

北京理工大学
计算机学院
毕 业 设 计 （ 论 文 ）
中 期 报 告

基于国产密码算法的云计算网络信息传输认证系统设计与实现

学 号 1120161912

姓 名 侯添久

专 业 软件工程

班 级 08111602

导 师 闫怀志

学 院 计算机学院

2020 年 4 月 13 日

一 毕业设计（论文）进展情况

简述毕业设计（论文）进展情况和任务完成情况

进展情况：

- 1、完成毕业设计的开题，了解毕业设计所需要使用到的国产密码算法，编写开题报告和 PPT 等。
- 2、搭建本地开发环境，确定研究的方法，使用 socket 进行网络通信来模拟云计算环境下的数据传输，客户端运行在 windows 下，服务端部署在 Linux 服务器上。确定使用 Java 语言进行开发，Linux 上搭建 Java 的运行环境，设计网络信息传输认证系统架构。
- 3、阅读文献，学习云计算环境下数据传输的形式以及使用何种方式进行数据存储是安全的，学习密码算法的同态性，通过密码算法的同态性来保证存放在远程云服务器上的数据安全。密码算法的同态性是指对于密文的操作等价于使用明文进行相同的操作，即密文操作的结果与直接使用明文操作的结果是相同的。
- 4、学习密码算法的分类以及每种密码算法的作用和应用场景，密码算法主要分为非对称密码算法，对称密码算法以及数字摘要算法。一般地，使用非对称密码算法进行身份认证，数字签名等，通过公钥与私钥来确定通信官方的身份；使用对称密码算法对数据进行加密，保证数据的安全性；数字摘要算法主要用来生成一个散列值，其具有单向不可逆的特性，用来保证数据在传输过程中没有被第三方修改。
- 5、确定所使用系统的架构，主要分为客户端与服务端，客户端接收用户输入的数据，然后使用相应的国产密码算法对输入的数据进行加密得到相应密文，然后通过网络 socket 将密文发送给服务端，服务端接收到数据后，对数据进行字符串拼接操作，然后将拼接结果以及客户端传输的数据返回给客户端，客户端接收到数据分别进行整体解密与分割字符串解密的方式得到两个结果，最后对比两个结果判断是否相同，若是相同，则说明该密码算法满足同态性，否则，说明该密码算法不满足同态性。
- 6、学习相应的国产密码算法，主要学习了非对称密码算法 SM2，数字摘要算法 SM3 以及对称密码算法 SM4 三种密码算法。其中 SM3 具有单向不可逆的特性，只可以计算出散列值，而无法通过散列值解析出明文数据，所以无法用于本课题的研究。
- 7、进行客户端的编码工作，使用 socket 进行数据通信。客户端使用了单例模式，减少不必要的内存消耗，并将需要建立 TCP 连接 IP 与端口通过配置化的方式写在配置文件中，每次在程序启动时读取配置文件获得端口与 IP，避免程序中多次使用时造成混乱。
- 8、进行服务端的编码工作。服务端将需要监听的端口写在配置文件中，并使用单例模式创建相应的 socket 对象，避免每次都去创建对象，造成频繁的垃圾回收操作，导致程序的性能降低。使用 Java 中的线程池来提高程序的响应速度，使用原子类进行计数统计使用，显示这是客户端第几次的连接，通过原子类避免多个客户端同时连接的情况下计数错误，发生线程安全问题。
- 9、对于网络通信进行测试，修改 bug。
- 10、编码国产密码算法，对于三类国产密码算法，均会对应到一个相应的操作类，通过该操作类实现对数据的加密与解密操作。并且对于每一个操作类，也是使用单例模式。完成网络信息传输认证系统的实现和测试工作。
- 11、对于国产密码算法的性能分析，通过使用每种密码算法加解密的时间判断其性能。由于操作系统的资源分配是动态，可能某次执行分配的内存多，空闲的 CPU 较多，运行时间短。而另一次执行分配的内存资源少，CPU 空闲较少，导致运行时间长。这中不可控的因素会导致结果出现较大的差异，所以可以对每种密码算法运行多次，求得其平均值，再另外运行一次，当两者的加密时间与解密时间小于我们所给定的误差时，可以认为此时间就是该算法的加密时间与解密时间。
- 12、对系统整体进行测试，并修改测试中发现的 bug。
- 13、录制系统的演示视频，并让老师观看，评判是否满足毕业设计的要求。

14、对于系统进行相应优化处理。

15、开始进行毕业论文编写，编写完成后发给老师，请老师帮忙指导自己的论文，提出相应的改进意见并对论文进行修改。

16、进行论文的查重，编写答辩的 PPT 并且准备相关的答辩材料。

任务完成：

1、完成了相应的国产密码算法的调研与学习，主要是对 sm2, sm3, sm4 算法的调研学习，对于密码算法同态性的研究，学习同态加密的概念以及同态密码算法的分类，主要分为完全同态密码算法以及部分同态密码算法，完全同态密码算法指可以对密文进行任意的操作，并且结果与直接使用明文进行操作得到的结果相同；部分同态密码算法是指对密文只可以进行某种特定的操作，不可以进行其他操作，否则，无法与直接使用明文进行计算等价。

