GCM

유튜브 주소 : https://youtu.be/3owyCICtjE4

블록암호 운용모드

AEAD

GCM 모드

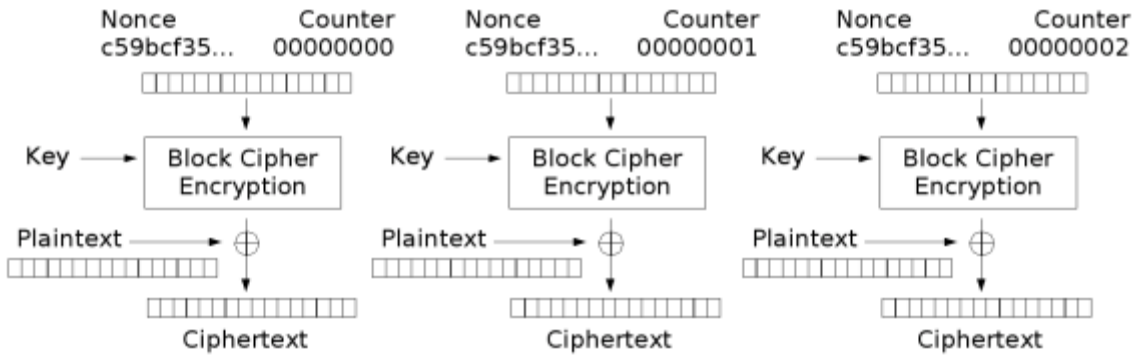
블록암호 운용모드

- 블록 암호를 블록 단위로 암,복호화되는 과정을 운용하는 절차
  - 평문의 암,복호화를 어떻게 반복하느냐에 따라 보안성이 달라짐
  - 암호화와 인증을 목적으로 정의
  - 공개키 암호에도 적용 가능하나 일반적이진 않음

- NIST에서는 5가지 운용 모드를 정의
  - ECB모드 - Electronic Code Blok mode (전자 부호표 모드)
  - CBC모드 - Cipher Block Chaining mode (암호 블록 연쇄 모드)
  - CFB모드 - Cipher-FeedBack mode (암호 피드백 모드)
  - OFB모드 - Output-FeedBack mode (출력 피드백 모드)
  - CTR모드 - Counter mode (카운터 모드)

블록암호 운용모드 - CTR 모드

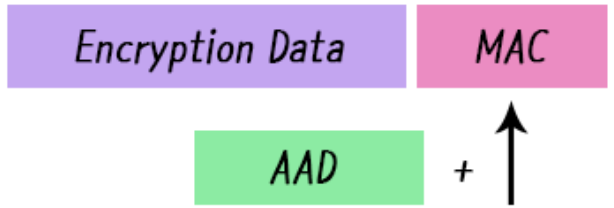
- 스트림 암호의 구조를 가짐
- 암호화 시 마다 Nonce를 구함
- 암호화 할 때 마다 1씩 증가하는 counter를 Nonce와 결합해 사용
- 이전 블록의 어떠한 값도 다음 블록에 영향을 주지 않음
  - 오류 전파가 없음
- 원하는 부분만 복호화 할 수 있음



CTR 모드 암호화

AEAD

- AEAD(Authenticated Encryption with Associated Data)
- 데이터의 기밀성과 무결성을 동시에 보호하는 암호화 방법
  - 즉, 데이터 암호화를 통한 기밀성과 MAC(Message Authentication Code) 계산을 통한 무결성 및 인증을 동시에 제공



AEAD 구조

- AE(Authenticated Encryption): 인증된 암호화 방식
- AD(Associated Data): 관련 데이터-> MAC 계산에 추가하여 인증 강화
  - AD: 일반적으로 AAD(Additional Associated Data)라고 부름
- TLS 1.3에서부터 Cipher suite로 AEAD Cipher가 추가되었음
- AEAD 알고리즘은 대표적으로 CCM, GCM이 존재

GCM 모드

- GCM mode: Galois/Counter Mode
  - CTR 기반 암호화 모드 중 하나
- CTR 모드에 메시지 인증 코드(MAC)를 결합한 구조를 지님
  - GCM의 메시지 인증 코드는 GMAC이라고 불리며, Galois Field 상에서 정의된 GHASH 함수를 이용하여 인증을 보장
- GHASH는 Galois Field 곱셈과 XOR 연산을 사용
- 기밀성: CTR 운용 모드를 통해 암호화되어 제공
- 무결성: 암호화된 데이터와 AAD 데이터를 활용한 GHASH 함수 연산을 통해서 제공

