1、背景

SM4算法是由国家商用密码管理办公室于2006年1月公布的分组对称密码算法，该算法在大量需要安全通信的应用中担当加密、解密的任务，具有安全、高校和简明等特点。如果能够提高SM4算法的加密和解密运算速度，也能在大文件的安全传输中提高效率。

CPU 为优化串行代码而设计，将大量的晶体管作为控制和缓存等非计算功能，注重低延迟地快速实现某个操作；GPU 则将大量的晶体管用作 ALU 计算单元，适合高计算强度的应用，具有运算密集型和高度并行的特点。因此，业界提出将GPU应用到密码算法的加速计算中。

2、可行性分析

SM4算法是分组加密算法，明文分组之间不存在数据依赖，加密时按明文分组进行加密，具备并行计算的条件。而加密（解密）是整个算法中最耗时的部分，因此，利用GPU的并行计算能力加速SM4算法计算具有理论可能性和实际需要。

3、加速运算模型



4、验证

5、分析和总结