

# 毕业设计开题报告

|  |  |
| --- | --- |
| 题目： | 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 |
| 专业： | 信息与计算科学 |
| 学生姓名： | 王智坚 |
| 学生学号： | 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 |

填表时间：2021年12月3日

**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].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,林建财,田丰,张学军.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. Washington and J. Zeng, "Distributed Image Encryption Based On a Homomorphic Cryptographic Approach," 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2019, pp. 0686-0696, doi: 10.1109/UEMCON47517.2019.8993025. |
| 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 | 起止日期 | 计划完成内容 | 实际完成内容 | | 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 | 学习数据传输原理与同态加密 |  | | 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 | 提交论文，  准备答辩。 |  |   **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 |
| 指导老师： 张必山  2021年12月3日 |
| 开题小组意见 |
| 答辩小组组长签字：  2021年12月19日 |
| 院系审核意见 |
| 院系主管领导签字：  2021年12月22日 |