**任务1**

**1. SM4算法基础**

分组结构：128位分组，32轮Feistel网络

核心操作有：

非线性变换τ：4个并行的8位S盒替换

线性变换L：L(B) = B ⊕ (B<<2) ⊕ (B<<10) ⊕ (B<<18) ⊕ (B<<24)

轮函数F：F(X, rk) = L(τ(X⊕rk))

**2. 基础优化实现**

循环展开：32轮展开为8组×4轮

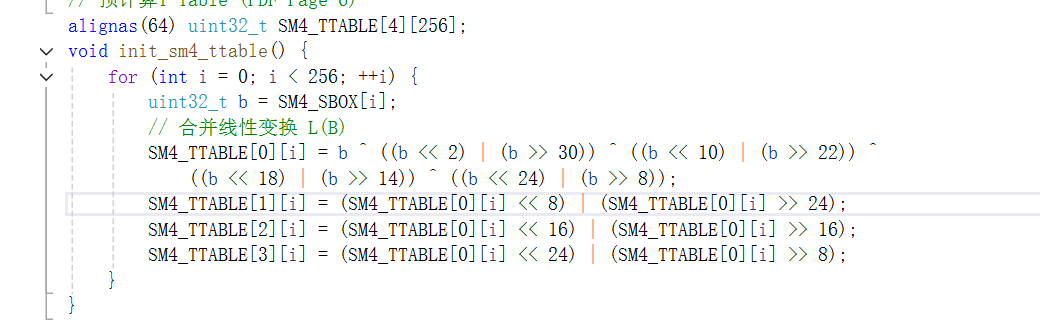
寄存器优化代码如下图所示：

图形用户界面, 文本, 应用程序

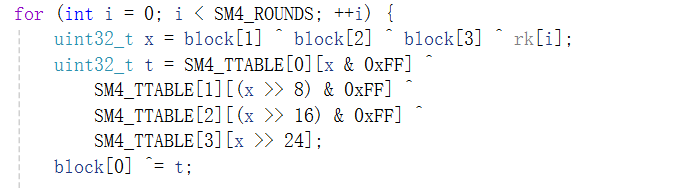
AI 生成的内容可能不正确。

**3. 进行T-Table优化（4KB查表）**

用于合并S盒和线性变换预计算表的具体内容如下图所示：



用于加密加速的具体代码如下：



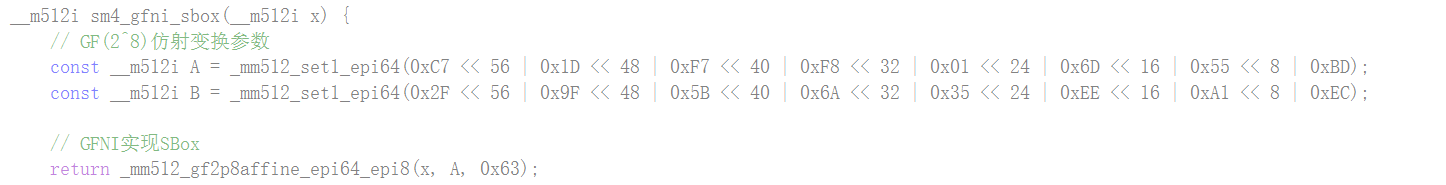
**4. 进行AES-NI指令加速**

首先要通过映射矩阵转换到AES域，具体的代码内容如下所示：

图形用户界面, 文本, 应用程序

AI 生成的内容可能不正确。

然后进行AVX512+GFNI加速，我们要并行处理，同时加密八个分组，先用GFNI加速S盒：



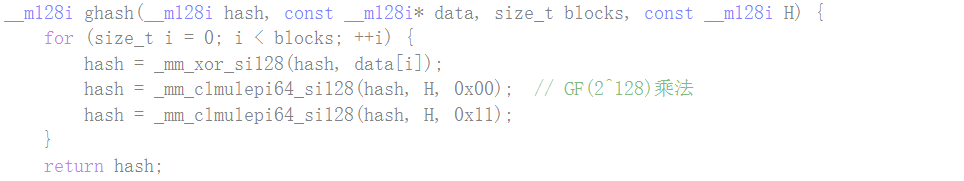
最后进行AVX512线性变换：

图形用户界面

AI 生成的内容可能不正确。

**5.进行SM4-GCM优化**

使用PCLMULQDQ指令实现它，具体内容如下图所示：



然后进行计数器模式加密：

