Galois/Counter Mode (GCM)

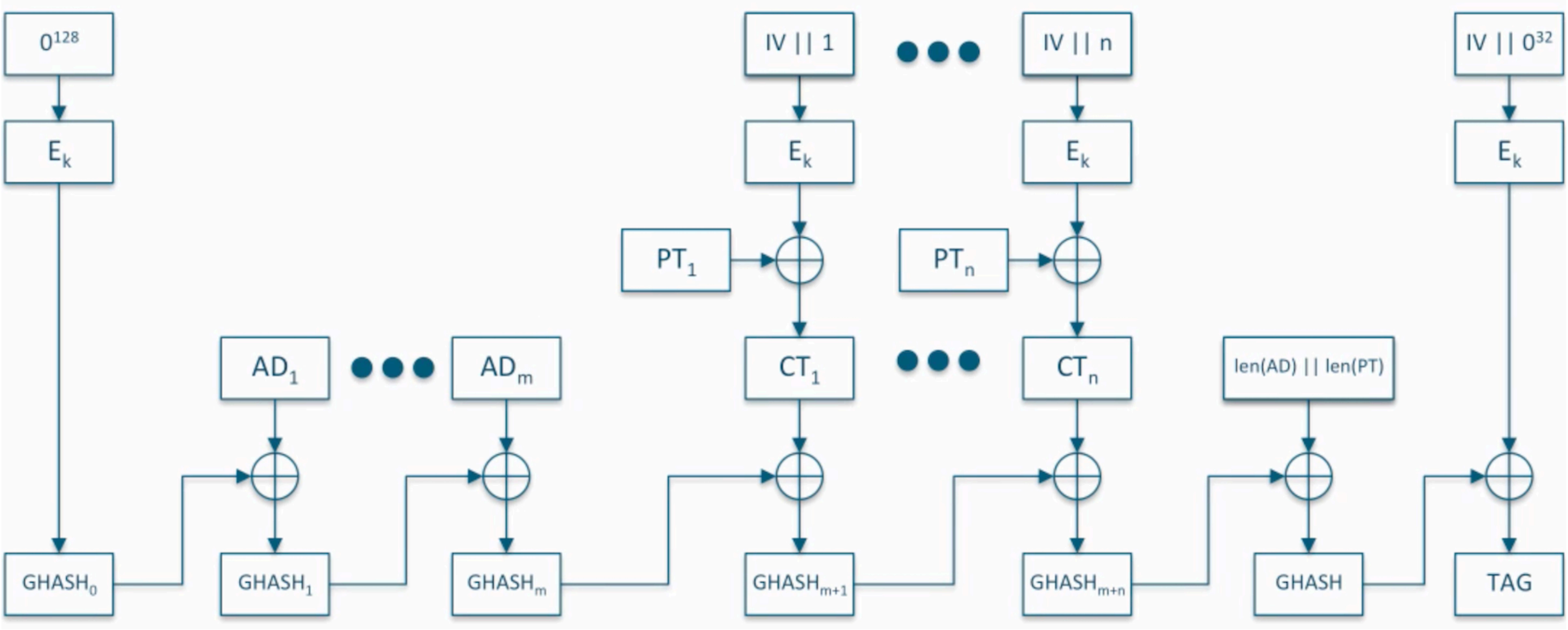
GCM Galois/Counter Mode

- Operating modes designed to provide both **data integrity** and **confidentiality**.
- Defined for block ciphers with a block size of 128 bits (e.g. AES).
- Provide Authenticated encryption with associated data (**AEAD**), for example network Packets.
- Accept Initialization Vector of arbitrary length (default: IV of 96 bits and counter of 32 bits).
- High performance due to **parallelization**.
- Return an **Authentication Tag**.

GMAC Galois message authentication code

- Authentication-only variant of the GCM which can be used as an incremental message authentication code.

Galois/Counter Mode (GCM)



The authenticated decryption operation is similar to the encryption, but with the order of the hash and encrypt step reversed. The tag that is computed by the decryption operation is compared to the tag associated with the ciphertext. If the two tags match (in both length and value), then the ciphertext is returned.

Galois/Counter Mode (GCM)

Galois Field

- Defined by the polynomial: **$x^{128} + x^7 + x^2 + x + 1$**
- GHASH function: **GHASH(H, A, C) = X_{m+n+1}**
- Single Message S_i :

$$S_i = \begin{cases} A_i & for\ i = 1, ..., m-1 \\ A^*{}_m \,||\, 0^{128-v} & for\ i = m \\ C_{i-m} & for\ i = m+1, ..., m+n-1 \\ C^*{}_n \,||\, 0^{128-u} & for\ i = m+n \\ len(A) \,||\, len(C) & for\ i = m+n+1 \end{cases}$$

- Then X_i is defined as:

$$X_i = \sum_{j=1}^{i} S_j \cdot H^{i-j+1} = \begin{cases} 0 & for\ i = 0 \\ (X_{i-1} \oplus S_i) \cdot H & for\ i = 1, ..., m+n+1 \end{cases}$$

- Iterative algorithm (each X_i depends on X_{i-1}). Only the final X_{m+n+1} is retained as output.

Galois/Counter Mode (GCM)

Parallelization

- The tag computation is essentially
  - Assemble A, C, len(A) || len(C), and Encrypt into a series of values $x_n, x_{n-1}, x_{n-2}, ..., x_0$
  - compute the polynomial $x_n h^n + x_{n-1} h^{n-1} + x_{n-2} hn - 2 + ... + x_0 h^0$
- Three-way parallelism, we could compute **j = h^{3}**

$$\begin{aligned} tag_2 &= j^0 x_2 + j^1 x_5 + j^2 x_8 + ... \\ tag_1 &= j^0 x_1 + j^1 x_4 + j^2 x_7 + ... \\ tag_0 &= j^0 x_0 + j^1 x_3 + j^2 x_6 + ... \end{aligned}$$

- Then combine them for the final result $tag = h^2 tag_2 + h^1 tag_1 + h^0 tag_0$

Galois/Counter Mode (GCM)

Security

- **Authentication Tag** and this is essential ensure the integrity of the data.
- **Changing a bit** in the ciphertext we will have a **fail** in the decryption, the tag obteined not correspond to the original one.
- The use of shorter authentication tags with GCM is **discouraged**.
- Adversary **likelihood of success** by choosing only the tags with n words (the total length of the ciphertext plus any additional authenticated data (AAD)) with probability measure 2^{-t} by a factor of n.
- System or protocol that implements GCM should **monitor** and, if necessary, **limit** the number of unsuccessful verification attempts for each key.