《数据安全》实验报告

姓名：管昀玫 学号：2013750 班级：计科一班

**实验名称：**

SEAL应用实践

**实验要求：**

参考教材实验2.3，实现将三个数的密文发送到服务器，完成的运算。

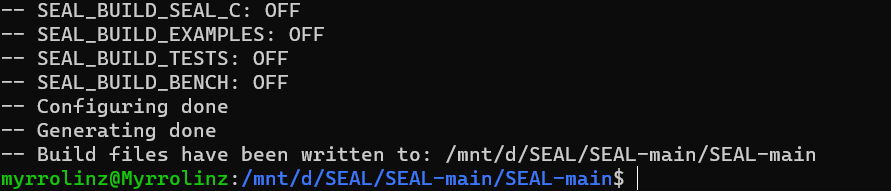
**实验过程：**

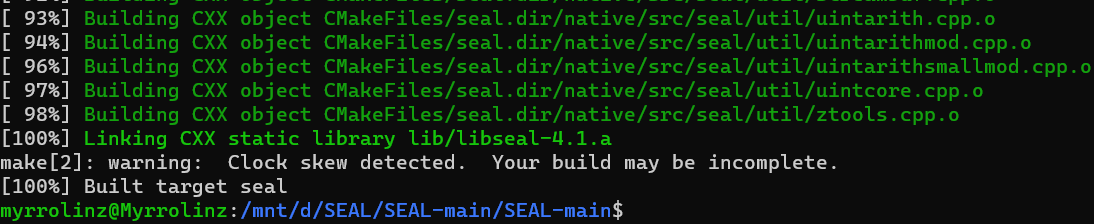
CKKS 是一个公钥加密体系，具有公钥加密体系的一切特点，例如公钥加密、 私钥解密等。代码中需要以下组件：

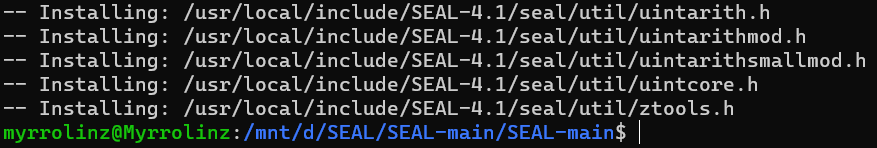
* 密钥生成器 keygenerator
* 加密模块 encryptor
* 解密模块 decryptor
* 密文计算模块 evaluator

1. 安装SEAL库

首先需要git clone相关GitHub repository，然后执行以下命令：

cmake .  


make  


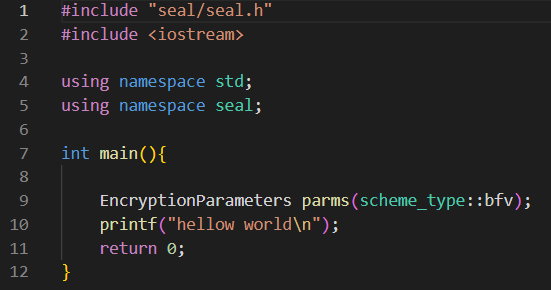
sudo make install  


由于网络原因，cmake时尝试多次才成功。个人经验：科学上网就能顺利安装。

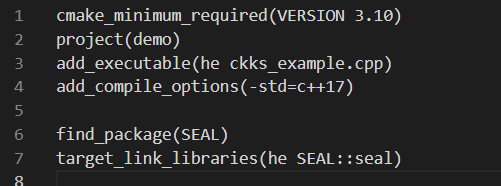
至此，SEAL库安装成功。

1. 简单测试程序

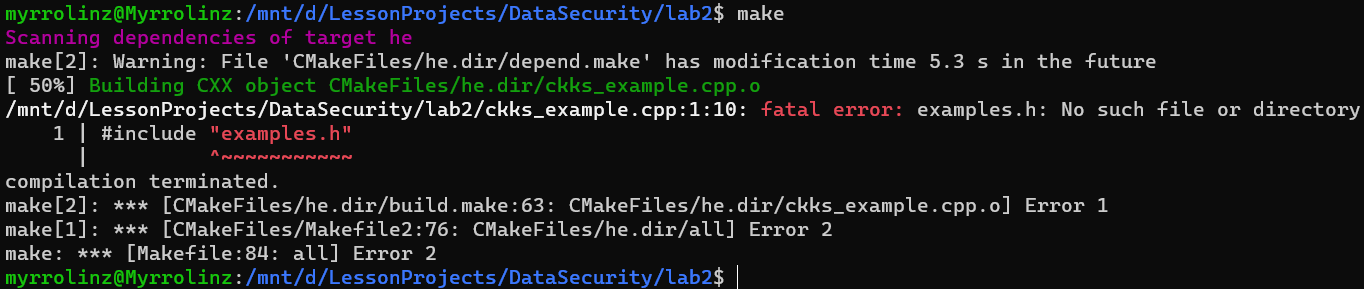
test.cpp如下所示:

