SGCM

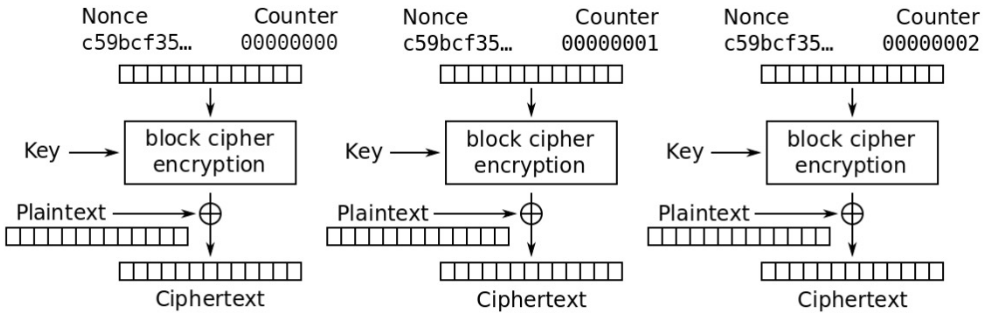
https://youtu.be/nZILgXpwRNA

SGCM

- Sophie Germain Counter Mode의 약자
- 수학자 Sophie Germain이 발견한 소수(Sophie Germain Prime) 활용하여 CTR 보안성 강화
  - Sophie Germain Prime
    - p 와 2p+1 모두 소수인 것
    - 2, 3, 5, 11, 29, 41, 53, 83 등

p	2	3	5	11	29	41	53	83	...
2p+1	5	7	11	23	59	83	107	167	....

- Counter(CTR) 운용
  - 입력 : 카운터 값 + 고정된 논스값
  - 출력 : 출력된 키 스트림
  - 암호문 : 출력 값 ⊕ 평문
  - 이전 블록과 직접적인 상관관계가 없기 때문에 병렬화 가능
  - CTR 모드에서 카운터 값을 무작위로 생성하는데 이 값은 예측되거나 중복되면 보안 위협



Counter (CTR) mode encryption

https://eprint.iacr.org/2011/326.pdf

GCM 운용모드

- 갈루아/카운터모드(Galois/Counter Mode)
- 블록 암호와 해시 함수를 조합하여 암호화와 인증을 동시 제공
  - CTR 모드를 통해 암호화 제공
  - 암호화된 데이터 + AAD 데이터 활용하여 GHASH 연산
  - AAD(Additional Authentication Data)?
    - 메시지 데이터와 함께 인증되었지만, 암호화되지 않는 추가 데이터
    - 알려져도 상관없는 메시지 헤더 등의 메타 데이터를 인증할 때 사용
    - AAD 몰라도 인증이 가능한 메시지 데이터에 대한 인증 보안 제공할 때 사용

