自由探索计划“天目启航”专项项目选题征集表

|  |  |  |  |
| --- | --- | --- | --- |
| **教师姓名** | **王辈** | **学 院** | **集成电路学院** |
| **职 称** | **讲师** | **联系方式** | **15155109375** |
| **邮 箱** | **wangbei91@nuaa.edu.cn** | **研究方向** | **密码学** |
| **项目名称** | **模运算的量子线路设计** | | |
| **项 目 简 介（200字左右）** | **随着量子计算的发展，以Shor算法为首的量子算法将对传统公钥密码算法（RSA/ECC）造成严重威胁，它可以在多项式时间内求解其底层数学困难问题（大整数分解/椭圆曲线离散对数）。由于当前量子计算机的发展还没有到通用阶段，量子计算的资源有限，所以在设计量子线路求解整数分解或离散对数时，节约量子资源(如量子比特数与量子门数)至关重要。以密码学量子安全性分析为背景，设计量子模加、模乘、模逆等量子线路，实现量子线路深度或量子比特数的优化。** | | |
| **人 员 技 术 需 求** | **主要职责、任务** | **需求人数** | **专业及技能要求** |
| **理论学习** | **2** | **线性代数和量子计算理论** |
| **量子编程语言学习** | **2** | **熟悉python或C++，学习量子编程语言** |
|  |  |  |
|  |  |  |
|  |  |  |
| **备 注** |  | | |