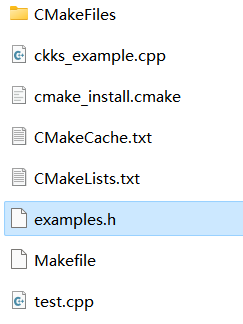
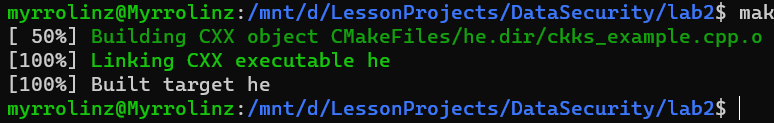
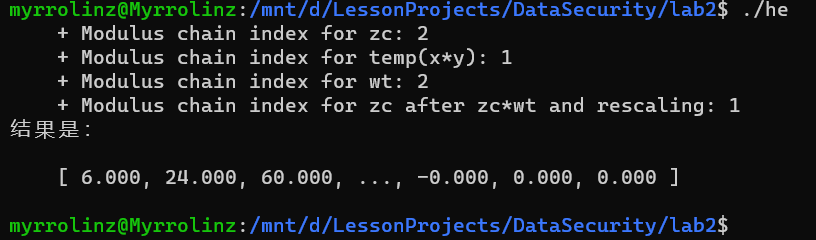


为了完成 test.cpp 的编译和执行，需要编写一个 CMakeLists.txt 文件，内容如下：



之后执行以下命令：

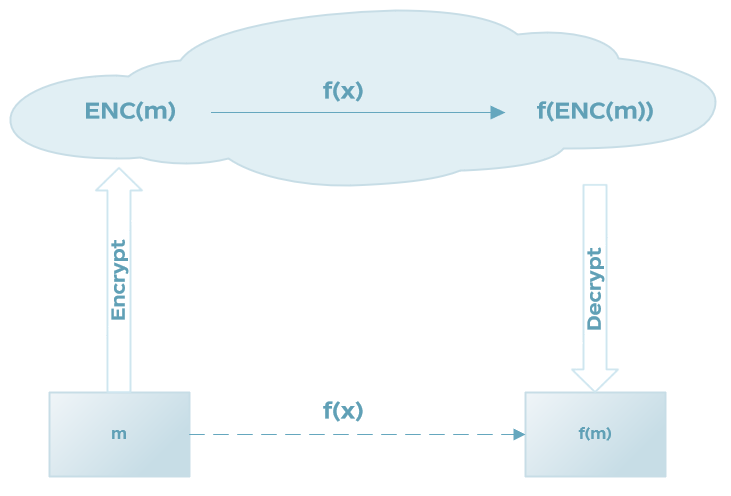
**cmake .**  
  
 **make**  


此处提示没有examples.h，只要从SEAL/native/examples中复制examples.h到我们的文件夹中即可。  
  
  
 **./he**  
  
 发现结果是正确的。

1. 计算

**心得体会：**

通过此次实验，我对同态加密有了更深的理解，学会了使用Paillier方案生成明文与密文，并学习到其中的数学原理——卡迈尔克函数与判定复合剩余假设。



半同态加密有一个很典型的应用场景：**连邦学习**。假设Alice和Bob想共同训练一个网络模型，Alice和Bob各自持有一部分训练数据，并且他们不想把自己的数据泄露给对方。那么在训练期间，Alice和Bob需要交互各自训练的梯度数据，并根据双方的梯度数据，共同计算一个对双方都合适的梯度值，用来执行联合梯度下降过程。

2019年，Ligeng Zhu等人发表的“Deep Leakage from Gradients”论文中给出了一种算法，可以从几次迭代的梯度数据中，推断出训练的数据，标签，模型等一系列隐私信息。这使得在分布式机器学习中，通过传输梯度数据来进联合模型训练变得不再安全。那么如果在梯度数据传输的过程中，传输的是加密后的梯度数据，并且这些加密数据可以进行二次计算，那么便可以规避梯度数据传输过程带来的安全风险。

还有一个典型应用场景是**隐私集合求和**。在在线广告投放的场景中，广告主（如商家）在广告平台（如媒体）投放在线广告，并希望计算广告点击的转化收益。然而，广告点击数据集和购买数据集分散在广告主和广告平台两方。使用加法 PHE 结合隐私集合求和（Private Intersection-Sum-with-Cardinality, PIS-C)协议可以在保护双方隐私数据前提下，计算出广告的转化率。协议中的“隐私保护求和”功能依赖于广告主将自己的交易数据用 PHE 加密发送给广告平台，使得广告平台在看不到原始数据的前提下，完成对交集中数据金额的聚合。该方案已被 Google 落地应用。