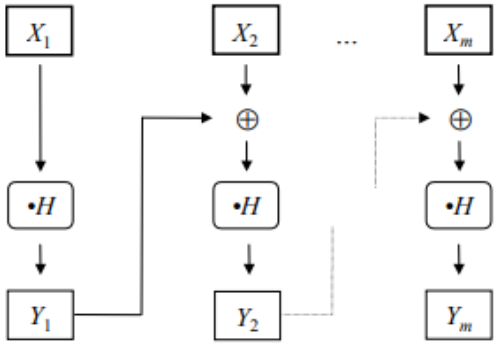


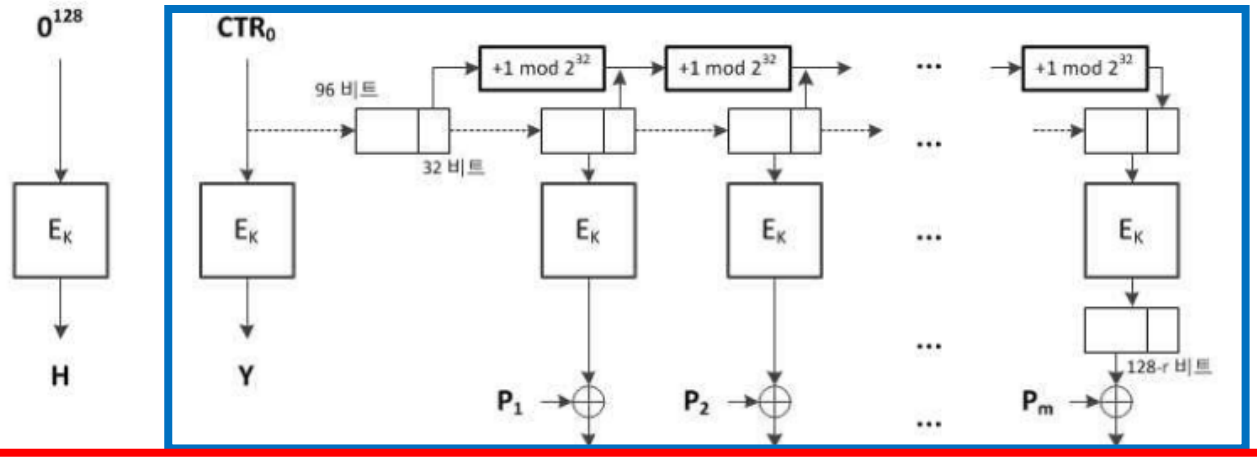
Figure 1: $\text{GHASH}_H(X_1 \| X_2 \| \ldots \| X_m) = Y_m$.

- GHASH 함수에서는 GF 곱셈 연산을 통해 인증 태그를 생성
  - GF 곱셈은 GF(2^{128}) 상에서 P(x) = $x^{128} + x^7 + x^2 + x + 1$의 기약 다항식을 사용하여 이루어짐

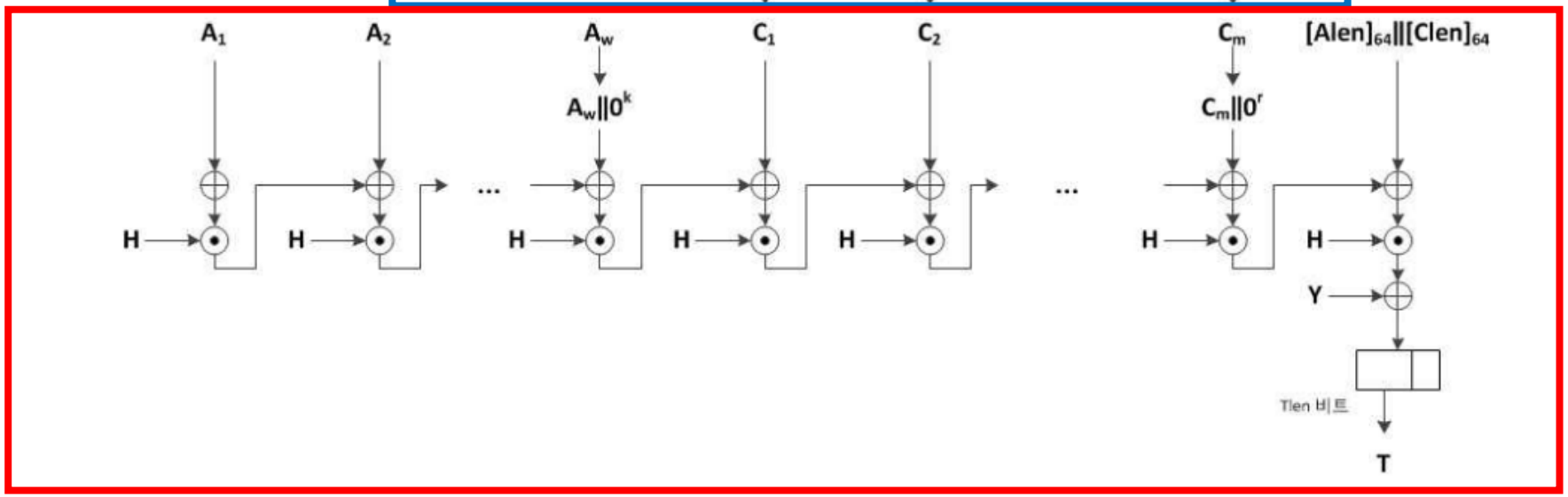
GCM 모드

- GCM 암호화
  - CTR0: 초기 카운터 블록
  - P: 평문
  - C: 암호문
  - A: AAD
  - H: 보조 비밀키
  - T: 인증값

