**OKCN-SEC：基于理想格RLWE的通用和**

**模块化的密钥协商协议**

**测试报告**

（Linux版）

2019年2月

**版本控制信息**

| 版本 | 日期 | 拟稿和修改 | 说明 |
| --- | --- | --- | --- |
| 1.0 | 2019-02-17 | 拟稿 | 文黎明，巩博儒 |
|  |  |  |  |

目 录

[第一章 概述 1](#_Toc9504090)

[1.1 测试目的 1](#_Toc9504091)

[1.2 测试对象及范围 1](#_Toc9504092)

[1.2.1 OKCN-SEC-RLWE-密钥生成 1](#_Toc9504093)

[1.2.2 OKCN-SEC-RLWE-密钥封装 1](#_Toc9504094)

[1.2.3 OKCN-SEC-RLWE-密钥解封装 2](#_Toc9504095)

[1.3 术语列表 2](#_Toc9504096)

[1.4 参考资料 2](#_Toc9504097)

[第二章 测试环境及说明 4](#_Toc9504098)

[2.1 测试环境物理拓扑结构 4](#_Toc9504099)

[2.2 硬件环境 4](#_Toc9504100)

[2.3 软件环境 4](#_Toc9504101)

[2.4 测试程序说明 4](#_Toc9504102)

[2.5 测试方法 6](#_Toc9504103)

[第三章 功能测试 9](#_Toc9504104)

[3.1 OKCN-SEC-RLWE-密钥生成-健壮性测试 9](#_Toc9504105)

[3.2 OKCN-SEC-RLWE-封装-健壮性测试 9](#_Toc9504106)

[3.3 OKCN-SEC-RLWE-解封装-健壮性测试 10](#_Toc9504107)

[3.4 OKCN-SEC-RLWE-正向功能验证 10](#_Toc9504108)

[3.5 OKCN-SEC-RLWE-反向功能验证 11](#_Toc9504109)

[3.6 OKCN-SEC-RLWE-完整功能中间结果展示 11](#_Toc9504110)

[第四章 性能测试 12](#_Toc9504111)

[4.1 时间性能 12](#_Toc9504112)

[4.1.1 OKCN-SEC-RLWE-密钥生成 12](#_Toc9504113)

[4.1.2 OKCN-SEC-RLWE-封装 13](#_Toc9504114)

[4.1.3 OKCN-SEC-RLWE-解封装 14](#_Toc9504115)

[4.2 时钟周期 15](#_Toc9504116)

[4.2.1 OKCN-SEC-RLWE-密钥生成 15](#_Toc9504117)

[4.2.2 OKCN-SEC-RLWE-封装 16](#_Toc9504118)

[4.2.3 OKCN-SEC-RLWE-解封装 17](#_Toc9504119)

[4.3 空间性能 18](#_Toc9504120)

[4.3.1 OKCN-SEC-RLWE算法的空间消耗 18](#_Toc9504121)

[第五章 测试总结 19](#_Toc9504122)

# 概述

## 测试目的

1. 基于理想格的密钥协商和密码封装机制算法的功能验证。

2. 基于理想格的密钥协商和密码封装机制算法的性能测试。

## 测试对象及范围

基于理想格的密钥协商算法程序实现包含 OKCN-SEC-RLWE。

本次测试针对这两部分算法进行功能验证和性能测试，具体包括：

1. 验证算法功能；

2. 测试算法的实现性能；

3. 给出测试平台上的存储需求。

算法各部分的API接口分别为：

### OKCN-SEC-RLWE-密钥生成

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

函数名 ：kem\_keygen

功能描述：基于OKCN-SEC-RLWE的密钥生成

输入参数：无

输出参数：pk -生成的公共密钥，1696字节

sk -生成的私有密钥，640字节

返回值 ：0-生成密钥成功

-1-内部处理错误

-2-接口参数错误

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

int kem\_keygen( unsigned char \*pk, unsigned char \*sk);

