第七届“复微杯”全国大学生电子设计大赛

支持多种抗量子密码算法的
硬件加速协处理器设计与实现

数字赛道-安全

1 赛题简介

随着量子计算的不断发展，传统密码学正面临前所未有的挑战。虽然目前尚无法准确预测实用的量子计算机何时能够成为现实，但通过“现存后解”（Store-Now-Decry-Later，SNDL）的攻击方式，一旦量子计算取得突破，传统公钥密码体系下的敏感信息将不再机密可信。因此，当前开始准备从传统密码迁移到抗量子密码是必然选择。

2024 年 8 月 13 日，美国国家标准与技术研究院（NIST）正式公布三种抗量子密码（PQC）算法标准：ML-KEM（FIPS 203）、ML-DSA（FIPS 204）及 SLH-DSA（FIPS 205）。我国早在 2018 年就开展了抗量子密码算法的一系列工作。中国密码学会举办的全国密码算法设计竞赛活动分别遴选出公钥密码算法和分组密码算法一、二、三等奖，其中 Aigis-enc 抗量子公钥加密算法、Aigis-sig 抗量子数字签名算法和 LAC.PKE 抗量子公钥加密算法被评为公钥密码算法一等奖。

本赛道要求参赛者设计并实现支持多种抗量子密码算法的硬件加速协处理器。初赛将根据各个参赛队伍提交的内容进行打分，选取其中表现优秀的队伍进入决赛。

2 赛题要求

2.1 功能要求

使用硬件描述语言实现支持多种抗量子密码算法的硬件加速协处理器，至少支持 ML-KEM（FIPS 203）、ML-DSA（FIPS 204）算法，选手需自行评估和定义其中的硬件加速功能。要求：

1. 可扩展性，硬件加速功能在必须支持的算法基础上，尽可能多地支持其它抗量子算法；
2. 安全性，考虑侧信道攻击和故障注入攻击在硬件设计中的防护实现；
3. 性能，综合考虑支持算法种类、面积、所需存储空间、综合频率、算法运行时间等性能结果。

2.2 输出要求

1）书面报告，需要包括：
   a) 算法调研和实现方案说明；
   b) 数字电路设计实现说明；
   c) 仿真及测试结果；
   d) 硬件加速协处理器使用说明；
2）数字设计代码。
3）综合实现报告，包括：
   a) 面积；
   b) 时序；

2.3 加分要求

1）使用 procise 且提供使用报告；
2）调研中分析或提出优化算法；
3）其它额外且有意义的工作。

3 评分标准

总分 100 分，评分标准如下。

分类	项目	细则	分数
书面报告	总体	结构完整、内容和逻辑清晰，图文规范。	**5**
	调研	算法及优化调研全面，理解准确。	**5**
	设计	系统方案合理，描述清晰，重点明确。	**5**
		硬件加速模块设计合理，描述清晰。	**5**
	功能[1]	硬件加速功能正确，硬件可扩展性强	**15**
	安全性	脆弱性分析和有效安全防护措施	**10**
	性能[2]	面积	**10**
		存储空间	**10**
		综合频率	**10**
		执行时间	**10**
代码	风格	模块划分清晰	**3**
		注释丰富	**2**
综合报告	面积时序	面积合理，时序通过，不存在违例情况	**10**
加分项	工具试用	如使用 **procise** 且提供使用报告，在调研中分析提出某些优化算法，但是基于 **FPGA** 资源无法实现	**(10)**
合计			**100(110)**

4 赛事安排

4.1 参赛队伍要求

每支参赛队伍人数上限为 5 人, 在书面报告中需要注明每位参赛成员的分工(例如：算法方案、代码编写、功能验证等)

4.2 赛事流程

阶段	时间	内容
初赛阶段	3.20-6.30	各支队伍根据本赛道要求完成并提交相应设计和书面报告
公布名单	7.16	公布入围决赛队伍名单
决赛阶段	8.14-8.17	决赛暂定采用线上答辩形式
颁奖典礼	8.28	对获奖队伍颁发奖项