编号：_____

桂林電子科技大学
GUILIN UNIVERSITY OF ELECTRONIC TECHNOLOGY

毕业设计(论文)任务书

课　　题：	关于隐私保护分布式统计的算法研究
学　　院：	数学与计算科学学院
专　　业：	信息与计算科学
学生姓名：	王智坚
学　　号：	1800710238
指导教师单位：	数学与计算科学学院
姓　　名：	张必山
职　　称：	副教授

题目类型： □实践报告（法学院） □案例分析（法学院） □工程设计 □工程技术研究 □软件开发 □实验研究 ☑理论研究 □委托设计（艺术与设计学院） □参赛设计（艺术与设计学院） □科研协作（艺术与设计学院） □命题性概念设计（艺术与设计学院） □应用研究（文科） □应用研究（外国语学院） □科研协作（北海） □生产实践（北海） □命题性概念设计（北海）

2021 年 11 月 22 日

注：1、本任务书一式两份，一份院或系留存，一份发给学生，任务完成后附在说明书内。

2、任务书均要求打印，打印字体和字号按照《本科生毕业设计（论文）统一格式的规定》执行。

一、毕业设计（论文）的内容

1.对课题的总体介绍

在分布式统计中，多台计算机的数据传输，对于一些隐私数据（公司的机密文件，个人专利数据等）不能得到有效的保护，此时，可以利用同态加密算法对数据进行加密，再通过认证传输协议使得传输过程信息不会被篡改，最终使得数据得到保护利用同态加密算法对隐私数据进行加密，对隐私数据的保护具有重大的实际意义。

2.课题内容

多方协作下的数据保护是一个重要课题。由于数据的隐私性，一旦发生泄露，对个人或对数据的提供商来说都是一种损失。因此在数据的传输过程中对数据加密，使用密文传输是一种很好的方法。本题研究分布式系统下的隐私保护问题。

3.课题的主要任务

同态加密下的数据加密安全；传输过程中的数据安全；出现不受信任的计算方时，能否防止其从计算过程中推导出原数据。

二、毕业设计（论文）的要求与数据

1. 熟悉数据传输的机理的理论知识；
2. 掌握同态加密算法有关的数学知识；
3. Matlab 编程软件；
4. 具备一定的编程能力。

三、毕业设计（论文）应完成的工作

1. 开题报告；
2. 毕业论文（一万字以上），要有中英文摘要，中文摘要 400 字，英文摘要 300 到 500 字，论文撰写规范，文字要通畅，图表齐全，书写工整，要有自己的创意，内容要充实，有理有据；
3. 专业英文文献原文及翻译各一份，翻译要求内容基本准确，符合中文表达方式，行文要流畅；
4. 读书笔记（至少 3000 字）。

四、应收集的资料及主要参考文献

[1] 王友琛. 基于区块链的安全多方计算研究[D]. 兰州：西北师范大学, 2020.

[2] 朱岩, 宋晓旭, 薛显斌, 秦博涵, 刘国伟. 基于安全多方计算的区块链智能合约执行系统[J].密码学报, 2019, 6(02): 246-257.

[3] 黄建华, 江亚慧, 李忠诚. 利用区块链构建公平的安全多方计算[J]. 计算机应用研究, 2020, 37(01): 225-230-244.

[4] 蒋瀚, 徐秋亮. 基于云计算服务的安全多方计算[J]. 计算机研究与发展, 2016, 53(10): 2152-2162.

[5] 蒋瀚, 徐秋亮. 实用安全多方计算协议关键技术研究进展[J]. 计算机研究与发展, 2015, 52(10): 2247-2257.

[6] 李顺东, 窦家维, 王道顺. 同态加密算法及其在云安全中的应用[J]. 计算机研究与发展, 2015,52(06): 1378-1388.

[7] 杨攀, 桂小林, 姚婧等. 支持同态算术运算的数据加密方案算法研究[J]. 通信学报, 2015, 36(01): 171-182.

[8] 刘明洁, 王安. 全同态加密研究动态及其应用概述[J]. 计算机研究与发展, 2014, 51(12): 2593-2603.

[9] M. I. Wade, M. Chouikha, T. Gill, W. Patterson, T. M. et al "Distributed Im age Encryption Based On a Homomorphic Cryptographic Approach," 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2019, pp. 0686-0696

五、试验、测试、试制加工所需主要仪器设备

1、计算机一台；

2、打印机一台。

任务下达时间：

2021 年 11 月 22 日

毕业设计开始与完成时间：

2021 年 11 月 29 日—2022 年 5 月 6 日

组织实施单位：数学与计算科学学院 信息与计算科学系

教研室主任意见：

符合专业培养方案要求，同意通过。

签字 李姣芬 2021 年 12 月 16 日

学院领导小组意见：

该任务书要求符合培养方案要求，审核通过。

签字 2021 年 12 月 22 日