**山 东 大 学**

**本科毕业论文（设计）开题报告**

|  |  |
| --- | --- |
| **姓 名:** | **韩金池** |
| **学 号:** | **201822180284** |
| **学 院:** | **网络空间安全学院(研究院)** |
| **专 业:** | **网络空间安全** |
| **指 导 教 师:** | **周梓梦** |
| **填 表 日 期:** | **2022年2月27日** |

**山东大学本科生院制**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 论文（设计）  题目 | 面向边缘系统的轻量级加密算法设计与实现 | | | | | | |
| 论文  （设计）类型 | 基础理论 |  | 选  题  来  源 | 指导教师  科研项目 | 国家项目 |  |
| 应用研究 |  | 部省(市)项目 |  |
| 开发研究 |  | 学校项目 |  |
|  |  | 生产单位 |  | |
|  |  | 自 拟 |  | |
| 论文（设计）的主要内容、理论意义和应用价值：  边缘系统随着物联网发展相伴而生，边缘计算技术意味着许多控制将通过本地设备实现而无需交由云端，处理过程将在本地边缘计算层完成。这无疑将大大提升处理效率，还可以产生更快的网络服务响应，而轻量级密码算法的设计目标是为资源受限的设备制定密码解决方案，因此我们将轻量级密码算法与边缘系统相结合，在不大幅度降低边缘计算处理效率的情况下，同时保证边缘系统通信的安全。  边缘系统主要使用由Powercast公司所推出的面向无源感知领域的无源传感器网络开发套件 PowercastP2110-EVAL-01作为边缘设备进行开发，它包括接收端、发送端、天线等硬件，源代码中还实现了满足**IEEE 802.15.4**规范的通信协议。基于边缘系统中数据安全与隐私保护的挑战和轻量级加密算法的优势，在边缘系统中设计和实现轻量级加密算法来有效的保障数据通信的安全性以及系统性能的稳定性。  该毕业设计聚集边缘系统的安全解决方案，对物联网这一新兴行业发展提供学术分析与实践，并且为物联网安全的普及和建设出一份力。此外，通过本课题的研究，可以综合利用在校所学计算机体系结构、密码学、程序设计语言等方面的知识，将理论与实践相结合。不仅增强了主动发现问题、分析问题和解决问题的能力，而且进一步提升了自身科研与实践技能，为以后从事的计算机或密码学相关工作打下坚实的基础。 | | | | | | | |
| 主要参考书目：  1.《Microchip 无线 (MiWi™) 应用程序编程接口——MiApp》  2.《Microchip 无线 (MiWi™) 介质访问控制器——MiMAC》  3.《Microchip 无线 (MiWi™) P2P无线协议》  4.《MRF24J40数据手册》 | | | | | | | |
|  | | | | | | | |

**毕业论文（设计）写作计划**

（ 2022 年 3 月 1 日 至 2022 年 5 月 24 日）

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 各阶段工作时间 | 论文（设计）各阶段工作内容及要求 | | | | 检查方式 |
|  |  | | | |  |
| 指导教师意见：  指导教师签字： 年 月 日 | | | | | |
| 初稿完成日期 | |  | 定稿日期 |  | |
| 学院审核意见：    负责人签字： 年 月 日（单位公章） | | | | | |

注：本开题报告填写一式二份（学院、指导教师各一份）