

北京理工大学  
计算机学院

本科生毕业设计（论文）周志

学生学号： 1120161912

学生姓名： 侯添久

指导教师： 闫怀志

题目类别： 毕业论文

题目性质： 理论研究

毕业设计（论文）题目： 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

2019 ~ 2020 学年

### 题目内容：

本课题主要进行基于国产密码算法的网络信息传输认证系统原型设计与实现工作。国产密码算法是中国自主设计并实现的成熟加密算法系列，未来将在我国信息系统的安全设计和实现中获得广泛应用。本课题拟根据具体信息系统中的网络信息传输认证需要，对已有的国产密码算法的具体实现进行分析和研究，选择适用的对称加密、非对称加密以及消息摘要算法，实现云计算信息系统中的网络信息传输认证，并进行实际系统的应用效果分析与验证。

### 任务要求：

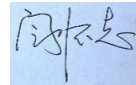
- 1、了解云计算网络信息传输认证和国产密码算法相关应用领域背景知识，了解国内外行业标准、规范和技术发展趋势，了解相关行业的政策和法律法规；
- 2、在指导教师指导下阅读国内外文献和相关知识，对已有的云计算网络信息传输认证和国产密码算法进行安全性分析和研究，根据云计算网络信息传输认证原理理解云计算安全保护的实现原理和方法。结合对现有云计算网络信息传输认证的研究，实现国产密码算法在其中的具体应用，最后在实际生产环境下进行分析与验证；
- 3、需要解决的问题有：A、云计算安全保护需求；B、云计算网络信息传输认证的实现原理与方法；C、实现对云计算网络信息传输认证的国产密码算法适配分析；D、实现一个简要的云计算信息系统中的网络信息传输认证的原型；
- 4、开发环境：操作系统：Windows 7 及以上和 Linux 发行版；开发语言：C、Java、Python 等，可根据实际系统选择；
- 5、完成毕业设计论文并提交相关文档；
- 6、毕业设计进度安排：
  - a. 查阅相关资料，完成基础知识的积累。（第 1 周-第 2 周）
  - b. 研究分析云计算网络信息传输认证的基本流程。（第 3 周-第 4 周）
  - c. 根据已有的云计算网络信息传输认证解决方案，实现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工作。（第 5 周-第 10 周）

d. 对云计算网络信息传输认证进行安全性分析，并验证其实际效果。（第 11 周-第 12 周）

e. 完成毕业论文，提交论文及相关文档。（第 13 周-第 15 周）

f. 完成本科生毕业论文答辩。（第 16 周）

指导教师签字：



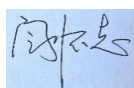
2019 年 1 月 6 日

2019 ~ 2020 学年 第 1 学期

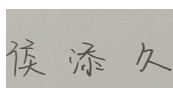
2020 年 1 月 6 日 ~ 2020 年 1 月 12 日（第 20 教学周）

本周工作情况	①了解所选课题的内容和要求。 ②完成开题报告初版的编写。
存在的主要问题	暂无。
后续工作计划	①完善开题报告的编写。 ②完成开题答辩 PPT 以及汇报工作。 ③了解国产密码算法。
指导教师意见	按照课题要求继续进行。有关国产密码算法，要搞清楚 SM 系列的区别。有具体问题联系我电话或微信指导。

指导教师签字：



学生签字：



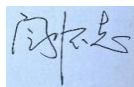
填写日期：2020-1-12

2019 ~ 2020 学年 第 1 学期

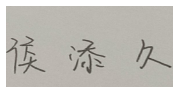
2020 年 1 月 13 日 ~ 2020 年 1 月 19 日（第 21 教学周）

本周工作情况	①了解所选课题的内容和要求。 ②完成开题报告初版的编写。
存在的主要问题	暂无。
后续工作计划	①完善开题报告的编写。 ②完成开题答辩 PPT 以及汇报工作。 ③了解国产密码算法。
指导教师意见	按照课题要求继续进行。有关国产密码算法，要搞清楚 SM 系列的区别。有具体问题联系我电话或微信指导。

指导教师签字：



学生签字：



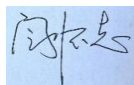
填写日期：2020-1-19

2019 ~ 2020 学年 第 2 学期

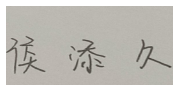
2020 年 2 月 24 日 ~ 2020 年 3 月 1 日（第 1 教学周）

本周工作情况	①了解国产对称加密算法—SM4，国产非对称加密算法—SM2，国产摘要算法—SM3。 ②使用 windows 做用户端，Linux 做服务端模拟云上资源，使用 Java 开发，开发工具使用 idea。
存在的主要问题	暂无。
后续工作计划	①了解加密算法在云计算中的应用过程。 ②搭建本地的 windows 开发环境，搭建云服务器的 Linux 的运行环境。
指导教师意见	使用 windows 做用户端，Linux 做服务端模拟云上资源，使用 Java 开发，开发工具使用 idea，思路可以。有问题联系我。