$$\boxed{H = E(K, 0^{128})}$$

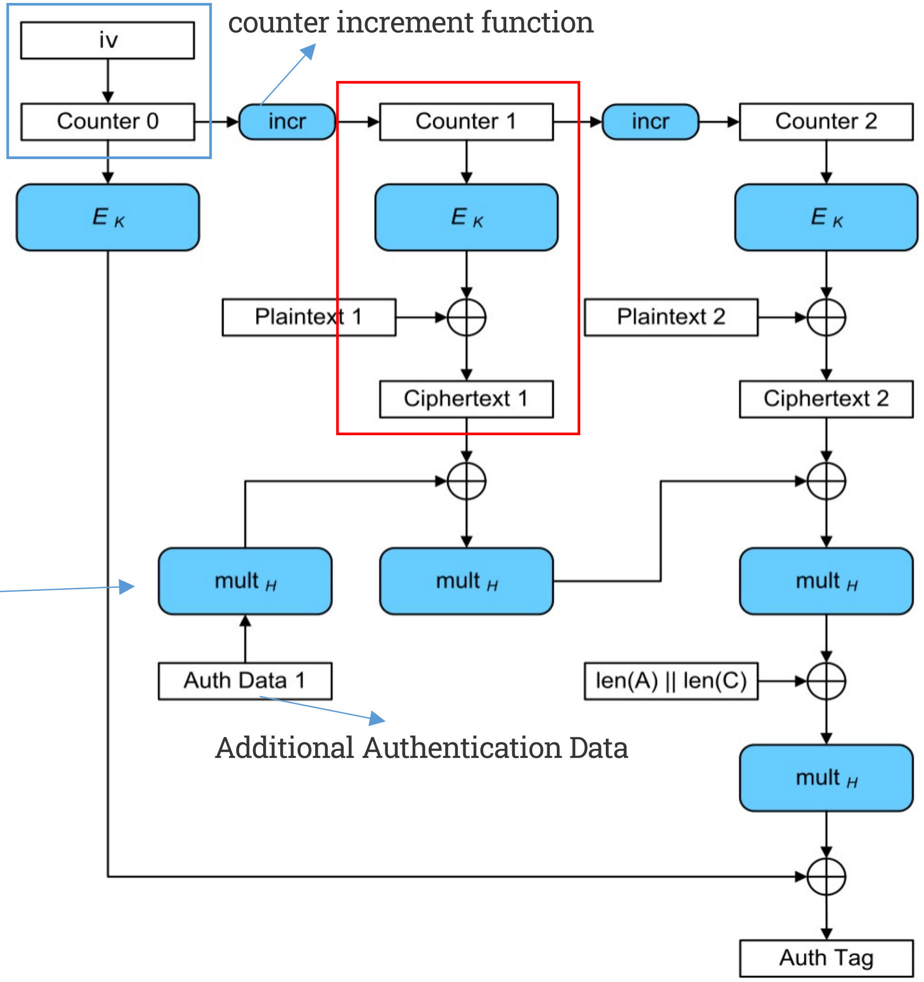
$$Y_0 = \begin{cases} IV \| 0^{31}1 & \text{if } \mathrm{len}(IV) = 96 \\ \mathrm{GHASH}(H, \{\}, IV) & \text{otherwise.} \end{cases}$$

$$Y_i = \mathrm{incr}(Y_{i-1}) \text{ for } i = 1, \ldots, n$$

$$C_i = P_i \oplus E(K, Y_i) \text{ for } i = 1, \ldots, n-1$$

$$C_n^* = P_n^* \oplus \mathrm{MSB}_u(E(K, Y_n))$$

$$T = \mathrm{MSB}_t(\mathrm{GHASH}(H, A, C) \oplus E(K, Y_0))$$



GCM 운용모드

- GHASH
  - Galois Field($GF(2^{128})$)상에서 다항식 연산을 통해 해시 값 계산
  - 입력 : 128-bit 메시지, 128-bit 인증 키 H
  - 출력 : 128-bit 인증 태그
  - 메시지 M을 128-bit 블록으로 나눠 다항식 연산 수행
- **Cycle Swapping Attack**에 취약
  - 다항식의 주기성 + 동일한 라운드 함수 반복

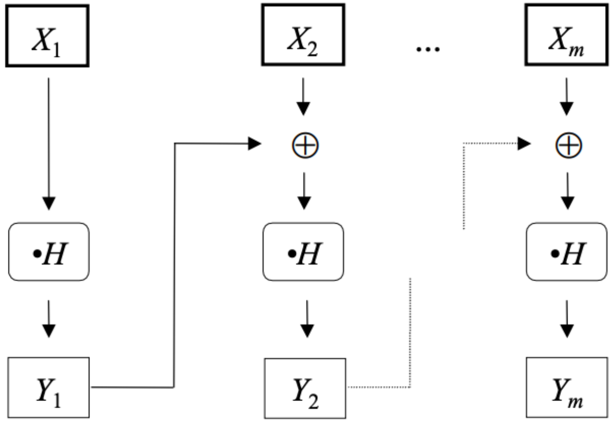


Figure 1: $\text{GHASH}_H(X_1 \| X_2 \| \ldots \| X_m) = Y_m$.

