课题预答辩申请表

|  |  |  |  |
| --- | --- | --- | --- |
| 申请人基本信息 | | | |
| 姓名 | 李小泉 | 学号 | 131199 |
| 导师 | 孙伟锋 | 责导 | 曹鹏 |
| 邮箱 | 605972145@qq.com | 电话 | 15366101580 |
| 课题成果基本信息 | | | |
| 课题名称 | 面向分组加密算法的可重构阵列处理单元的优化与设计 | | |
| 课题目标 | 针对分组密码算法的可重构实现提出了一套新的PE设计方案，用于减小功能单元的冗余，提高资源利用率，从而提高整个可重构平台的面积效率。 | | |
| 应用价值 |  | | |
| 课题指标 | |  |  | | --- | --- | | 考核指标 | 相应提升要求 | | 功能单元平均利用率 | 相较于其它所有架构平台提高50%以上 | | 性能面积比 | 相较于其它所有架构平台提高30%以上 | | | |
| 对比对象 | 与4个架构进行对比   1. RPU架构：所在单位在2015年设计的可重构密码架构（清华无锡研究院和实验室的合作项目）； 2. Cyptoraptor架构[1]：国外最新的研究成果，德州大学研发的一款高性能可重构处理器，发表于2014年的ICCAD； 3. RCPA[2]：解放军信息工程大学研究提出的一款高性能和高灵活的密码处理器； 4. COBRA[3]：是一款面向对称密钥算法提出的指令级分布式可重构处理器，串行结果的典型代表。 5. G Sayilar and D Chiou．Cryptoraptor: high throughput reconfigurable cryptographic processor[C]．IEEE/ACM International Conference on Computer-Aided Design，2014：155-161 6. Yang X, Dai Z, Yongfu A Z. Research and Design of Reconfigurable Computing Targeted at Block Cipher Processing[J]. Journal of Computer Research & Development, 2009, 46(6):962-967. 7. J Elbirt and C．Paar．An instruction-level distributed processor for symmetric-key cryptography[J]．IEEE Transactions on Parallel and Distributed Systems，2005，16(5)：468-480 | | |
| 对比结果 | 功能单元平均利用率提升百分比在110%到400%之间  性能面积比提升在150%到630%之间  两个指标均达到课题要求   |  |  |  | | --- | --- | --- | | 考核指标 | 提升百分比 | | | 功能单元平均利用率 | RPU | 360% | | Cyptoraptor | 400% | | RCPA | 170% | | COBRA | 110% | | 性能面积比 | RPU | 150% | | Cyptoraptor | 440% | | RCPA | 410% | | COBRA | 630% | | | |
| 来源项目基本信息 | | | |
| 项目类型和名称 |  | | |
| 考核指标 |  | | |
| 完成情况 |  | | |
| 项目负责人确认 |  | | |
| 附件列表 | | | |
| 文档 | 列出相关设计和测试文档 | | |
| 代码 | 列出相关设计和测试的代码目录 | | |
| 图表 | 列出相关设计、测试和实物的图或表格名称 | | |