Applied Cryptography
CPEG 472/672
Lecture 8B

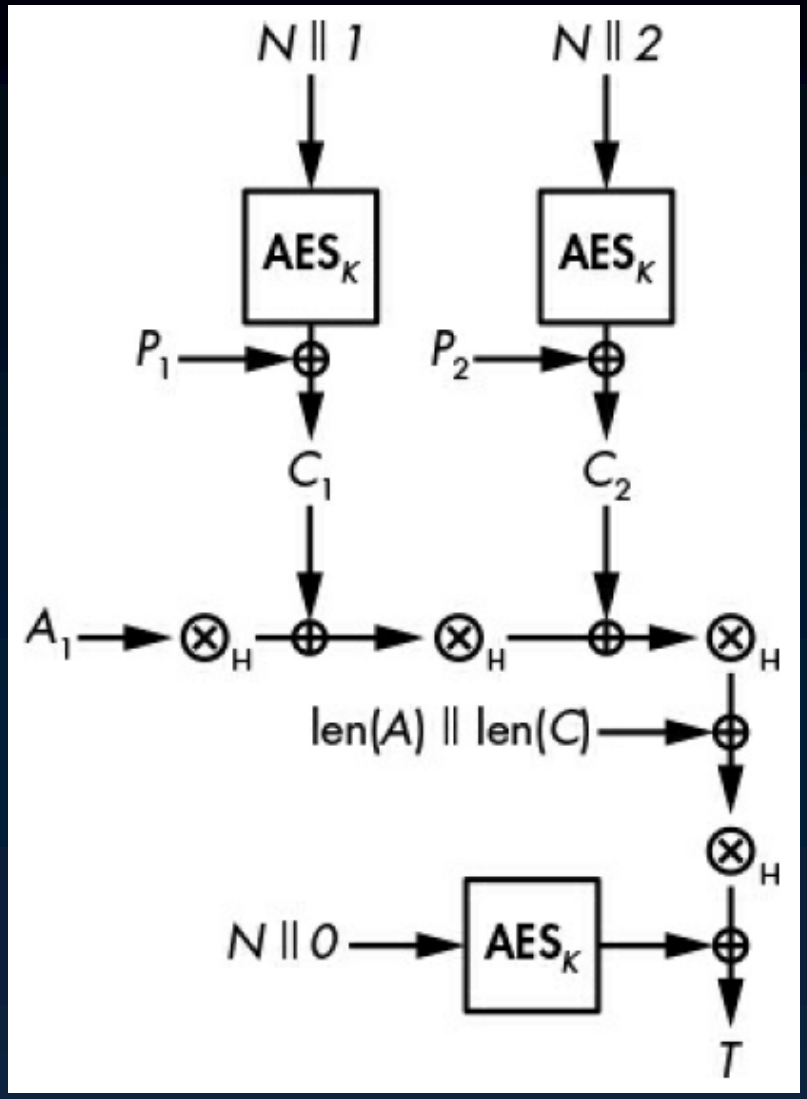
Instructor: Nektarios Tsoutsos

AES-GCM

NIST SP800-38D

- Most widely used authenticated cipher
  - AES CTR mode + C-W MAC (EtM)
  - Associated data
  - Secret key K (128 bits), nonce N (96 bits)
  - Encryption CTR starts at 1 (not 0)
- C-W MAC
  - Tag = GHASH xor PRF
  - The PRF is AES(K, N || 0x00)
  - GHASH: UH using GF(2) polymul and XORs
    - CLMUL instruction in x86

