Construction based on a Carter-Wegman MAC (built on a one-time MAC)

One-time MAC: analog of one-time pad for integrity
- Information-theoretic security against adversaries that only see one message-tag pair
- Does not need cryptography — can be much faster than cryptographic constructions

Basic construction: let \( p \) be a large prime (messages will be elements of \( \mathbb{Z}_p \) - integers modulo \( p \))

KeyGen: sample \( \alpha, \beta \in \mathbb{Z}_p \) (two random integers in \( \{0, \ldots, p-1\} \)). Key is \( k = (\alpha, \beta) \)

\[ \text{Sign}(k, m) : \text{output } t = \alpha m + \beta \pmod{p} \]

\[ \text{Verify}(k, m, t) : \text{accept if } t = \alpha m + \beta \pmod{p} \text{ and reject otherwise} \]

Security: given \( m, \tau = \alpha m + \beta \), adversary wins only if it outputs \( m' \neq m \) and \( \tau' = \alpha m' + \beta \)

Since \( \alpha, \beta \in \mathbb{Z}_p \), we can show that for any choice of \( m \neq m' \) and \( \tau, \tau' \in \mathbb{Z}_p \):

\[ \frac{\Pr_{\alpha, \beta \in \mathbb{Z}_p} [\alpha m + \beta = \tau'] | \alpha m + \beta = \tau]}{\Pr_{\alpha, \beta \in \mathbb{Z}_p} [\alpha m + \beta = \tau]} = \frac{1}{p} = \text{negl}(\lambda) \]

in particular, for all \( m \neq m' \) and \( \tau, \tau' \in \mathbb{Z}_p \):

\[ \frac{\Pr_{\alpha, \beta \in \mathbb{Z}_p} [\alpha m + \beta = \tau'] \land [\alpha m' + \beta = \tau]}{\Pr_{\alpha, \beta \in \mathbb{Z}_p} [\alpha m + \beta = \tau'] \land [\alpha m' + \beta = \tau]} = \frac{1}{p} = \text{negl}(\lambda) \]

regardless of adversary's running time.

For longer messages \( m = m_0 \cdots m_l \) where each \( m_i \in \mathbb{Z}_p \), define the MAC to be

\[ \tau = m_0 \alpha^l + m_1 \alpha^{l-1} + \cdots + m_l \alpha + \beta \pmod{p} \]

Very fast to evaluate: to process each message block: multiply by \( \alpha \) and add current block

- Still provides information-theoretic security:
  - for any \( m \neq m' \) of length up to \( l \) and \( \tau, \tau' \in \mathbb{Z}_p \):
  
  \[ \tau = \beta + \sum_{i \in [l]} m_i \alpha^{l-i+1} \]
  
  \[ \tau' = \beta + \sum_{i \in [l]} m_i' \alpha^{l-i+1} \]
  
  \[ \Rightarrow \sum_{i \in [l]} (m_i - m_i') \alpha^{l-i+1} = 0 \]

  polynomial of degree at most \( l \)

  \[ \Pr_{I_m \in \mathbb{Z}_p} [\alpha \text{ is a root of this poly}] = \frac{1}{p} \]

  the tag \( \tau \) adversary sees perfectly hides \( \alpha \) since \( \beta \neq \mathbb{Z}_p \), so \( m, \tau, \tau' \) is independent of \( \alpha \)

Carter-Wegman MAC ("encrypted MAC") : very lightweight, randomized MAC from the one-time MAC:
- Let (Sign, Verify) be a one-time MAC (or more generally, a universal hash function)
- Let \( F : \mathbb{Z}_p \times R \rightarrow \{0,1\}^* \) be a PRF

The Carter-Wegman MAC is defined as follows:

\[ \text{Sign}(k, m) : r \in R \]

\[ t = \text{Sign}(k, m) + F(k, r) \]

\[ \text{Verify}(k, m, t) : \text{output } 1 \text{ ifVerify}(k, m, F(k, r) \oplus t) \]

\[ \text{and } 0 \text{ otherwise} \]

\[ \text{output } (r, t) \]

very simple construction!

but tags are longer (need both a nonce and a PRF output)

Advantage: Use a fast one-time MAC (no cryptography!) on long message
Apply cryptographic operation to short output (slower)

Paradigm used in GCM mode of operation

PolyB05
GCM encryption: encrypt message with AES in counter mode compute Carter-Wegman MAC on resulting message using GHASH as the underlying hash function and the block cipher as underlying PRF

Typically, use AES-GCM for authenticated encryption

\[ GF(2^{128}) \text { is defined by the polynomial } g(x) = x^{128} + x^7 + x^2 + x + 1 \]

\[ \Rightarrow \text { elements are polynomials over } \mathbb{F}_2 \text { with degree less than } 128 \] (can be represented by 128-bit string: each bit is coefficient of polynomial)

\[ \Rightarrow \text { can add elements (xor) and multiply them (as polynomials) - implemented in hardware } \]

(also used for evaluating the AES round function)

\[ \Rightarrow \text { GHASH } (K, m) := m[0] K + m[1] K^{-1} + \ldots + m[l-1] K \]

\[ \text { values } m[0], \ldots, m[l-1] \text { give coefficients of polynomial, evaluate at point } K \]

\[ \text { GHASH } \text { operates on blocks of } 128-\text{bits } \]

\[ \text { operations can be expressed as operations over } GF(2^{128}) \]

\[ \text { GF(2^{128}) - Galois field with } 2^{128} \text { elements } \]

\[ \text { implemented in hardware - very fast! } \]

Oftentimes, only part of the payload needs to be hidden, but still needs to be authenticated.

\[ \Rightarrow \text { e.g., sending packets over a network: desire confidentiality for packet body, but only integrity for packet headers (otherwise, cannot route!) } \]

AEAD: authenticated encryption with associated data

\[ \Rightarrow \text { augment encryption scheme with additional plaintext input; resulting ciphertext ensures integrity for associated data, but not confidentiality } \]

\[ \text { (will not define formally here, but follows straightforwardly from AE definitions) } \]

\[ \Rightarrow \text { can construct directly via "encrypt-then-MAC": } \]

\[ \Rightarrow \text { can construct } \]

\[ \Rightarrow \text { encrypt payload and MAC the ciphertext + associated data } \]

\[ \Rightarrow \text { AES-GCM is an AEAD scheme } \]