**1. 简介**

* **SM4** 是中国国家标准分组对称密码算法，分组长度 128 位，密钥长度 128 位，采用 32 轮迭代结构。
* **GCM (Galois/Counter Mode)** 是一种认证加密模式，结合计数器模式 (CTR) 加密与 GHASH 认证，保证数据的机密性与完整性。

SM4-GCM 即是将 SM4 算法与 GCM 模式结合，实现同时加密和认证。

**2. 算法过程**

**2.1 计数器模式 (CTR) 加密**

给定：

* 明文分组：PiP\_iPi​
* 计数器块：JiJ\_iJi​
* SM4 密钥：KKK

密文：

图片包含 徽标

AI 生成的内容可能不正确。

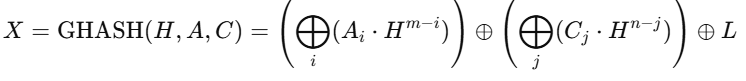
其中，EKE\_KEK​ 表示使用 SM4 密钥 KKK 的块加密。

计数器初值 J0J\_0J0​ 通常由 IV 和常量构成，之后递增。

**2.2 GHASH 认证**

GHASH 用于认证消息，定义如下：

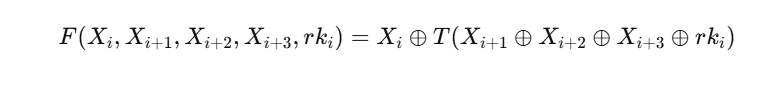
* 输入为认证数据 AAA 和密文 CCC
* 认证子密钥计算：
* 计算：



* 其中 L是附加的长度信息，乘法和加法均在 GF(2^{128}) 域进行。
* 最终认证标签：



**3. 数学推导**

* SM4 的核心是一个基于 S 盒和线性变换 LLL 的迭代轮函数：
* 其中
* GCM 中的 GHASH 操作是域上的多项式计算，保证认证强度。

**4. 优化思路**。

**GCM 优化**

* **GHASH 加速**：使用 Karatsuba 算法和向量化实现多项式乘法。
* **计数器块生成向量化**：批量生成计数器块加速 CTR。
* **内存布局优化**：保证数据对齐，减少缓存未命中。
* **多线程并行处理**：对大数据分段处理加速。

**GHASH 加速的数学推导**

**1. GHASH 定义**

GHASH 是 GCM 模式中的消息认证码（MAC）函数，定义在有限域 GF(2^{128})上。

给定：

* 认证密钥 H∈GF(2^{128})，由加密密钥加密全 0 得到，即 H=E\_K(0^{128})
* 认证数据块 X1,X2,...,Xm∈GF(2^{128})
* GHASH 输出为：

简化写为递推：



**2. 乘法在 GF(21282^{128}2128) 的定义**

* 这里的乘法是有限域 GF(2128)GF(2^{128})GF(2128) 上的乘法，基于不可约多项式：
* 黑色的钟表

  AI 生成的内容可能不正确。
* 运算等价于对二进制多项式模 p(x) 的乘法。

**3. 计算复杂度与优化难点**

* 传统乘法需要 128 次移位和条件异或，性能瓶颈明显。
* GHASH 在实际加密中对性能影响大，尤其在大数据量时。

**4. Karatsuba 乘法加速**

Karatsuba 算法是减少大整数（多项式）乘法复杂度的经典方法。

设



乘积：



其中：

文本, 信件

AI 生成的内容可能不正确。

**优点**：只用 3 次 64 位乘法代替了 4 次，提高效率。

**5. 向量化实现**

* 利用 SIMD 指令（如 AVX2、AVX512）实现并行 Karatsuba 乘法。
* 一次处理多组 X,YX, YX,Y，充分利用 CPU 向量寄存器宽度。
* 通过位操作和条件异或，完成模多项式的归约。