### OKCN-SEC-RLWE-密钥封装

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

函数名 ：kem\_enc

功能描述：基于OKCN-SEC-RLWE的密钥封装

输入参数：pk -接收方的公钥，1696字节

输出参数：ss -共享密钥，95字节

ct -密文，1955字节

返回值 ：0 -成功

-1-内部处理错误

-2-接口参数错误

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

int kem\_enc(unsigned char \* pk,unsigned char \* ss, unsigned char \* ct);

### OKCN-SEC-RLWE-密钥解封装

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

函数名 ：kem\_dec

功能描述：基于OKCN-SEC-RLWE的密钥解封装

输入参数：sk -接收方的私钥，640字节

ct -密文，1955字节

输出参数：ss -生成的共享密钥，95字节

返回值 ：0 -成功

-1-内部处理错误

-2-接口参数错误

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

int kem\_dec(unsigned char \* sk, unsigned char \* ct, unsigned char \* ss);

## 1.3 术语列表

本文中涉及的专业术语见表1.1：

表1.1 术语

|  |  |
| --- | --- |
| OKCN | 基于理想格的带噪音对称密钥共识算法。 |
| CPUCYCLE | CPU周期又称[机器周期](https://baike.baidu.com/item/%E6%9C%BA%E5%99%A8%E5%91%A8%E6%9C%9F/276831)，从内存读取一条[指令字](https://baike.baidu.com/item/%E6%8C%87%E4%BB%A4%E5%AD%97/3220363)的最短时间来定义，这个基准时间就是CPU周期（机器周期）。本文中除了使用时间来衡量算法性能，也给出了算法消耗的时钟周期。 |

## 1.4 参考资料

《算法文本-基于理想格RLWE的通用和模块化的密钥封装机制》

# 测试环境及说明

## 测试环境物理拓扑结构

仅单机

## 硬件环境

**设备类型**：微型计算机

**型号**：HP Pavilion Gaming Desktop PC

**CPU**：Intel® Core™ i7-8700 CPU @ 3.20GHz \*12

**内存**：RAM 8GB(1\*8GB) DDR4 2666 NECC

**硬盘**：HDD 1TB 7200RPM SATA 3.5 cDT 2nd

SSD 128G 2280 PCIe NVMe Value

**显卡**：GFX Nvd GeF GTX1060 6GB

## 软件环境

**操作系统**：Ubuntu 18.04.1 LTS

**开发语言**：C

**编译工具**：gcc version 7.3.0 (Ubuntu 7.3.0-27ubuntu1~18.04)

## 测试程序说明

测试程序的发布方式参照开源库通用方式，即在算法发布库中集成对应的测试验证程序。整个算法库的源码组织结构包含：

* okcn-sec子目录，包含了OKCN-SEC-RLWE算法实现及其测试程序；

因算法库依赖开源库openssl，在进行算法库和测试程序的编译前请先编译安装openssl。先从官网下载源码包，然后执行如下命令编译安装：

tar -zxvf openssl-1.1.0j.tar.gz

cd openssl-1.1.0j

sudo ./config

sudo make

sudo make install

测试程序含功能的验证和性能测试。测试程序与算法库一样均为c语言开发，具体编译方法如下(linux,gcc)：

获取算法源码tar包后执行如下命令即可：

tar -xvf rlwe.tar

cd rlwe/okcn-sec/ref

make clean all

编译生成的rlwe/okcn-sec/ref/libokcn.so即为OKCN-SEC-RLWE算法库文件。

编译生成的rlwe/okcn-sec/ref//testokcnkem即为OKCN-SEC-RLWE算法测试验证可执行程序。

所有测试程序均采用列表菜单方式提供不同项目的测试，使用时执行对应算法的测试程序即可进入测试菜单，菜单内容包括功能测试部分和交互式性能测试部分，图2.1为OKCN-SEC-RLWE算法测试验证可执行程序testokcnkem的测试界面：



图2.1 测试界面

选择对应菜单项并输入编号即可开始测试。

## 测试方法

1. 测试案例的组织分三个层次：a.算法的健壮性、稳定性验证；b.算法功能验证；c.算法性能测试。
2. 测试案例中对成功和失败的判断均指测试程序按指定逻辑返回特定的错误码。
3. 为获取性能测试准确数据，测试将对所有接口分别根据收敛情况进行不同数量级的重复测试以获取正确的统计结果。