指导教师签字：



学生签字：



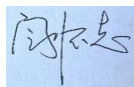
填写日期：2020-3-1

2019 ~ 2020 学年 第 2 学期

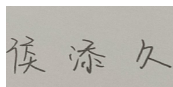
2020 年 3 月 2 日 ~ 2020 年 3 月 8 日（第 2 教学周）

本周工作情况	①本地搭建好开发环境，Linux 上搭建好 Java 的运行环境。 ②了解云计算的同态加密技术与代理重加密技术。
存在的主要问题	目前准备采用同态加密技术做国产密码算法的传输认证，不知道此方向是否满足老师的要求？
后续工作计划	①加密技术对比，国产密码算法选择。 ②开始编码。
指导教师意见	同态加密技术可以，满足课题要求。有问题联系我。

指导教师签字：



学生签字：



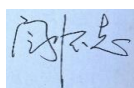
填写日期：2020-3-8

2019 ~ 2020 学年 第 2 学期

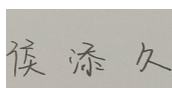
2020 年 3 月 9 日 ~ 2020 年 3 月 15 日（第 3 教学周）

本周工作情况	①进行外文文献的翻译工作。 ②编码使用 socket 进行数据传输。
存在的主要问题	暂无。
后续工作计划	①完成外文文献的翻译工作。 ②完成 socket 数据传输并测试。
指导教师意见	继续按照计划完成后续工作，有问题联系我。

指导教师签字：



学生签字：



填写日期：2020-3-15

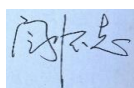


2019 ~ 2020 学年 第 2 学期

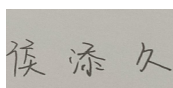
2020 年 3 月 16 日 ~ 2020 年 3 月 22 日（第 4 教学周）

本周工作情况	①完成 Java 客户端编写数据通信。 ②完成外文翻译工作。
存在的主要问题	根据调查，全同态加密目前没有实际的实现，所以可以完成针对密文的某个简单的函数操作吗？
后续工作计划	①完成 Java 服务端编写。 ②测试 socket 数据通信。
指导教师意见	继续按照计划完成后续工作，有问题联系我。

指导教师签字：



学生签字：



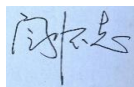
填写日期：2020-3-22

2019 ~ 2020 学年 第 2 学期

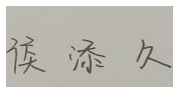
2020 年 3 月 23 日 ~ 2020 年 3 月 29 日（第 5 教学周）

本周工作情况	①完成了 Java 的 socket 数据通信服务端编写。 ②socket 数据通信本地测试。
存在的主要问题	暂无。
后续工作计划	①将服务端部署在阿里云服务器上。 ②调研具体的同态加密算法的实现，选择合适的国产密码算法。
指导教师意见	继续按照计划完成后续工作，有问题联系我。

指导教师签字：



学生签字：



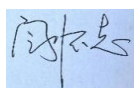
填写日期：2020-3-29

2019 ~ 2020 学年 第 2 学期

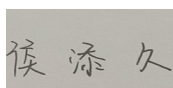
2020 年 3 月 30 日 ~ 2020 年 4 月 5 日（第 6 教学周）

本周工作情况	①调研具体国产密码算法的同态性。 ②socket 客户端测试。
存在的主要问题	暂无。
后续工作计划	①选择合适的国产密码算法。 ②国产密码算法编码。
指导教师意见	继续按照计划完成后续工作，有问题联系我。

指导教师签字：



学生签字：



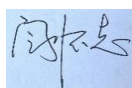
填写日期：2020-4-5

2019 ~ 2020 学年 第 2 学期

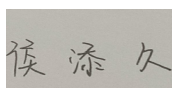
2020 年 4 月 6 日 ~ 2020 年 4 月 12 日（第 7 教学周）

本周工作情况	①选择合适的国产密码算法。 ②完成相应的国产密码算法的编码。
存在的主要问题	暂无。
后续工作计划	①国产密码算法测试。 ②进行整体 socket+ 国产密码算法测试。 ③进行网络信息传输认证系统的设计。
指导教师意见	继续按照计划完成后续工作，有问题联系我。

指导教师签字：



学生签字：



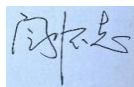
填写日期：2020-4-12

2019 ~ 2020 学年 第 2 学期

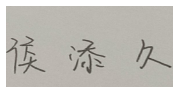
2020 年 4 月 13 日 ~ 2020 年 4 月 19 日（第 8 教学周）

本周工作情况	①完成国产密码算法的测试工作。 ②进行了 socket+国产密码算法的整体测试。 ③完成网络信息传输认证系统的设计工作。
存在的主要问题	暂无。
后续工作计划	①对于系统架构优化改进。 ②对相应的国产密码算法的同态性进行研究。 ③网络信息传输认证系统的实现与测试。
指导教师意见	继续按照计划完成后续工作，有问题联系我。

