MAC

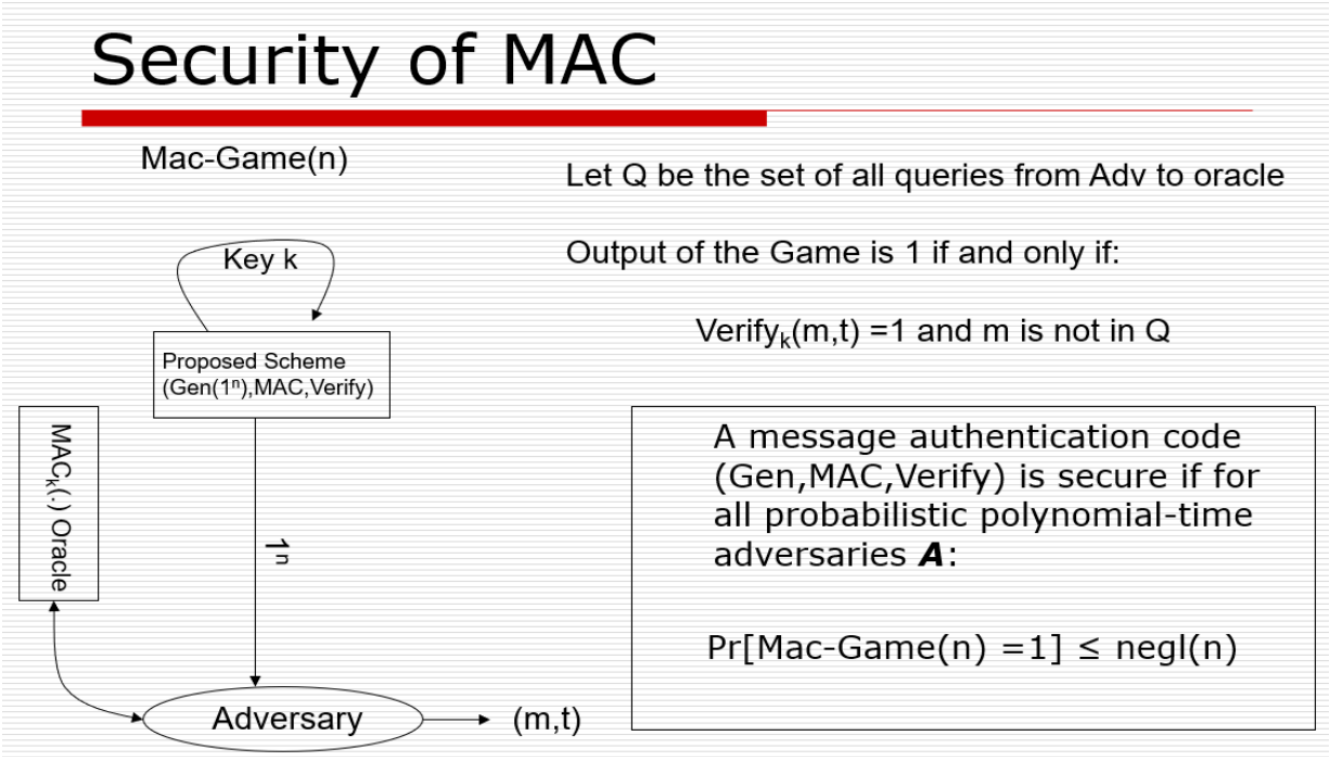
A message authentication code is an algorithm that is applied to a message. The output of the algorithm is a MAC tag (or just tag) that is sent along with the message. Security is formulated by requiring that no adversary can generate a valid MAC tag on any message that was not sent by the legitimate communicating parties.

DEFINITION 4.1 (message authentication code – syntax): *A* message authentication code *or* MAC *is a tuple of probabilistic polynomial-time algorithms* $(\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ *fulfilling the following:*

1. *Upon input* 1^n*, the algorithm* Gen *outputs a uniformly distributed key* k *of length* n*;* $k \leftarrow \mathsf{Gen}(1^n)$.
2. *The algorithm* Mac *receives for input some* $k \in \{0,1\}^n$ *and* $m \in \{0,1\}^*$*, and outputs some* $t \in \{0,1\}^*$*. The value* t *is called the* MAC tag.
3. *The algorithm* Vrfy *receives for input some* $k \in \{0,1\}^n$*,* $m \in \{0,1\}^*$ *and* $t \in \{0,1\}^*$*, and outputs a bit* $b \in \{0,1\}$.
4. *For every* n*, every* $k \in \{0,1\}^n$ *and every* $m \in \{0,1\}^*$ *it holds that* $\mathsf{Vrfy}_k(m, \mathsf{Mac}_k(m)) = 1$.

If there exists a function $\ell(\cdot)$ *such that* $\mathsf{Mac}_k(\cdot)$ *is defined only over messages of length* $\ell(n)$ *and* $\mathsf{Vrfy}_k(m,t)$ *outputs* 0 *for every* m *that is not of length* $\ell(n)$*, then we say that* $(\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ *is a* fixed length MAC *with length parameter* ℓ.

No polynomial-time adversary should be able to generate a valid MAC tag on any “new” message (i.e., a message not sent by the communicating parties).



Fixed length MACs

If there exists a function l(·) such that Mack(·) is defined only over messages of length l(n) and Vrfyk (m,t) outputs 0 for every m that is not of length l(n), then we say that (Gen, Mac, Vrfy) is a fixed length MAC with length parameter l.