4、各算法总体测试流程见图2.2。

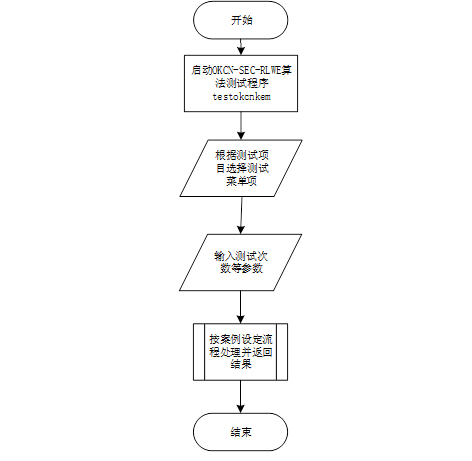


图2.2 总体测试流程图

基于理想格的密钥协商和密码封装机制算法的通用测试流程（含反向功能验证）见图2.3。



图2.3 基于理想格的密钥协商和密码封装机制算法通用测试流程图

性能测试流程即在通用测试流程基础上对算法库各API接口的时间和CPU周期消耗进行统计分析和比较。

# 功能测试

## OKCN-SEC-RLWE-密钥生成-健壮性测试

**案例编号：okcn-kem**-i001

**案例说明：**验证OKCN-SEC-RLWE的密钥生成接口在如下非法参数情况下的健壮性：

1. 公有密钥pk为NULL；
2. 私有密钥sk为NULL；
3. 公有密钥pk和私有密钥sk均为NULL；

操作流程及测试结果见表3.1。

**对应测试程序菜单项：**1

表3.1 OKCN-SEC-RLWE-密钥生成-健壮性测试

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **功能点** | **前提条件** | **操作流程** | 预期结果 | **是否符合预期** |
| OKCN-SEC-RLWE的密钥生成接口在非法参数情况下的健壮性 | 无 | 1. 调用算法库接口，并将输出参数公有密钥pk置为NULL。 2. 调用算法库接口，并将输出参数私有密钥sk置为NULL。 3. 调用算法库接口，并将输出参数公有密钥pk和私有密钥sk置为NULL。 | 算法库对非法参数调用均能做正确反馈（应答码等于-2），不会出现进程异常退出，如core dump的情况 | 是 |

**测试结论:** 测试通过

## OKCN-SEC-RLWE-封装-健壮性测试

**案例编号：okcn-kem**-i002

**案例说明：**验证OKCN-SEC-RLWE的封装接口在如下非法参数情况下的健壮性：

1. 公有密钥pk为NULL；
2. 共享密钥ss为NULL；
3. 密文ct为NULL；

操作流程及测试结果见表3.2。

**对应测试程序菜单项：**2

表3.2 OKCN-SEC-RLWE-封装-健壮性测试

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **功能点** | **前提条件** | **操作流程** | 预期结果 | **是否符合预期** |
| OKCN-SEC-RLWE的封装接口在非法参数情况下的健壮性 | 无 | 1. 调用算法库接口，并将输入参数公有密钥pk置为NULL。 2. 调用算法库接口，并将输出参数共享密钥ss置为NULL。 3. 调用算法库接口，并将输出参数密文ct置为NULL。 | 算法库对非法参数调用均能做正确反馈（应答码等于-2），不会出现进程异常退出，如core dump的情况 | 是 |

**测试结论:** 测试通过

## OKCN-SEC-RLWE-解封装-健壮性测试

**案例编号：okcn-kem**-i003

**案例说明：**验证OKCN-SEC-RLWE的解封装接口在如下非法参数情况下的健壮性：

1. 私有密钥sk为NULL；
2. 密文ct为NULL；
3. 共享密钥ss为NULL；

操作流程及测试结果见表3.3。

**对应测试程序菜单项：**3

表3.3 OKCN-SEC-RLWE-解封装-健壮性测试

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **功能点** | **前提条件** | **操作流程** | 预期结果 | **是否符合预期** |
| OKCN-SEC-RLWE的解封装接口在非法参数情况下的健壮性 | 无 | 1. 调用算法库接口，并将输入参数私有密钥pk置为NULL。 2. 调用算法库接口，并将输入参数密文ct置为NULL。 3. 调用算法库接口，并将输出参数共享密钥ss置为NULL。 | 算法库对非法参数调用均能做正确反馈（应答码等于-2），不会出现进程异常退出，如core dump的情况 | 是 |

