SM4 与 SM4-GCM 算法数学推导与优化表示

1 SM4 分组密码数学表示

SM4 是一种分组长度为 128 位、密钥长度为 128 位的分组密码算法，总共进行 32 轮迭代加密。设明文输入为：

$$(X_0, X_1, X_2, X_3)$$

其中 X_i 为 32 位无符号整数。

1.1 轮函数定义

第 i 轮 $(i = 0, 1, \ldots, 31)$ 中，状态更新公式为：

$$X_{i+4} = X_i \oplus F(X_{i+1}, X_{i+2}, X_{i+3}, rk_i) \tag{1}$$

其中：

$$F(X_1, X_2, X_3, rk) = T(X_1 \oplus X_2 \oplus X_3 \oplus rk) \tag{2}$$

1.2 非线性与线性变换

T 函数由非线性变换 τ 和线性变换 L 组成：

$$T(B) = L(\tau(B)) \tag{3}$$

非线性变换 τ：

$$\tau(B) = (S(b_0), S(b_1), S(b_2), S(b_3))$$

其中 $B = (b_0, b_1, b_2, b_3)$ 为 4 字节表示，$S(\cdot)$ 为 S-Box 查表。

线性变换 L：

$$L(B) = B \oplus (B \lll 2) \oplus (B \lll 10) \oplus (B \lll 18) \oplus (B \lll 24)$$

其中 $\lll$ 表示循环左移。

1.3 T-table 优化表示

预计算：

$$T_{\text{table}}[b] = L(S(b))$$

轮函数可改写为：

$$X_{i+4} = X_i \oplus T_{\text{table}}[b_0] \oplus (T_{\text{table}}[b_1] \lll 8) \oplus (T_{\text{table}}[b_2] \lll 16) \oplus (T_{\text{table}}[b_3] \lll 24)$$

1.4 密钥扩展

原始密钥：

$$(MK_0, MK_1, MK_2, MK_3)$$

经过固定参数 FK 处理：

$$K_i = MK_i \oplus FK_i, \quad i = 0, 1, 2, 3$$

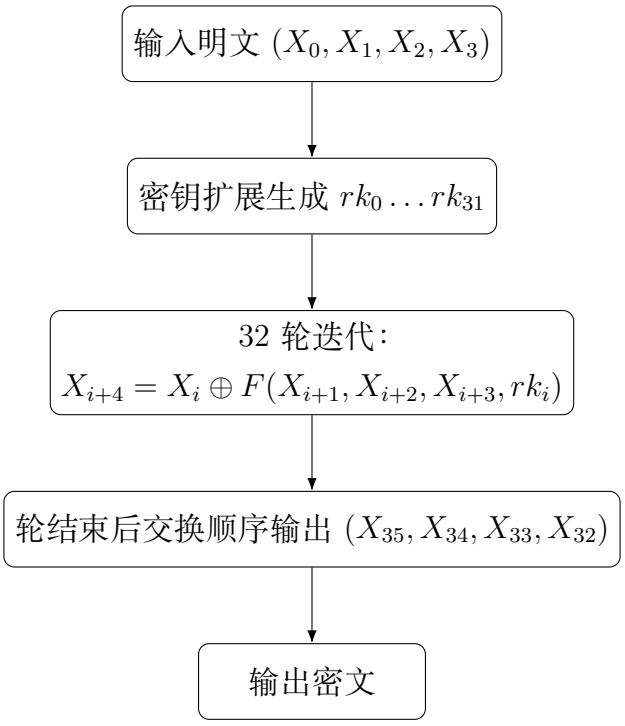
轮密钥生成：

$$K_{i+4} = K_i \oplus T'(K_{i+1} \oplus K_{i+2} \oplus K_{i+3} \oplus CK_i)$$

其中 $L'(B) = B \oplus (B \lll 13) \oplus (B \lll 23)$，最终：

$$rk_i = K_{i+4}, \quad i = 0, 1, \ldots, 31$$

1.5 SM4 加密流程图



2 SM4-GCM 模式数学表示

GCM 结合了 CTR 加密与基于 $GF(2^{128})$ 的 GHASH 认证。

2.1 初始化

若 $|IV| = 96$ 位：

$$J_0 = IV \parallel 0^{31} \parallel 1$$

否则：

$$J_0 = \mathrm{GHASH}_H(\mathrm{pad}(IV) \parallel \mathrm{len}(IV))$$

其中 $H = E_K(0^{128})$。

2.2 CTR 加密

每个分组：

$$\mathrm{CTR}_i = \mathrm{Inc}(J_0, i)$$

$$C_i = P_i \oplus E_K(\mathrm{CTR}_i)$$

2.3 GHASH 计算

$$Y_0 = 0^{128}, \quad Y_i = (Y_{i-1} \oplus X_i) \cdot H$$

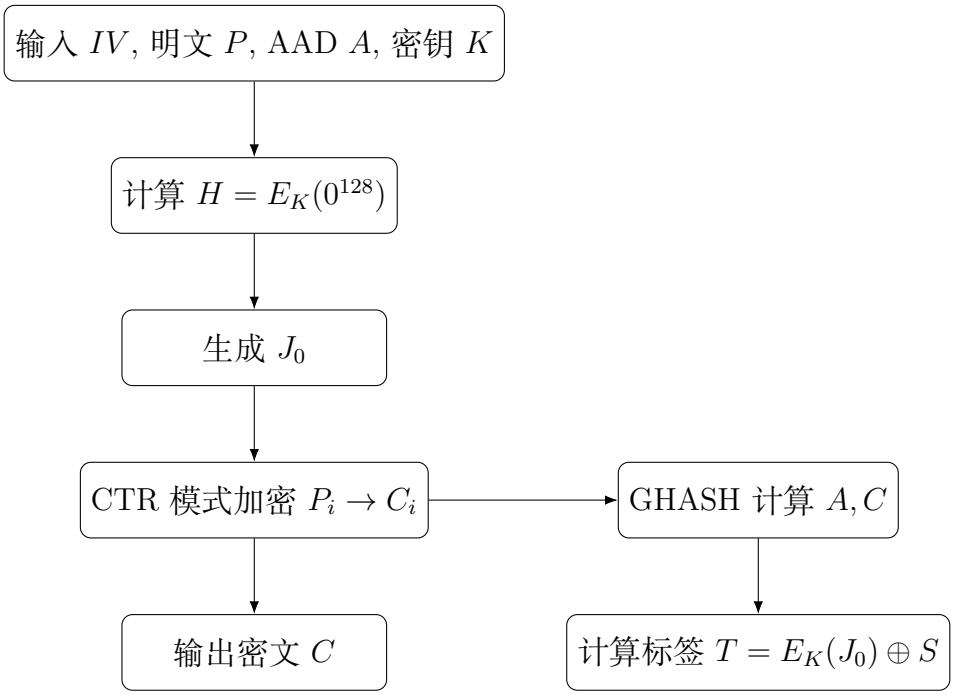
最终：

$$S = Y_n$$

2.4 认证标签

$$T = E_K(J_0) \oplus S$$

2.5 SM4-GCM 加密流程图



3 GCM 总公式

$$
\boxed{
\begin{aligned}
&H = E_K(0^{128}) \\
&C_i = P_i \oplus E_K(\mathrm{Inc}(J_0, i)) \\
&S = \mathrm{GHASH}_H(A \parallel C) \\
&T = E_K(J_0) \oplus S
\end{aligned}
}
$$