

实验环境：

操作系统win10,编译器visual studio 2022,处理器Intel(R) Core(TM) i5-1035G1 CPU @ 1.00GHz 1.19 GHz

SM3的优化方法主要有：

- 1、减少函数调用
- 2、尽量使用逻辑运算
- 3、使用simd指令集进行优化

优化效果：

优化前：

```
Microsoft Visual Studio 调试控制台

time :5.581

D:\desk\大二下ppt\创新创业课程\sm3_c\sm3\x64\Debug\sm3.exe (进程 56056) 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。 . . .
```

进行一百万次sm3用时6s左右。

优化后：

```
Microsoft Visual Studio 调试控制台

66c7f0f4 62eedd9 d1f2d46b dc10e4e2 4167c487 5cf2f7a2 297da02b 8f4ba8e0
一百万次sm3运行时间 time :2.684s

D:\desk\大二下ppt\创新创业课程\sm3_c\sm3_SMID\x64\Debug\sm3_SMID.exe (进程 88124) 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。 . . .
```

进行一百万次sm3用时仅需3s,提速100%。