

北京理工大学

本科生毕业设计（论文）开题报告

学 院： 计算机学院


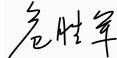
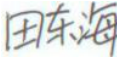
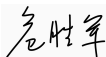
专 业： 软件工程

班 级： 08111602

姓 名： 侯添久

指导教师： 闫怀志

二〇二〇年一月二日

姓名	侯添久	学号	1120161912	班级	08111602	专业	软件工程
导师	闫怀志	校外导师（职称）	无		校外导师单位	无	
论文选题	题目名称	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					
	题目性质	软件开发（ ）		理论研究（ √ ）			
		工程设计（ ）		技术科学研究与工程技术研究（ ）			
评审组成员	题目来源	结合科研（ √ ）		结合生产实际（ ）			
		结合实验室建设（ ）		自拟题目（ ）			
评审意见	姓 名	职 称	工作单位及职务			签 字	
	戴银涛	副教授	北京理工大学				
	危胜军	副教授	北京理工大学				
	田东海	讲师	北京理工大学				
<p>（含：选题意义；选题是否满足毕业要求；技术方案是否可行；进度安排是否合理等）</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>侯添久同学的毕业设计题目是基于国产密码的云计算网络信息传输认证系统设计与实现，主要对已有的国产密码算法进行安全性分析与研究，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与方法。结合对现有云计算网络信息传输认证研究，实现国产密码算法在其中应用，最后在实际生产环境下进行分析与验证，毕业设计具有一定使用价值。选题满足毕业要求，技术方案可行，进度安排合理，难度合适，同意开题。</p> </div>							
成 绩		合格					
评审组长签字：  2020 年 1 月 6 日							

注：成绩以“合格”“不合格”记；评审组长为高级职称人员。

1 毕业设计（论文）选题的内容

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。

2 研究方案

2.1 本选题的主要任务

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。

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。

实现云计算安全保护需求，云计算网络信息传输认证的实现原理与方法，对云计算网络信息传输认证的国产密码算法适配分析，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。

2.2 技术方案的分析、选择

实现网络中的传输认证，可以从最熟悉的 HTTP 开始，HTTP 只是进行了数据的传输，并没有实现传输的认证的功能。在 HTTP 协议之上，可以加上一层 SSL 作为传输认证功能的实现，相应的会产生一个与之相应的网络协议——HTTPS，与 HTTP 相比，HTTPS 具有身份认证，对数据的加密传输，以及数据完整性校验等功能。那么，对于本课题就可以借鉴 HTTPS 的 SSL 的实现进行相应方案的设计。