CTR 모드 연산



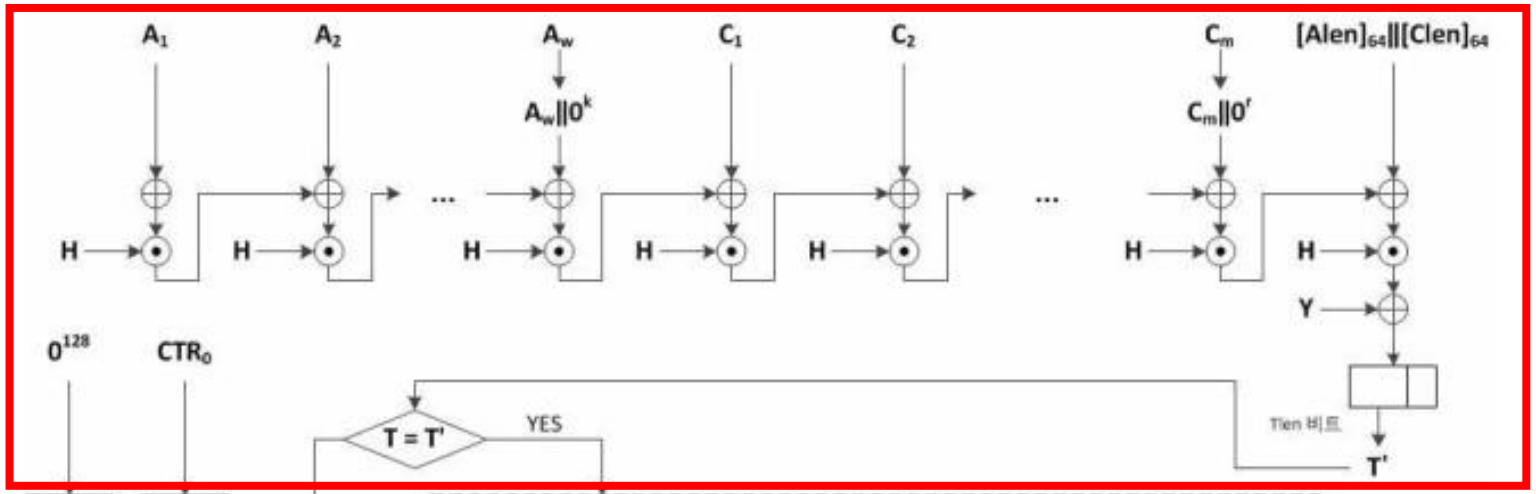
GMAC 연산



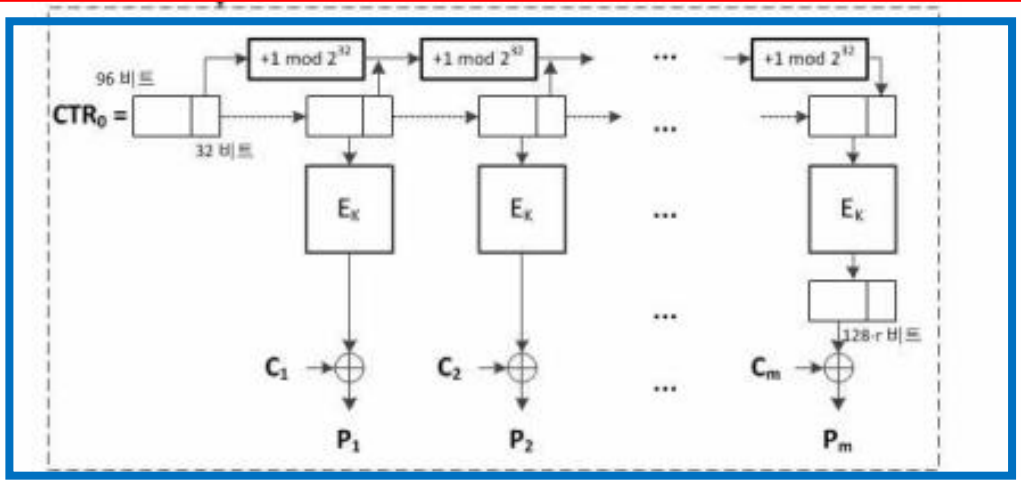
GCM 모드

- GCM 복호화
  - CTR0: 초기 카운터 블록
  - P: 평문
  - C: 암호문
  - A: AAD
  - H: 보조 비밀키
  - T: 인증값

GMAC 연산



CTR 모드 연산



Q & A