算法测试平台 - 性能测试报告

报告生成时间	2025-09-15 17:40:19
平台版本	1.0.0
测试环境	生产环境

测试基本信息

项目	值
算法名称	Kyber768
算法类别	密钥封装机制(KEM)
测试任务	Kyber768_性能测试_2025-09-15_17-39
测试次数	100
开始时间	2025-09-15 09:39:53
完成时间	2025-09-15 09:39:56
测试时长	3.18 秒
算法来源	liboqs
算法版本	1.0
算法描述	test2
任务状态	已完成

性能指标概览

指标名称	数值	单位	评价
平均密钥生成时间	0.7549	ms	优秀
平均封装时间	0.4458	ms	优秀
平均解封装时间	0.4563	ms	优秀
成功率	100.00	%	优秀
公钥大小	1184	bytes	良好
私钥大小	2400	bytes	良好
密文大小	1088	bytes	良好

测试环境信息

项目	信息
操作系统	Windows 10
处理器架构	AMD64
CPU核心数	12 核心
内存大小	15 GB
磁盘空间	189 GB
Python版本	3.9.13
测试模式	真实测试
平台版本	1.0.0
数据库类型	SQLite

平台状态信息

状态项	当前值	状态评价
系统运行时间	1 天 1 小时	正常
CPU使用率	0.8%	正常
内存使用率	71.1%	正常
磁盘使用率	67.3%	正常
可用内存	4 GB	充足
平台服务状态	运行中	正常
数据库连接	正常	正常
测试引擎状态	就绪	正常

详细统计信息

keygen_time 统计

统计项	数值
样本数量	100
平均值	0.7549
最小值	0.6005
最大值	0.8937
中位数	0.7612
标准差	0.0858

encaps_time 统计

统计项	数值
样本数量	100
平均值	0.4458
最小值	0.3619
最大值	0.5391
中位数	0.4490
标准差	0.0504

decaps_time 统计

统计项	数值
样本数量	100
平均值	0.4563
最小值	0.3629
最大值	0.5357
中位数	0.4588
标准差	0.0490

public_key_size 统计

统计项	数值
样本数量	1
平均值	1184.0000
最小值	1184.0000
最大值	1184.0000
中位数	1184.0000
标准差	0.0000

private_key_size 统计

统计项	数值
样本数量	1
平均值	2400.0000
最小值	2400.0000
最大值	2400.0000
中位数	2400.0000
标准差	0.0000

ciphertext_size 统计

统计项	数值
样本数量	1
平均值	1088.0000
最小值	1088.0000
最大值	1088.0000
中位数	1088.0000
标准差	0.0000

success_rate 统计

统计项	数值
样本数量	1
平均值	100.0000
最小值	100.0000
最大值	100.0000
中位数	100.0000
标准差	0.0000

性能分析和建议

基于测试结果的性能分析：

1. 算法性能评价：
□ 算法成功率表现优秀，稳定性良好
□ Keygen Time 性能优秀
□ Encaps Time 性能优秀
□ Decaps Time 性能优秀

2. 建议和优化方向：
□ 如需提升性能，可考虑算法参数优化
□ 建议在不同硬件环境下进行对比测试
□ 对于生产环境，建议进行更大规模的压力测试
□ 关注算法的内存使用效率和安全性

3. 测试环境说明：
□ 当前测试基于生产环境
□ 实际性能可能因硬件配置而有所差异
□ 建议定期进行性能基准测试

报告生成于: 2025-09-15 17:40:21
算法测试平台 - 后量子密码算法性能测试与验证平台