

# SM4相关project

## SM4正常实现

按照SM4正常算法流程走下来的一套实现，在每一轮中主要采用T函数方法进行每一轮迭代

- sm4\_table中主要是各种表的具体数据
- sm4\_f中主要是定义的各项函数，包含T1 GetRK T encryptSM4 decryptSM4 encryptSM4\_t\_table encrypt\_simd
- sm4\_.cpp中为具体时间测试等，其中测试数据为：

明文： 01234567 89abcdef fedcba98 76543210

密钥： 01234567 89abcdef fedcba98 76543210

密文： 681edf34 d206965e 86b3e94f 536e4246

## SM4\_T\_table实现

T\_table可以通过设置一个flag位来直接生成该表，也可以通过直接复制粘贴，这里采用第二种方法在sm4\_table中直接将表给出，其作用主要体现在每一轮迭代时不是采用T函数而是进行查表运算减少了异或、移位等运算从而加快了速度。

将32位中8位进行摘取的方式这里采用在移位后强制类型转化为8位从而得到索引直接进行查表运算即可

运行结果如下：

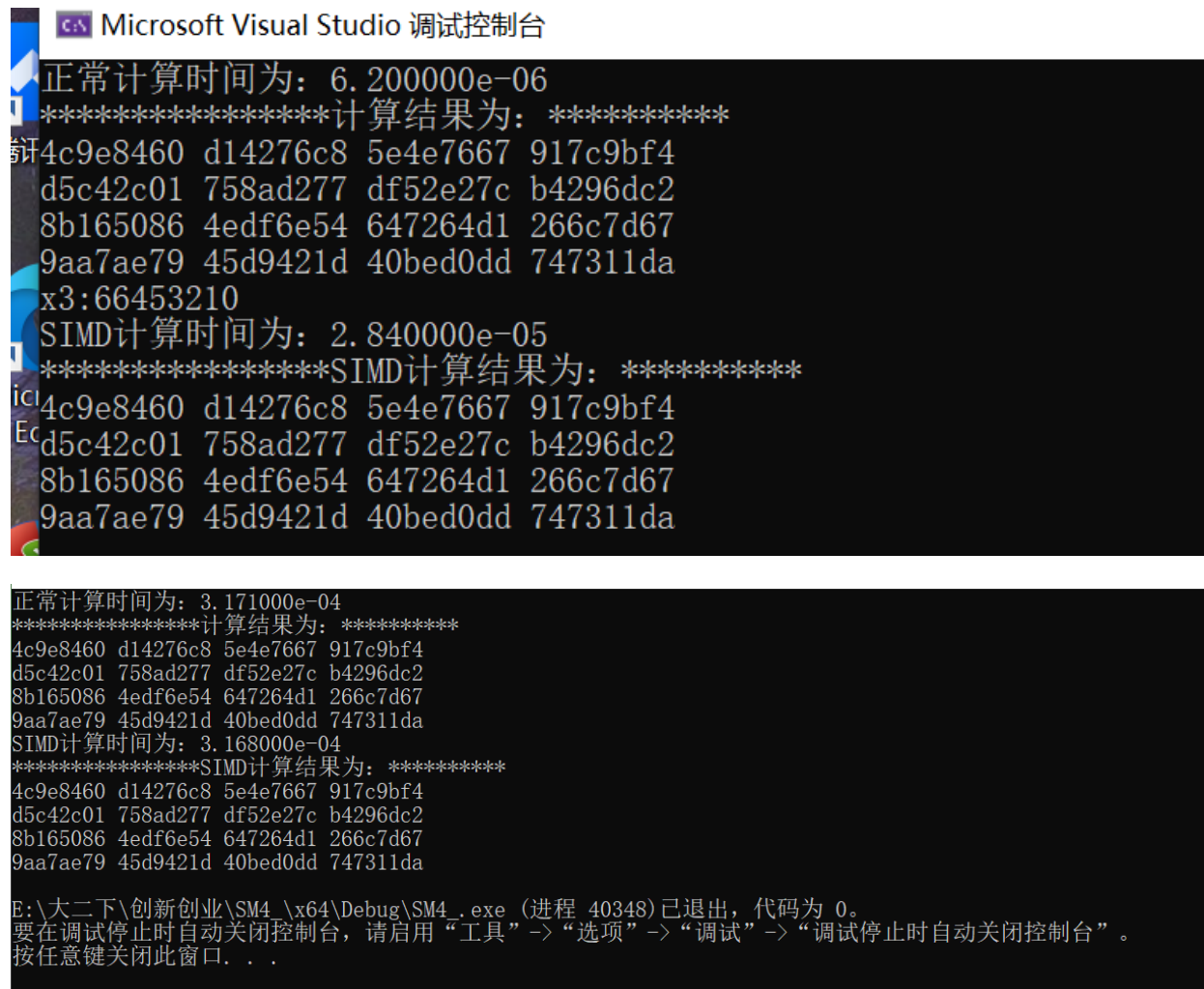
```
正常计算时间为: 5.600000e-06
*****正常计算结果为: *****
681edf34 d206965e 86b3e94f 536e4246
T_table计算时间为: 1.440000e-05
*****T_table计算结果为: *****
681edf34 d206965e 86b3e94f 536e4246
E:\大二下\创新创业\SM4\x64\Debug\SM4_.exe (进程 39376)已退出, 代码为 0。
要在调试停止时自动关闭控制台, 请启用“工具”->“选项”->“调试”->“调试停止时自动关闭控制台”。
按任意键关闭此窗口. . .

正常计算时间为: 4.710000e-05
*****正常计算结果为: *****
681edf34 d206965e 86b3e94f 536e4246
T_table计算时间为: 3.460000e-05
*****T_table计算结果为: *****
681edf34 d206965e 86b3e94f 536e4246
E:\大二下\创新创业\SM4\x64\Debug\SM4_.exe (进程 29912)已退出, 代码为 0。
要在调试停止时自动关闭控制台, 请启用“工具”->“选项”->“调试”->“调试停止时自动关闭控制台”。
按任意键关闭此窗口. . .
```

