**一、SM4 算法简介**

SM4 是中国国家密码管理局发布的分组对称加密算法，广泛用于国家商用密码领域。其核心特性如下：

* **分组长度**：128 位
* **密钥长度**：128 位
* **轮数**：32 轮
* **结构类型**：类似 Feistel 网络的迭代结构

每轮运算主要包含：密钥加、非线性变换（S盒）、线性变换（轮函数 L）

**二、加密过程数学推导**

文本, 信件

AI 生成的内容可能不正确。其中：

1. **轮函数 F 的定义**：
2. 文本

   AI 生成的内容可能不正确。**T 是复合变换（SubBytes + L）**：
   * SubBytes：对 32 比特字逐字节替换 SBox(x\_i)
   * L(x) = x \oplus (x <<< 2) \oplus (x <<< 10) \oplus (x <<< 18) \oplus (x <<< 24)

**三、SM4 优化实现目标**

目标是将上述过程在软件中执行尽可能高效。

**1. T-table 优化**

将 SubBytes 与线性变换 L 合并查表：

* 用预生成的表 T0~T3 替代逐字节查 SBox + 多次轮转
* 节省指令周期，减少 cache miss

**2. 使用 SIMD 向量指令**

* **SSE/AVX**：并行处理多个 block，例如一次处理 4 个 block（AVX2）或 8 个（AVX512）
* **VPROLD**：替代普通逻辑左旋，例如 \_mm\_rol\_epi32 等
* **GFNI（Galois Field New Instructions）**：在 AVX512+GFNI 支持下，用于仿射变换（SBox 硬件加速）

**3. AES-NI 加速借鉴**

虽然 SM4 不同于 AES，但可以复用如下技术：

* **Intel AES-NI 指令集**理念：表查替代字节操作、流水线优化、轮密钥 cache
* **密钥扩展预处理**，避免每轮重复运算

**四、优化路径总结**

| **优化策略** | **技术方案** | **加速效果** |
| --- | --- | --- |
| 表查加速 | T-table | 约 2-3x |
| SIMD 并行 | AVX2/AVX512 | 提升 4-8 倍 |
| SBox 加速 | GFNI 指令 | 提升 1.5-2x |
| 位移加速 | VPROLD 替代 <<< | 提升部分轮次 |
| 内存访问优化 | Cache alignment, prefetching | 降低 cache miss |
| 多线程并行 | OpenMP 或线程池 | 线性扩展 |