一种组合式大分组分组密码算法的软件实现及应用

为了提高国密分组密码算法的安全强度，抵御量子计算攻击，设计一种基于国密算法 SM4 和 SM3 的组合式 512 比特分组密码算法，可以支持 128、256、384 和 512 比特密钥长度。可以用于高度敏感数据的安全保护。 需要将密码算法软件正确实现，保证具有较高加解密效率，保证软件整体实现的安全性及具有实用性。具体应用方面可以将其用于存储中的数字文件的加密和解密，即制作一个文件加密软件，也可以寻找更合适的场景做具体应用。

完成的软件应满足：

1.按图实现加解密算法，支持规定的密钥长度。

2.在密钥管理、分组密码工作模式、不满组处理、随机数生成、消息认证码产生、报文完整性等方面应该有合理的自主创新。

3.加解密大文件时，主频 1.8GH（8 核 I5-8265U）的普通 PC 机上运算效率不低于每秒 100000 个分组。

4.软件界面美观、实用（易操作）。

参考资料：

算法说明：

分组长度 512 比特，密钥长度可 128、256、384、512 比特。基于 SM4 和 SM3 算法，采用 Feistel 结构，迭代 4 轮，见图 1 。

图中的“SM3”表示用 SM3 算法对输入的 384 比特数值（3 个 128 比特串接），计算 256 比特 hash 值。

加密时，SM4-Ki 表示以 Ki 为密钥，将 128 比特数据加密，i=1,2,3,4。

解密时，SM4-Ki 表示以 Ki 为密钥，将 128 比特数据解密，i=1,2,3,4。解密时，由密文组分割为 $A_4|B_4|C_4$，以 A_4 的左 128 比特为输入，以 K4 为密钥，用 SM4 算法解密，得到 C_3。以 A_4 的右 128 比特为输入，以 K1 为密钥，用 SM4 算法解密，得到 B_3。将 B_3、K2 和 C_3 联接为 384 比特数据串 $B_3|K2|C_3$，将 B_4 和 C_4 联接为 256 比特 $B_4|C_4$，用 SM3 算法对 $B_3|K2|C_3$ 计算 hash 值，得到 256 比特乱数，用该乱数与 $B_4|C_4$ 异或，得到 A_3。如此，可逐轮地逆推到 A_0、B_0 和 C_0。

当使用 128 比特密钥时，K1=K2=K3=K4。

当使用 256 比特密钥时，左 128 比特为 K1，右 128 比特为 K2，K3=K1，K4=K2。

当使用 384 比特密钥时，左 128 比特为 K1，中 128 比特为 K2，右 128 比特为 K3，K4=K1⊕K2⊕K3。

当使用 512 比特密钥时，按 4 个 128 比特，分别为 K1、K2、K3 和 K4。

有关文件加密的建议：

将该算法做成文件加密软件时，建议密文头部为：

第 1 字节为固定字符。第 2 字节为分组算法和工作模式标识。第 3 字节为密钥索引。第 4 至 14 字节为附加说明信息（主要是文件属性类信息，允许留白），第 15 至 22 字节为 IV（初始向量，可选的），第 23 至 32 字节为消息认证码（用于校验密钥），第 33 字节开始是密文正文。末尾不满组时可用密文填充（CBC 模式能否做到密文填充）。最后有 8 字节报文完整性认证标签。

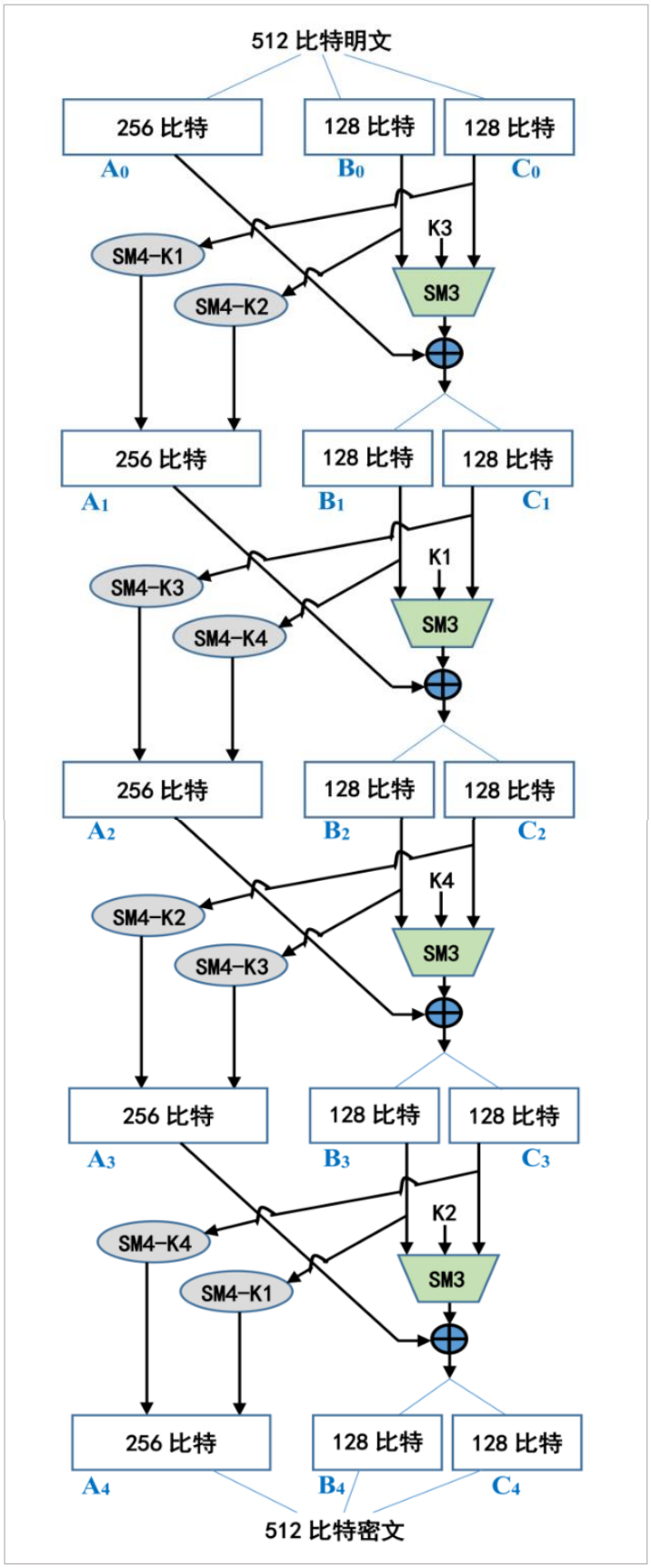

图 1　512 比特分组加密示意图

要求：

1、 可组队参与完成，每队成员不多于 3 人

2、 完成时间为 11 月 24 日（第 13 周结束）

3、 交付件包括完整的代码和系统展示（要求有界面）、完整的设计文档、答辩报告

4、 最后成绩由系统完整度（代码）、设计文档、答辩三部分组成