编号：_____

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

毕业设计开题报告

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
姓　　名：	张必山
职　　称：	副教授

填表日期：2021 年 12 月 3 日

开题报告填写要求

1．开题报告作为毕业设计（论文）答辩委员会对学生答辩资格审查的依据材料之一。此报告应在指导教师指导下，由学生在毕业设计（论文）工作前期内完成，经指导教师签署意见审查后生效。

2．开题报告内容必须用黑墨水笔工整书写，或按教务处统一设计的电子文档标准格式打印，禁止打印在其它纸上后剪贴，完成后应及时交给指导教师签署意见。

3．学生查阅资料的参考文献应在 10 篇及以上（不包括辞典、手册）。

4．有关年月日等日期的填写，应当按照国标 GB/T 7408—94《数据元和交换格式、信息交换、日期和时间表示法》规定的要求，一律用阿拉伯数字书写。如“2012 年 12 月 25 日”或“2012-12-25”。

毕业设计（论文）开题报告

1．本课题的研究内容、重点及难点

研究内容：

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。

重点及难点：

加密后的数据传输构建模型，讨论模型的可行性。

2．准备情况（已查阅的参考文献或进行的调研）

[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, et al. Zeng, "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.

毕业设计（论文）开题报告

3．实施方案、进度实施计划及预期提交的毕业设计资料

实行方案：收集汽车产品、数码产品或其他样本数据，据预处理，包括对冗余、与任务无关数据的删除，缺失数据、数据异常性的讨论等；利用预处理的后的数据结合数据传输原理建立数学模型，对所建立的数学模型所采用的加密算法实现隐私数据的保护做出科学的解释。

进度计划：

序号	周次	计划完成内容
1	第一周～第二周	拟制研究计划，收集有关文献，提交开题报告。
2	第三周～第四周	阅读相关文献和书籍，并完成论文引言。
3	第五周～第七周	学习同态加密，安全多方计算协议，了解仿真实验。
4	第八周～第十周	论文初稿完成，完成外文资料翻译。
5	第十一周～第十二周	修改论文。
6	第十三周～第十四周	总结并完成论文。
7	第十五周～第十六周	根据盲审意见修改论文，提交论文，准备答辩，制作 ppt。

预期效果：

建立出数学模型，讨论其对数据的保护性并完成一篇高质量的毕业论文。

毕业设计（论文）开题报告

指导教师意见
同意。请按任务书要求和开题报告的计划，按时按进度完成毕设工作。 指导教师： 2021 年 12 月 3 日
开题小组意见
研究内容具体，重难点分析到位，研究方案和进度计划可行，符合专业培养方案，审核通过！ 开题小组组长签字： 2021 年 12 月 19 日
院系审核意见
符合培养方案要求，同意开题。 院系主管领导签字： 2021 年 12 月 22 日