国家 ASIC 工程中心学位论文修改情况表

研究生姓名	李小泉	学 号	131199	导师姓名	孙伟锋
学科/专业	微电子学与固体物理学				
学位论文题目	面向分组加密算法的可重构阵列处理单元优化与设计				

对学位论文内容所做的具体修改和充实情况

1. 是否应该先设计后优化，题目表述是否有疑义？
2. 顺序上有不妥，但优化与设计是同等级的名词，这样写也可以。
3. VF2 是何义，Ullmann 是何义，表 4-1 中算法的引文标准是否有误？
4. VF2 和 Ullmann 都是算法的名词，没有特殊的含义，具体介绍在论文第 45 页，图 4-1 中的文献标注有误，将原来的 68 调整为 71。
5. 你设计实现的 PE 阵列结构，如何使用，与 ASIC 设计有何区别？
6. 我设计的 PE 阵列是密码可重构系统中的一个重要部分，和外围借口电路和配置电路组成一个完整的可重构系统，与 ASIC 设计的区别主要体现在本文的 PE 阵列设计面向可重构系统，各个功能是可配置的，具有可编程性。
7. 附录是否置于参考文献之后？
   已按照老师意见对附录和参考文献的顺序进行了修改
8. 没有流片，为什么？
   课题时间比较紧张，因此没有进行后续的流片工作。
9. 对比结果中别人是否流片了？别人的数据是什么数据？
   论文中对比的其它架构也是综合的结果。
10. 可重构阵列处理单元包含什么？
    包含处理单元内部的各种功能单元和不同处理单元在阵列中的分布。
11. 面积效率跟原来相比提高多少，提高的方法是什么，付出的代价是什么？
    面积效率跟原来的相比提高比例在 57.1%~643.5%之间，本文从算法算子次序特征和算法映射反馈设计两方面消除密码可重构 PE 阵列中的冗余功能单元，给出了一套无功能冗余的密码可重构 PE 阵列设计方案，从而提升了整个系统的面积效率。和原来的架构相比，由于对部分功能单元进行了消除，对于未来出现的某些没有在本文测试结合中的算法，可能存在限制。
12. 是否只适用于这 30 中算法？
    不是，本文提出的架构适用于中 Feistel 网络结构、SP 网络结构、ARX 结构以及算法算子在本文处理单元功能范围内的所有算法。
13. 你的优化算法的映射时怎样做的？
    分析算法映射问题模型，将算法映射问题归纳为图论中的子图同构问题，通过修改 VF2 子图同构算法的约束条件，同时添加五个成本约束函数，完成整个算

法映射流程。

14. 你所谓的优化标准是什么？

架构中的冗余功能单元和低利用率单元都是可优化对象，优化的标准是在保证整体性能的前提下尽可能地降低阵列面积。

研究生（签名）：　　年　月　日

责任导师意见

责任导师（签名）：　　年　月　日