指导教师签字：



学生签字：



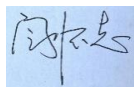
填写日期：2020-4-19

2019 ~ 2020 学年 第 2 学期

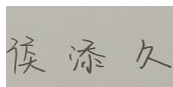
2020 年 4 月 20 日 ~ 2020 年 4 月 26 日（第 9 教学周）

本周工作情况	①使用 Java 的线程池，原子类，单例模式等对自己的方案进行优化改进。 ②完成对于国产密码算法的同态性研究。 ③完成传输认证系统的编码测试工作。
存在的主要问题	暂无。
后续工作计划	①对于国产密码算法加解密效率研究。 ②录制毕业设计的讲解视频。
指导教师意见	继续按照计划完成后续工作，有问题联系我。

指导教师签字：



学生签字：



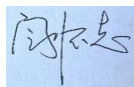
填写日期：2020-4-26

2019 ~ 2020 学年 第 2 学期

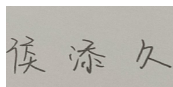
2020 年 4 月 27 日 ~ 2020 年 5 月 3 日（第 10 教学周）

本周工作情况	①完成对于国产密码算法加解密效率的研究。 ②完成毕业设计视频的录制。
存在的主要问题	暂无。
后续工作计划	①邀请老师根据视频对于毕业设计的中存在的问题给出指导。 ②开始编写毕业设计论文。
指导教师意见	可以按照要求开始撰写毕业论文。

指导教师签字：



学生签字：



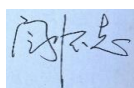
填写日期：2020-5-3

2019 ~ 2020 学年 第 2 学期

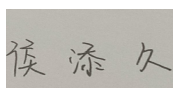
2020 年 5 月 4 日 ~ 2020 年 5 月 10 日（第 11 教学周）

本周工作情况	①根据老师的反馈，系统没有什么问题。 ②开始编写毕业设计，构思论文的整体结构，章节以及具体的内容。
存在的主要问题	暂无。
后续工作计划	①完成毕业设计论文的组织结构设计。 ②完成毕业设计论文中的前三章编写。
指导教师意见	继续按照计划完成后续工作，有问题联系我。

指导教师签字：



学生签字：



填写日期：2020-5-10

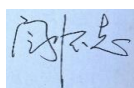


2019 ~ 2020 学年 第 2 学期

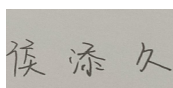
2020 年 5 月 11 日 ~ 2020 年 5 月 17 日（第 12 教学周）

本周工作情况	①完成了毕业设计论文的组织结构设计。 ②完成论文前三章的编写。
存在的主要问题	暂无。
后续工作计划	①完成毕业设计的论文。 ②邀请老师对毕业设计的内容进行指导。
指导教师意见	继续按照计划完成毕业论文。

指导教师签字：



学生签字：



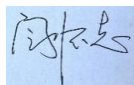
填写日期：2020-5-17

2019 ~ 2020 学年 第 2 学期

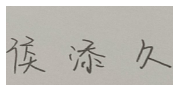
2020 年 5 月 18 日 ~ 2020 年 5 月 24 日（第 13 教学周）

本周工作情况	①完成了毕业设计论文的编写。 ②根据老师的指导意见修改毕业论文，并且邀请老师再次指导论文。
存在的主要问题	暂无。
后续工作计划	①完成毕业设计所有的修改。 ②对于毕业设计论文开始进行第一次查重检测。
指导教师意见	根据指导意见对论文进行修改。

指导教师签字：



学生签字：



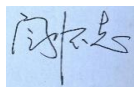
填写日期：2020-5-24

2019 ~ 2020 学年 第 2 学期

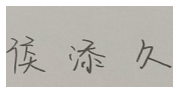
2020 年 5 月 25 日 ~ 2020 年 5 月 31 日（第 14 教学周）

本周工作情况	①根据老师的反馈，修改了毕业设计论文中不足的地方。 ②完成了毕业论文第一次的查重检测，查重率为 5.4%，符合学院要求。
存在的主要问题	暂无
后续工作计划	①开始准备毕业答辩的相关材料。 ②完成论文最终版提交。 ③准备最后的毕业答辩。
指导教师意见	准备好答辩相关材料，完成毕业论文提交。

指导教师签字：



学生签字：



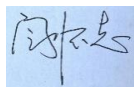
填写日期：2020-5-31

2019 ~ 2020 学年 第 2 学期

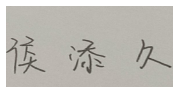
2020 年 6 月 1 日 ~ 2020 年 6 月 7 日（第 15 教学周）

本周工作情况	①完成毕业答辩所需要的材料。 ②完成系统详细的讲解视频录制。 ③提交了论文的最终版，检测结果符合学院要求。
存在的主要问题	暂无
后续工作计划	①准备毕业答辩。 ②提交后续所需要的材料。
指导教师意见	好好准备毕业答辩。

指导教师签字：



学生签字：



填写日期：2020-6-7