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** | **哈希函数SHA3的硬件设计** | | |
| **项 目 简 介（200字左右）** | **哈希函数是密码学中的重要工具，目前以Keccak函数设计的SHA3函数在后量子密码算法应用广泛。基于格的后量子密码算法Kyber/Dilithium硬件实现中哈希函数的资源占比较大，当前一些通过折叠（folded）设计的方式降低了部分资源但还有很大的进步空间。请针对Keccak函数的硬件设计，相比最新研究成果降低一定的周期数与其他硬件资源指标（LUT,FF,DSP）等。** | | |
| **人 员 技 术 需 求** | **主要职责、任务** | **需求人数** | **专业及技能要求** |
| **调研材料，理论学习** | **2** | **哈希函数学习，keccak函数学习** |
| **Verilog代码撰写与资源评估** | **2** | **熟悉Verilog** |
|  |  |  |
|  |  |  |
|  |  |  |
| **备 注** |  | | |