SM4-GCM工作模式说明

1. GCM概述

GCM（Galois/Counter Mode）是一种认证加密模式，它结合了CTR（Counter）模式的加密和GMAC（Galois Message Authentication Code）的认证功能，能够同时提供数据的机密性和完整性。

SM4-GCM是将SM4分组密码算法与GCM工作模式结合的一种加密方案。

2. GCM的组成

GCM由两部分组成：

1. CTR模式：用于提供机密性
2. GHASH函数：用于提供完整性和认证

3. 数学描述

3.1 加密过程

给定：

- 密钥K（128位）
- 明文P（任意长度）
- 初始向量IV（推荐12字节）
- 附加认证数据A（任意长度）

加密过程：

1. 生成哈希密钥$H = SM4(K, 0^{128})$
2. 生成初始计数器Y_0：
   - 若$len(IV) = 96$，则$Y_0 = IV \| 0^{31}1$
   - 否则，$Y_0 = GHASH_H(IV \| 0^{s+64} \| len(IV)_64)$，其中$s = (128 - (len(IV) \times 8 \mod 128)) \mod 128$
3. 生成计数器序列$Y_i = Y_0 + i \mod 2^{128}$
4. 生成密钥流$S_i = SM4(K, Y_i)$
5. 计算密文$C = P \oplus S_1 \| S_2 \| ...$
6. 计算认证标签$T = GHASH_H(A \| C \| len(A)_64 \| len(C)_64) \oplus S_0$

最终输出为(C, T)

3.2 解密过程

给定：

- 密钥K（128位）

- 密文C（任意长度）
- 初始向量IV（与加密时相同）
- 附加认证数据A（与加密时相同）
- 认证标签T

解密过程：

1. 生成哈希密钥$H = SM4(K, 0^{128})$
2. 生成初始计数器Y_0（与加密时相同）
3. 生成计数器序列$Y_i = Y_0 + i \mod 2^{128}$
4. 生成密钥流$S_i = SM4(K, Y_i)$
5. 计算明文$P = C \oplus S_1 \| S_2 \| ...$
6. 计算验证标签$T' = GHASH_H(A \| C \| len(A)_64 \| len(C)_64) \oplus S_0$
7. 验证$T = T'$，若不相等则解密失败

4. GHASH函数

GHASH是GCM模式中用于计算认证标签的核心函数，定义如下：

给定哈希密钥H和数据块序列$X_1, X_2, ..., X_m$，则：

$$GHASH_H(X_1, X_2, ..., X_m) = ((((X_1 \oplus Y_0) \cdot H) \oplus X_2) \cdot H) \oplus ... \oplus X_m) \cdot H$$

其中$Y_0 = 0^{128}$，$\cdot$表示在伽罗瓦域$GF(2^{128})$上的乘法。

伽罗瓦域$GF(2^{128})$上的乘法定义为：

对于两个128位元素a和b，它们的乘积$c = a \cdot b$满足：

$$c(x) = (a(x) \cdot b(x)) \mod p(x)$$

其中$p(x) = x^{128} + x^7 + x^2 + x + 1$是不可约多项式。

5. 安全性考虑

- 初始向量IV不应重复使用，对于相同的密钥，每次加密应使用不同的IV
- 推荐IV长度为96位（12字节），这是最有效的长度
- 认证标签T的长度推荐为128位（16字节），提供足够的安全性
- GCM模式对密文和附加认证数据的任何篡改都能检测到