SM4算法

硬件

Intel Core i7-6600U，NVIDIA Geforce GTX 965M

环境

Windows 10，Visual Studio Community 2017（版本15.45），CUDA 9.1.85

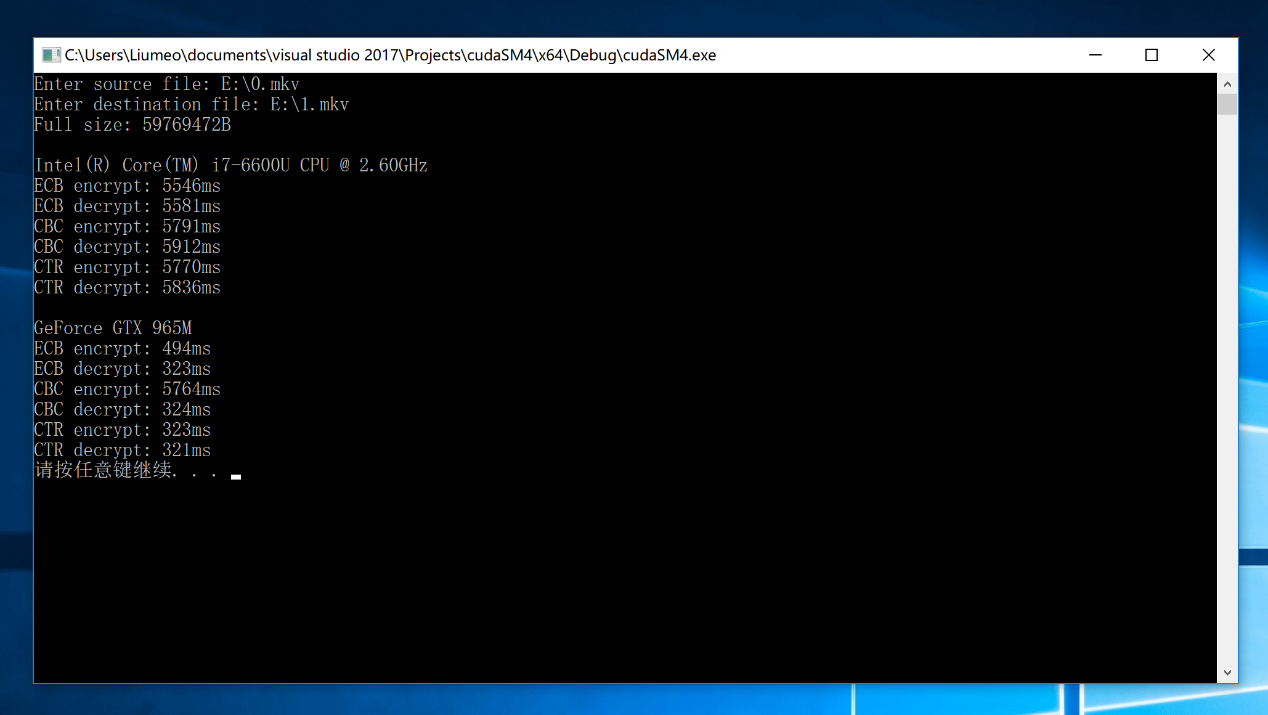
内容

首先实现了CPU的ECB、CBC、CTR模式。为减少无关操作，一律按照本机的小端方式存储、运算（在调试ECB时将明文和密文分别转换成大端，验证与官方文档的示例吻合）。CBC、CTR模式随机生成128位初始向量并放入密文开头。

然后在GPU上实现了三种模式，其中CBC模式的加密由于次序性无法并行，仍使用CPU计算。

测试

将一个58MB的视频从硬盘读入内存数组，不足16字节的末尾补0，用各种方式先加密到另一个数组，再解密回原数组，最后写到硬盘另一位置。新视频能正常播放，说明12次运算都是正确的。



可以看出，CPU运算的时间均为5000多毫秒，但GPU只需要300多毫秒（ECB加密时启动GPU有额外耗时，CBC加密用CPU），硬件加速的目的实现。

问题

1.最新版的Visual Studio与CUDA不兼容导致编译失败，详见<https://devtalk.nvidia.com/default/topic/1022648/cuda-setup-and-installation/cuda-9-unsupported-visual-studio-version-error/>

2.加密大文件时会爆掉显存。