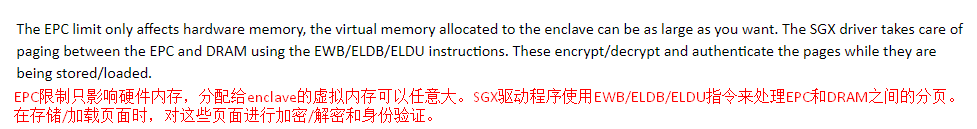
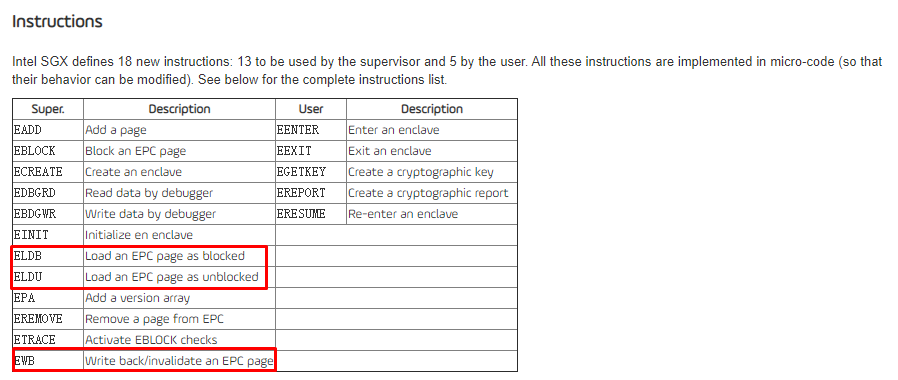
SGX 空间限制和性能情况的确认

一、 SGX 的内存大小是否只有128M或者256M?

这里的128M或者256M是物理内存的大小，是由BIOS分配的，在实际开发中通过硬件加驱动实现的“换页”操作，基本可以无限制（但是会影响性能，下面第二节会讲到）。





参考：

1. <https://groups.io/g/corda-dev/topic/is_the_sgx_size_limitation_a/21282207?p=,,,20,0,0,0::recentpostdate%2Fsticky,,,20,1,0,21282207>
2. <https://blog.quarkslab.com/overview-of-intel-sgx-part-1-sgx-internals.html>
3. <https://github.com/intel/linux-sgx/issues/87>

二、 SGX 的性能怎样？

SGX肯定会导致性能下降，因为：1）SGX在CPU内对数据会进行加解密操作，出了CPU全部是加密过的内容；2）额外的安全性检查；3）物理内存的使用限制；4）进出Enclave需要切换上下文等。

找到一篇文章从几个角度对比分析SGX的性能。

1. 运行查找最大值的计算

有4个场景：

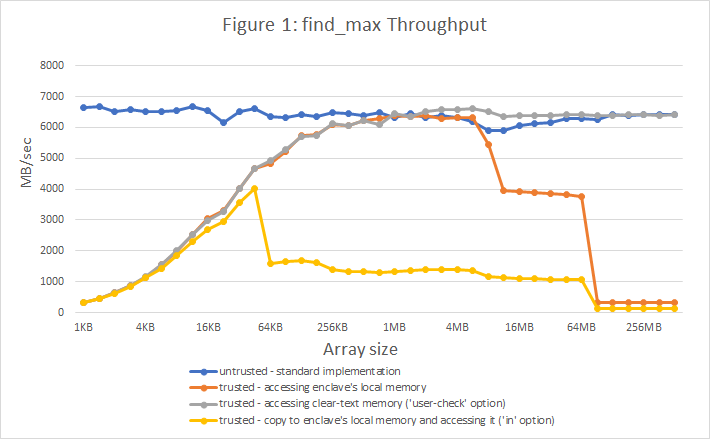
A)在Enclave外面计算；

B)把数据拷贝到Enclave里面，并在里面计算；

C)数据提前放在Enclave里面，然后在Enclave里面计算；

D)数据在Enclave外面，在Enclave里面计算

下面是测试结果，横轴是数据量的大小，纵轴是吞吐率



可以看出：数据量小的时候，性能差距还是挺大的，主要是上下文切换导致的；随着数据量的增加，上下文切换的时间占比小了；在64M的时候断崖式下降，这是因为EPC的物理内存大小就是64M，这个时候需要做切换页的操作。

2）计算SHA256

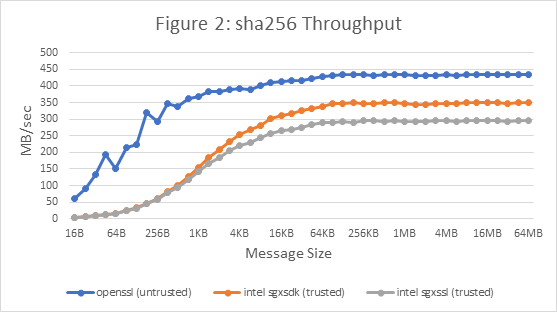
分3种场景，数据都放在Enclave外面，跟上面的D一样：

A)在Enclave外面使用Openssl库

B)在Enclave里面使用sgxsdk

C)在Enclave里面使用sgxssl

测试结果如下



可以看出：开始时还是有很大的差距，上下文切换的问题；但是最后还是有差距

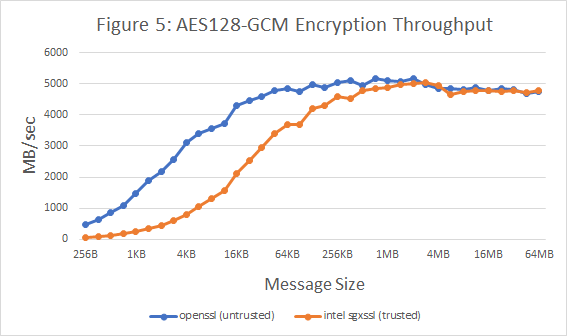
3）测试AES加密

分两个场景，数据也是放在Enclave外面，即测试1种的D场景：

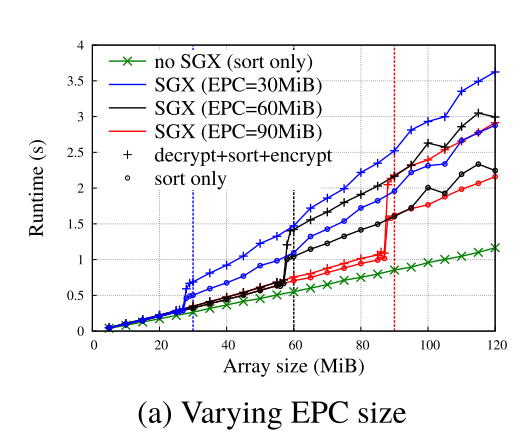
A)Enclave外面使用openssl库

B)Enclave里面使用sgxssl

结果如下：



另外，有一张图可以显示出页切换对性能的影响。



结论：

1. 影响性能的因素：上下文切换、页切换。数据量小的时候上下文切换影响明显，数据量大的时候页切换影响明显。通过将数据放在Enclave外面的方式可以降低切换页的影响。
2. Enclave内部运行如果需要加解密操作，需要依赖于库的使用，性能的好坏就受库的实现的影响。

参考：

1. <https://medium.com/@danny_harnik/impressions-of-intel-sgx-performance-22442093595a>
2. <https://software.intel.com/en-us/forums/intel-software-guard-extensions-intel-sgx/topic/796820>