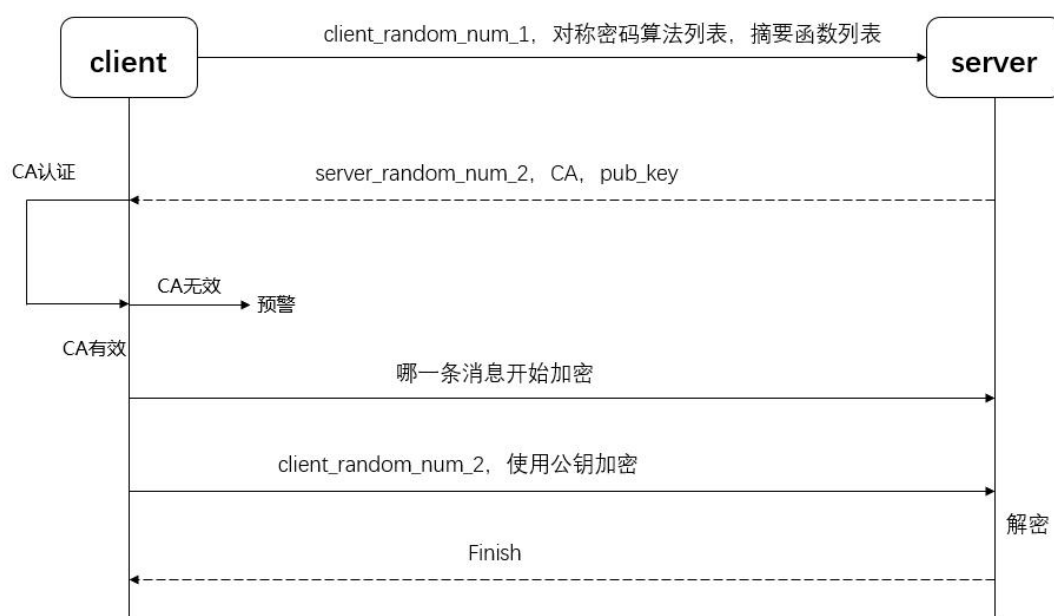
HTTPS 建立连接的过程主要分为以下几个阶段：

用户端生成一个随机数 1，并将自己的所支持的密码算法列表。摘要函数列表和该随机数 1 发送给服务端。

服务端接收之后，选择适当的密码算法和摘要函数，并生成一个随机数 2，之后将 CA 证书，随机数 2 发送给用户端。

用户端接收之后，先进行 CA 证书验证，如果 CA 证书有效，获取其公钥，然后生成随机数 3，并使用公钥加密该随机数，发送给服务端。

服务端接收到相应的随机数，根据双方三个随机数确定下来对称密钥，双方可以进行相应的数据传输。



对于现在互联网的发展，人们已经不是简单的将应用部署在自己的服务器上，而是会使用云来承担服务器的角色，将自己的应用程序部署在云上，而不用去考虑高并发下服务器资源等问题，资源的虚拟化完全可以更加智能化的处理。但是在云上部署的应用程序使用简单的 HTTPS 进行传输，因为会存在三种角色，用户，应用程序提供者，云服务提供商，那么对于用户的数据来讲，由原来应用程序提供者获得变为应用程序提供者和云服务提供商都会获取到，用户的数据相当于被泄漏。

解决上述问题可以使用同态加密技术，同态加密是基于数学难题的计算复杂性理论的密码学技术。对经过同态加密的数据进行处理得到一个输出，将这一输出进行解密，其结果与用同一方法处理未加密的原始数据得到的输出结果是一样的。

实现方案可以从经典的五层网络模型出发，在传输层，使用面向连接可靠的传输协议 TCP，使用 socket 套接字进行操作完成数据传输的功能，基于 TCP 之上加一层 SSL 来进行身份认证，数据加密，数据完整性验证。在密码算法的使用上使用相对应的国产密码算法，整体的加密流程采用同态加密技术。

其中，身份认证使用国产密码算法相应的非对称加密算法，数据加密使用国产密码算法对应的对称加密算法，数据完整性校验使用一些摘要函数。

对于密码算法的适配分析，考虑从结果出发，使用不同数据，对不同的密码算法进行加解密。然后判断其身份认证和加解密时间的长短来进行密码算法的适配。

2.3 实施技术方案所需的条件

开发环境：Windows，Java（jdk1.8），idea

软件条件：Jdk1.8，idea

硬件条件：Linux 服务器一台，Windows 开发机一台

服务端程序部署：将写好的服务端程序打成 jar 包部署在 Linux 服务器上。

用户端程序：使用 Java 编写用户端进行模拟。

2.4 存在的主要问题和关键技术

目前存在的主要问题是对于相应的国产密码算法和同态加密技术了解的不多，需要仔细去研究密码算法的原理和同态加密技术的执行流程。对于密码算法在此场景下的适配分析，只是单纯的从实践的角度去考虑，没有严格的理论上的依据的支撑，一定程度上缺少说服力，而且，在计算机中，单纯靠加解密算法时间进行判断会受到较大的干扰，因为计算机整个内存是一直在不断变化的，可能会存在有的时候内存资源较大，操作系统分给该进程的资源不需要执行一些内存淘汰策略，但是有的时候，内存资源较少，分给该进程的内存资源少，执行时内存不够，就需要执行一定的内存淘汰策略，导致耗时增加。

技术的关键在于密码算法的选取，需要选取非对称加密算法，对称加密算法以及一个摘要算法，主要从加解密效率进行研究。选取的原则：效果较好，加解密效率高国产密码算法。

2.5 预期能够达到的研究目标

预期所可以达到的研究目标是能够使用国产密码算法进行基本传输的认证——身份认证，数据加密，数据完整性校验，同时加解密所需要的时间较短，加解密的效率较高。

最后提交的有源代码，单元测试计划，系统测试计划，需求分析文档，概要设计文档，详细设计文档，用户手册。

3 课题计划进度表

查阅相关资料，完成基础知识的积累。（第1周-第2周）

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）

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）

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）

完成毕业论文，提交论文及相关文档。（第13周-第15周）

完成本科生毕业论文答辩。（第16周）

4 参考文献

- [1] 程晋格. 国密算法在数据存储及码流数据传输中的应用[J] 2018, (07):15-18.
- [2] 王栋, 李国春, 俞学豪, 陈智雨, 葛冰玉, 谢磊, 谭静. 基于量子保密通信的国产密码服务云平台建设思路[J] 2018, (07):171-178.
- [3] 刘悦, 贾忠田, 张波. 结合国产密码算法的应用密码学课程教学探讨[J] 2018, (03):10-13.
- [4] 鲍海燕. 基于同态加密算法的网络信息安全保护 [J] 2019, (24):22-25.