2、完成系统架构设计，编码工作。主要完成了客户端与服务端 socket 编写，测试，并且将服务端代码打包放在了阿里云服务器上，客户端直接在 windows 下运行。

3、完成对于每种密码算法的实验，主要是通过使用每种密码算法对数据进行加密，然后服务端拼接后返回给客户端进行对比，结果为 SM2 非对称密码算法不需要无法解密出正确的结果，得到的结果是乱码，无法识别；对于 SM3 因为具有单向不可逆的特性，所以无法进行实验；对于 SM4 算法的 ECB 模式，客户端解密后可以拿到正确的结果，但是中间会多出空格；对于 SM4 算法的 CBC 模式，客户端解密后得到的结果中有部分数据缺失，无法得到完成的数据。

4、完成网络信息传输认证系统的编码和实现工作。使用非对称密码算法 SM2 进行身份认证，对称密码算法 SM4 进行数据的加密以及数字摘要算法 SM3 生成散列值然后对散列值校验。

5、对于国产密码算法的性能分析，分别计算出了其加密时间与解密时间。SM2 算法的加密时间为 6ms，解密时间为 2ms；SM3 算法计算散列值的时间为 0.017ms~0.019499ms；SM4 算法的 ECB 模式下加密时间为 0.017ms~0.0323ms，解密时间为 0.037ms~0.0745ms；SM4 算法的 CBC 模式下加密时间为 0.015ms~0.020799ms，解密时间为 0.073ms~0.0767ms。通过数据可以看出性能最好的密码算法是对称密码算法 SM4 的 ECB 模式。

6、对于系统的优化，通过使用零拷贝技术的 MMAP 方式，减少数据在内核空间与用户空间频繁的拷贝造成程序性能下降，同时减少不必要的代码，提高程序运行效率。

7、完成视频录制，并将视频发送给毕业设计指导老师，经老师确认后开始进行毕业设计论文的编写工作。

8、目前处于毕业论文的编写中。

二 取得成果和存在问题

简述开展研究取得的成果和当前研究存在的问题

开展研究取得的成果：

- 1、学习了密码算法的分类，对称密码算法、非对称密码算法以及数字摘要算法等，并且学习了每种密码算法相应的应用场景，对称加密一般用于对于数据的加解密，非对称加密用于身份认证和数字签名，数字摘要算法主要对数据完整性进行校验等。
- 2、学习了相应的国产密码算法，非对称密码算法 SM2，数字摘要算法 SM3，对称密码算法 SM4，并且学习了密码算法的同态特性，对于数据安全性有了更加深刻的认识，了解了之前所熟悉的 RSA 非对称加密算法具有乘法的同态性。
- 3、重新认识了云计算的安全，在云环境中，不仅仅是考虑数据传输过程中数据的安全，更要考虑到数据存储的安全，不能直接以明文的形式存储数据，而是应该对数据进行加密，存储密文。对于需要使用到计算的数据，不需要将数据解密然后计算，因为解密拿到明文后可能会发生数据的泄露，无法保证数据安全，可以使用相应的具有同态性的密码算法，通过该密码算法加密数据，直接使用密文进行计算即可，只要保证使用密文计算的结果等价于直接使用明文计算的结果，最后把密文返回给用户，用户解密后拿到预期的结果。
- 4、对比了三种密码算法的性能，结果显示对于 SM4 的 ECB 模式加解密的效率最好。

当前研究存在的问题：

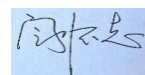
密码算法的同态性大致分为两种——全同态特性和部分同态特性。全同态是指对于所有的计算操作都具有同态性，部分同态特性是指对于部分计算操作具有同态特性，对于国产密码算法的同态性只是使用了 sm4 加密算法的 ECB 模式，也只是简单的对字符串的拼接操作同态性，还未找到满足全同态特性的加密算法。

三 导师意见

导师对中期报告的审阅意见

侯添久同学自开题以来,已完成了相应国产密码算法学习与调研,网络信息传输认证原理以及云计算安全保护的实现原理,对网络传输认证系统设计符合预期的要求,工作内容安排合理,工作进度符合要求,可以按时完成毕设工作,顺利毕业。

导师签字:



2020 年 4 月 15 日

四 专业责任教授意见

专业责任教授意见

侯添久同学自开题以来,已经完成了国产密码算法的调研与学习,网络信息传输认证原理以及云计算安全保护原理的学习,开始了部分编码工作,工作内容安排合理,选题符合开题报告要求,能够按时完成毕设工作。

责任教授签字:



2020 年 4 月 18 日