   - Cha computes $t_i \leftarrow \mathsf{MAC}(1^\lambda, k, m_i)$ and sends back to Adv
3. Adv outputs (m', t')
4. Adv wins if $\mathsf{Verify}(1^\lambda, k, m', t') = 1$ and $(m', t') \neq (m_i, t_i) \forall i$.

Definition 3 (EUF-CMA security)**.** *A MAC scheme is EUF-CMA secure if for any PPT adversary A,*

$$\Pr[A \text{ wins EUF-CMA}(\lambda)] = \mathrm{negl}(\lambda).$$

Note: there is no encryption here. MAC only protects integrity, not privacy.

Theorem 4. *Let $F_\lambda = \{f_k : \{0,1\}^\lambda \to \{0,1\}^{m(\lambda)}\}_{\lambda \in \mathbb{N}}$ be a PRF family. The following MAC scheme is correct and EUF-CMA-secure:*

$\mathsf{Gen}(1^\lambda)$*:*

- *Sample $f_k \leftarrow F_k$ uniformly at random*
- *Output k*

$\mathsf{MAC}(1^\lambda, k, m)$*:*

- *Output $f_k(m)$*

$\mathsf{Verify}(1^\lambda, k, m, t)$*:*

- *If $f_k(m) = 1$ outputs 1 (accept)*
- *Otherwise, outputs 0 (reject).*

Proof. The correctness is immediate. We show the security by a contradiction.

Assume that the scheme is not EUF-CMA-secure, meaning that there is a PPT adversary A that wins the game with noticeable probability. We construct an adversary B that uses A to break the security of F_λ. Specifically, B plays the game FN-IND defined on F_λ while simulating A as follows:

1. For $i = 1, \ldots, \mathrm{poly}(\lambda)$:
   - B receives m_i from A and sends to its Cha
   - B receives $f(m_i)$ from its Cha and forwards to A

2. B receives (m', t') from A
3. B sends m' to its Cha and gets back $t = f(m')$
4. If $t = t'$ then output 1 (f is a pseudorandom function)
5. Otherwise, output 0 (f is a truly random function).

Observe here that

- If f is a pseudorandom function then the game that A is playing is exactly the EUF-CMA game defined on the MAC scheme given in the theorem statement. This means that, by our assumption, A will win this game with noticeable probability.
- On the other hand, if f is a truly random function, A can not do noticeably better than random guess. Then in this case, the probability that B output 1 is exactly the probability that A guesses $f(m')$ correctly, which is $1/2^\lambda$ and is negligible.

It follows that

$$\begin{aligned}
\Pr[B \text{ wins FN-IND}(\lambda)] &= \frac{1}{2}\left(\Pr[B \text{ guesses } 1 | b = 1] + \Pr[B \text{ guesses } 0 | b = 0]\right) \\
&= \frac{1}{2}\left(\Pr[A \text{ guesses } 1 | b = 1] + 1 - \Pr[B \text{ guesses } 1 | b = 0]\right) \\
&\geq \frac{1}{2}\left(\frac{1}{p(\lambda)} + 1 - \text{negl}(\lambda)\right) \\
&= \frac{1}{2} + \frac{1}{q(\lambda)},
\end{aligned}$$

for some polynomial p and q. This contradicts the fact that F_k is a PRF family and concludes the proof. □