The attack described in [12] is based on the observation that powers of H sometimes repeat in a short cycle when the the arithmetic of Equation 2 is performed in $GF(2^{128})$. If we know that $H^{m-i+1} = H^{m-j+1}$ with $i \neq j$, we may simply swap X_i and X_j and the resulting authentication tag stays the same. The powers of H repeat in cycles which are determined by $n = \text{ord}(H)$, the multiplicative order of H. We may therefore produce collisions by swapping any two ciphertext blocks X_i and X_j if $i \equiv j \mod n$. Note that this swapping attack can be also applied to any number of individual pairs of bits in corresponding positions of blocks separated by n positions or its multiple.

$$Y_m = \sum_{i=1}^{m} X_i \times H^{m-i+1}. \qquad (2)$$

SGCM

- 곱셈 연산과 GHASH 함수를 제외하고 GCM과 동일
  - Sophie Germain 소수 기반으로 하는 **기약 다항식 p** 사용

3 The Sophie Germain Counter Mode SGCM

Mathematically SGCM differs from GCM inly in the underlying field where GHASH's arithmetic operations are performed. While GCM uses the binary field $GF(2^{128})$, SGCM uses traditional modular arithmetic in $GF(p)$, where

$$p = 2^{128} + 12451 = 340282366920938463463374607431768223907. \quad (3)$$

Here $\frac{p-1}{2}$ is also a prime, a Sophie Germain prime. [1]

https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-38d.pdf

SGCM

- 곱셈 연산과 GHASH 함수를 제외하고 GCM과 동일
  - $H = E(K, 0^{128}) + 2$
  - GCM과 다른 다항식 사용

Let X be a concatenation of unencrypted authenticated data, CTR-encrypted ciphertext, and padding. This data is split into 128-bit blocks X_i:

$$X = X_1 \mid\mid X_2 \mid\mid \cdots \mid\mid X_n. \tag{1}$$

A 128-bit block cipher such as AES is used to derive the hash subkey $H = \boxed{E_K(0)}$. The same AES key K is also used as the data encryption key. GHASH is based on arithmetic operations in a finite field. Horner's rule is used to evaluate the polynomial Y, given m 128-bit message blocks X_i with padding.

$$Y_m = \sum_{i=1}^{m} X_i \times H^{m-i+1}. \tag{2}$$

The authentication tag is $T = Y_m + E_K(IV \mid\mid 0^{31} \mid\mid 1)$, assuming that a 96-bit Initialization Vector (IV) is used. Other options exist.

Now let X_i denote the sequence of blocks as defined in Equation 1 and let $\boxed{H = E_K(0) + 2}$ be the hash subkey. We start with $Y_0 = 0$ and iterate for $i = 1, \ldots, n$ the following:

$$\boxed{Y_i = (Y_{i-1} + X_i)\ H \mod p. \qquad (4)}$$

The final iteration satisfies $Y_n = SGHASH_H(X)$. Should the value be equal to 2^{128} or larger and hence require more than 16 bytes of storage, the result should be truncated mod 2^{128}. This special case is exceedingly rare ($P \approx 2^{-114.396}$). This value is then used in equal fashion as $GHASH_H(X)$ is used in the GCM specification.

https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-38d.pdf

SGCM

- AES 와 GHASH 사용하여 암호화와 인증 수행
- 입력도 GCM 운용모드와 동일
  - IV(초기벡터)+ 카운터 값
- 내부 알고리즘 GCM과 유사
- GCM의 GHASH 함수의 취약점을 Sophie Germain Prime Cycle을 사용하여 GHASH 다항식의 보안성 강화

Q & A