**测试结论:** 测试通过

## OKCN-SEC-RLWE-正向功能验证

**案例编号：okcn-kem**-p001

**案例说明：**验证OKCN-SEC-RLWE能否实现发送方和接收方获取相同的共享密钥，如表3.4所示。

**对应测试程序菜单项：**4

表3.4 OKCN-SEC-RLWE-正向功能验证

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **功能点** | **前提条件** | **操作流程** | 预期结果 | **是否符合预期** |
| 验证OKCN-SEC-RLWE能否实现发送方和接收方获取相同的共享密钥 | 无 | 1. 调用算法库密钥生成接口，生成接收方的公钥和私钥。 2. 发送方调用算法库封装接口，使用接收方的公钥生成密文和共享密钥。 3. 接收方调用算法库解封装接口，使用自己的私钥和密文生成共享密钥。 4. 确认发送方和接收方的共享密钥是否一致，如一致则继续，否则返回验证失败。 5. 重复以上流程10000次 | 发送方和接收方的共享密钥一致 | 是 |

**测试结论:** 测试通过

## OKCN-SEC-RLWE-反向功能验证

**案例编号：okcn-kem**-p002

**案例说明：**确认OKCN-SEC-RLWE修改密文ct后接收方解封装是否返回错误，如表3.5所示。

**对应测试程序菜单项：**5

表3.5 OKCN-SEC-RLWE-反向功能验证

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **功能点** | **前提条件** | **操作流程** | 预期结果 | **是否符合预期** |
| 确认OKCN-SEC-RLWE修改密文ct后接收方解封装是否返回错误 | 无 | 1. 调用算法库密钥生成接口，生成发送方和接收方的公钥和私钥。 2. 发送方调用算法库封装接口，使用接收方的公钥生成密文和共享密钥。 3. 篡改密文。 4. 接收方调用算法库解封装接口，使用自己的私钥和篡改后的密文来生成共享密钥， 5. 比较双方的共享密钥，如不等则继续，否则返回验证失败。 6. 重复以上流程10000次 | 解封装时返回错误 | 是 |

**测试结论:** 测试通过

## OKCN-SEC-RLWE-完整功能中间结果展示

**案例编号：okcn**-kem-f001

**案例说明：**对OKCN-SEC-RLWE算法进行完整过程的测试并记录测试数据到当前目录下的okcn\_kem\_test\_result.txt文件。

**对应测试程序菜单项：**6

**测试结论：**

测试通过，相关测试数据见《OKCN-SEC-RLWE-功能测试数据记录.txt》

# 性能测试

性能测试包括时间性能、CPU时钟周期数据的测试及算法所需存储空间的分析。测试程序菜单包含了交互式性能测试选项，也可以通过执行对应测试程序时带参数t来启动算法的自动性能测试，此时测试数据将写入当前目录下的性能测试文件，自动性能测试的使用说明见表4.1。

表4.1 自动性能测试使用说明

|  |  |
| --- | --- |
| **命令** | **说明** |
| ./testokcnkem t | 启动OKCN-SEC算法自动性能测试， 测试数据记录到当前目录下的okcn\_kem\_test\_performance.txt文件中。 |
| ./testakcnkex t | 启动AKCN-SEC算法自动性能测试， 测试数据记录到当前目录下的akcn\_kex\_test\_performance.txt文件中。 |
| ./rlwe\_e8 t | 启动AKCN-E8算法自动性能测试， 测试数据记录到当前目录下的rlwe\_kem\_test\_performance.txt文件中。 |