AES-GCM construction

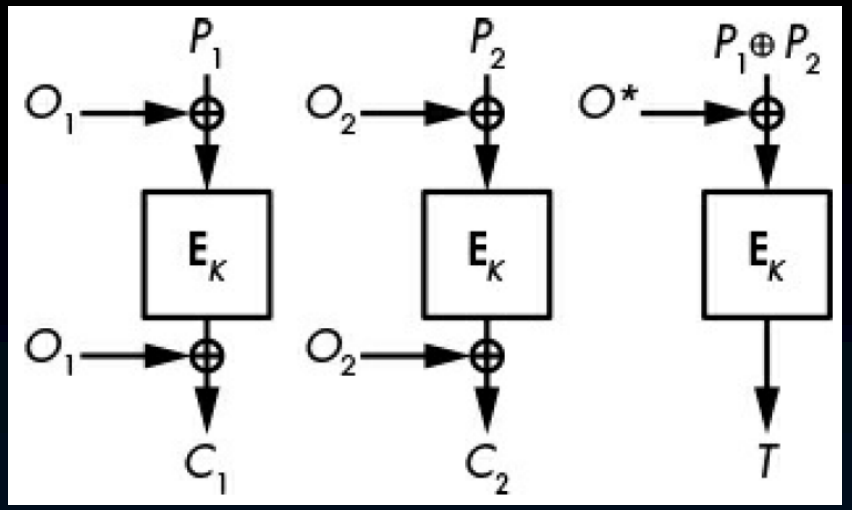


GCM security and efficiency

- Security
  - Fragile if nonce is reused
    - T=GH(AES(K,0), A, C) xor AES(K,N||0)
  - Can recover GH(A1,C1) xor GH(A2,C2)
    - Can leak GH key which is AES(K,0)
- Efficiency
  - Encryption & decryption parallelizable
  - MAC not parallelizable
    - Associated data processed first
  - Streamable (two layers)

OCB mode

Offset codebook (2001)



- Faster than GCM
  - Patented, free for non military use
- Blends encryption & auth in 1 layer
  - Only one secret key K
- C=E(K,P xor O) xor O
  - Offset O depends on key K and nonce N
- T= E(K, (xor of all P blks) xor O*)
  - Can auth associated data as well
    - T = T xor E(K,Ai xor Oi)

OCB security

- Less fragile to nonce reuse than GCM
  - Reusing nonce help identify if two ctxt blocks at the same index encrypt the same ptxt blk
  - Smaller impact vs GCM
- Reusing nonce breaks authentication
  - Combine blocks from another two msgs
  - Create fake message with same checksum
  - But: attacker can’t recover MAC key

OCB efficiency

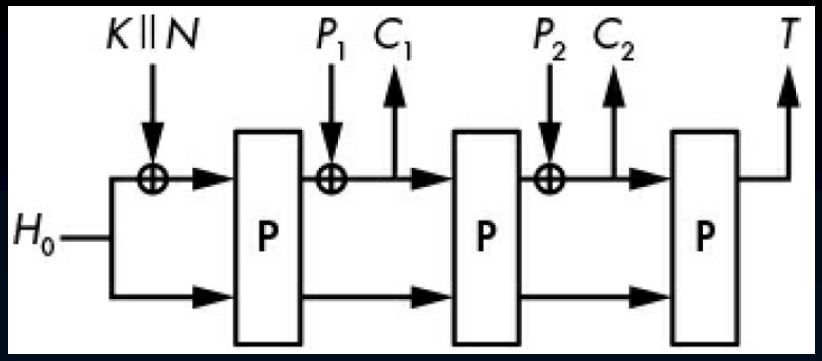
- Parallelizable
- Streamable
- 1 processing layer
- Essentially: Calls to cipher and XORs
  - Less expensive compared to GHASH
- OCB needs both encryption & decryption
  - GCM needs only encryption

SIV

Synthetic IV

- Authenticated cipher mode
  - Mostly used with AES, 2 keys, nonce for tag
  - More rebust to nonce reuse vs GCM, OCB
    - Attacker learns if same ptxt is encrypted twice
    - Can’t tell if n’th block is the same
- Combines cipher + PRF
  - Tag = PRF(K1, Nonce || ptxt)
  - Ctxt = E(K2, Tag, ptxt)
    - The nonce of E is the tag
- Not streamable

Permutation-based AEAD



- Uses a permutation P
  - E.g., AES with fixed key
- Initial state H0, K, N
  - P updates the internal state
- XOR ptx blk, get ctxt blk
  - Finally get state bits as tag T
  - Needs correct padding
- More nonce resistant than GCM and OCB
  - Security depends on number of non-XORed bits of the state
  - Reveals if ptxt prefix is the same
- Single layer, streamable, non-parallelizable

AES-GCM security

- GHASH internals
  - $X_i = (X_{i-1}$ xor $C_i)$ polymul H
  - H = AES(K,0x00)
  - X_0 = 0x00
  - $X_n = C_1$ xor H^n xor C_2 xor H^{n-1} xor .. xor C_n xor H^1
- Weak hash keys => forgery
  - H=0 => X_n=0
  - H=1 => tag is xor of ctxt blocks (can reorder)
  - H^e=H => short cycles (can swap blocks)
- Small auth tags in AES-GCM
  - n-bit tags, 2^m blks => Prob(forgery)=$2^{(m-n)}$

Hands-on exercises

- Polymul
- OCB mode
- SIV

Reading for next lecture

- Aumasson: Chapter 9 (until end of chapter)
  - We will have a short quiz on the material