第一张为单次加密，第二张为15次加密，可以看出在对单次加密时使用T\_table后速度并没有加快，而在将该过程扩展到15次时这时T\_table的作用显示了出来。而在日常对消息加密时消息长度一般很长当采用ECB模式进行加密时这个时候T\_table可以明显加快速度。

## SM4用SIMD加速

这里采用128位4个32寄存器的模式来进行同时对四组明文进行加密的时间测试，结果如下：



```
Microsoft Visual Studio 调试控制台
正常计算时间为: 6.200000e-06
*****计算结果为: *****
4c9e8460 d14276c8 5e4e7667 917c9bf4
d5c42c01 758ad277 df52e27c b4296dc2
8b165086 4edf6e54 647264d1 266c7d67
9aa7ae79 45d9421d 40bed0dd 747311da
x3:66453210
SIMD计算时间为: 2.840000e-05
*****SIMD计算结果为: *****
4c9e8460 d14276c8 5e4e7667 917c9bf4
d5c42c01 758ad277 df52e27c b4296dc2
8b165086 4edf6e54 647264d1 266c7d67
9aa7ae79 45d9421d 40bed0dd 747311da

正常计算时间为: 3.171000e-04
*****计算结果为: *****
4c9e8460 d14276c8 5e4e7667 917c9bf4
d5c42c01 758ad277 df52e27c b4296dc2
8b165086 4edf6e54 647264d1 266c7d67
9aa7ae79 45d9421d 40bed0dd 747311da
SIMD计算时间为: 3.168000e-04
*****SIMD计算结果为: *****
4c9e8460 d14276c8 5e4e7667 917c9bf4
d5c42c01 758ad277 df52e27c b4296dc2
8b165086 4edf6e54 647264d1 266c7d67
9aa7ae79 45d9421d 40bed0dd 747311da

E:\大二下\创新创业\SM4\_x64\Debug\SM4_.exe (进程 40348) 已退出, 代码为 0。
要在调试停止时自动关闭控制台, 请启用“工具”->“选项”->“调试”->“调试停止时自动关闭控制台”。
按任意键关闭此窗口. . .
```

如上图，图一为一次加密4个无明显提速，但当加密明文数量不断提高至100组时SIMD速度有了提高，达到了预期效果。