## 时间性能

### OKCN-SEC-RLWE-密钥生成

案例编号：okcn-kem-pt01

案例说明：对OKCN-SEC-RLWE算法生成密钥的性能统计。

统计指标：耗时。

测试步骤：

**第一步：**数据准备：无。

**第二步：**按一次生成的密钥数分别是1、10、100、1000、10000、100000、1000000个的情况，对生成密钥统计总耗时和单次耗时，最终归纳出单次密钥生成耗时的收敛值。相关耗时的变化情况见表4.2：

表4.2 OKCN-SEC-RLWE-密钥生成耗时统计

|  |  |  |
| --- | --- | --- |
| **次数** | **总耗时(秒)** | **平均耗时(微秒)** |
| 1 | 0.000142 | 142 |
| 10 | 0.001332 | 133 |
| 100 | 0.010365 | 103 |
| 1000 | 0.098862 | 98 |
| 10000 | 0.968698 | 96 |
| 100000 | 9.637123 | 96 |
| 1000000 | 96.18613 | 96 |

OKCN-SEC-RLWE算法密钥生成平均耗时统计结果如图4.1所示。

图4.1 OKCN-SEC-RLWE-密钥生成平均耗时统计

**测试结论：**

在测试机上OKCN-SEC-RLWE算法的单次密钥生成平均耗时约为96微秒。

### OKCN-SEC-RLWE-封装

案例编号：okcn-kem-pt02

案例说明：测试OKCN-SEC-RLWE算法密钥封装的性能。

统计指标：耗时。

测试步骤：

**第一步：**数据准备：每次封装前先生成一组密钥。

**第二步：**按一次进行的密钥封装数分别是1、10、100、1000、10000、100000、1000000次的情况，对密钥封装统计总耗时和单次耗时，最终归纳出单次封装耗时的收敛值。相关耗时的变化情况如表4.3所示。

表4.3 OKCN-SEC-RLWE-密钥封装耗时统计

|  |  |  |
| --- | --- | --- |
| **次数** | **总耗时(秒)** | **平均耗时(微秒)** |
| 1 | 0.000215 | 215 |
| 10 | 0.002387 | 208 |
| 100 | 0.017769 | 177 |
| 1000 | 0.171272 | 171 |
| 10000 | 1.673209 | 167 |
| 100000 | 16.65867 | 166 |
| 1000000 | 166.2218 | 166 |

OKCN-SEC-RLWE算法密钥封装平均耗时统计结果如图4.2所示。

图4.2 OKCN-SEC-RLWE-密钥封装平均耗时统计

**测试结论：**

在测试机上OKCN-SEC-RLWE算法的单次封装平均耗时约为166微秒。

### OKCN-SEC-RLWE-解封装

案例编号：okcn-kem-pt03

案例说明：测试OKCN-SEC-RLWE算法密钥解封装的性能。

统计指标：耗时。

测试步骤：

**第一步：**数据准备：每次解封装前先生成一组封装数据。

**第二步：**按一次进行的密钥解封装数分别是1、10、100、1000、10000、100000、1000000次的情况，对密钥解封装统计总耗时和单次耗时，最终归纳出单次解封装耗时的收敛值。相关耗时的变化情况如表4.4所示：

表4.4 OKCN-SEC-RLWE-密钥解封耗时统计

|  |  |  |
| --- | --- | --- |
| **次数** | **总耗时(秒)** | **平均耗时(微秒)** |
| 1 | 0.000078 | 78 |
| 10 | 0.000722 | 72 |
| 100 | 0.005556 | 55 |
| 1000 | 0.053204 | 53 |
| 10000 | 0.5204 | 52 |
| 100000 | 5.180264 | 51 |
| 1000000 | 51.697119 | 51 |

OKCN-SEC-RLWE算法密钥解封装平均耗时统计结果如图4.3所示。

图4.3 OKCN-SEC-RLWE-密钥解封平均耗时统计

**测试结论：**

在测试机上OKCN-SEC-RLWE算法的单次解封装平均耗时约为51微秒。

## 时钟周期

### OKCN-SEC-RLWE-密钥生成

案例编号：okcn-kem-pc01

案例说明：对OKCN-SEC-RLWE算法生成密钥的性能统计。

统计指标：cpu周期。

测试步骤：

**第一步：**数据准备：无。

**第二步：**按一次生成的密钥数分别是1、10、100、1000、10000、100000、1000000个的情况，对生成密钥统计消耗的总的CPU周期和单次CPU周期，最终归纳出单次生成密钥CPU周期消耗的收敛值。相关消耗的变化情况如表4.11所示。

表4.11 OKCN-SEC-RLWE-密钥生成消耗cpu周期统计

|  |  |  |
| --- | --- | --- |
| **次数** | **总耗费cpu周期** | **平均消耗cpu周期** |
| 1 | 308751 | 308751 |
| 10 | 3069484 | 306948 |
| 100 | 30900557 | 309005 |
| 1000 | 307350782 | 307350 |
| 10000 | 3070412685 | 307041 |
| 100000 | 30722946157 | 307229 |
| 1000000 | 307327826473 | 307327 |

OKCN-SEC-RLWE算法密钥生成平均消耗CPU周期统计结果如图4.10所示。

图4.10 OKCN-SEC-RLWE-密钥生成平均消耗cpu周期数

**测试结论：**

在测试机上OKCN-SEC-RLWE算法的单次密钥生成平均CPU周期约为307000。

### OKCN-SEC-RLWE-封装

案例编号：okcn-kem-pc02

案例说明：测试OKCN-SEC-RLWE算法密钥封装的性能。

统计指标：cpu周期。

测试步骤：

**第一步：**数据准备：每次封装前先生成一组密钥。

**第二步：**按一次密钥封装数分别是1、10、100、1000、10000、100000、1000000个的情况，对密钥封装统计消耗的总的CPU周期和单次CPU周期，最终归纳出单次密钥封装CPU周期消耗的收敛值。相关消耗的变化情况如表4.12所示。

表4.12 OKCN-SEC-RLWE-密钥封装消耗cpu周期统计

|  |  |  |
| --- | --- | --- |
| **次数** | **总耗费cpu周期** | **平均消耗cpu周期** |
| 1 | 527367 | 527367 |
| 10 | 5295805 | 529580 |
| 100 | 53101439 | 531014 |
| 1000 | 530849205 | 530849 |
| 10000 | 5299099332 | 529909 |
| 100000 | 53021800416 | 530218 |
| 1000000 | 530363425956 | 530363 |

图4.11是OKCN-SEC-RLWE算法密钥封装CPU周期消耗收敛统计结果。

图4.11 OKCN-SEC-RLWE-封装平均消耗cpu周期统计

**测试结论：**

在测试机上OKCN-SEC-RLWE算法的单次封装平均CPU周期约为530000。

### OKCN-SEC-RLWE-解封装

案例编号：okcn-kem-pc03

案例说明：测试OKCN-SEC-RLWE算法密钥解封装的性能。

统计指标：cpu周期。

测试步骤：

**第一步：**数据准备：每次解封装前先生成一组封装数据。

**第二步：**按一次密钥解封装数分别是1、10、100、1000、10000、100000、1000000个的情况，对密钥解封装统计消耗的总的CPU周期和单次CPU周期，最终归纳出单次密钥解封装CPU周期消耗的收敛值。相关消耗的变化情况如表4.13所示。

表4.13 OKCN-SEC-RLWE-解封装消耗cpu周期统计

|  |  |  |
| --- | --- | --- |
| **次数** | **总耗费cpu周期** | **平均消耗cpu周期** |
| 1 | 165245 | 165245 |
| 10 | 1744297 | 174429 |
| 100 | 16455340 | 164553 |
| 1000 | 164617545 | 164617 |
| 10000 | 1645456935 | 164545 |
| 100000 | 16461915617 | 164619 |
| 1000000 | 164634345600 | 164634 |

图4.12是OKCN-SEC-RLWE算法密钥解封装CPU周期平均消耗统计结果。

图4.12 OKCN-SEC-RLWE-解封装平均消耗cpu周期统计

**测试结论：**

在测试机上OKCN-SEC-RLWE算法的单次解封装平均CPU周期约为164600。

## 空间性能

下面我们将针对OKCN-SEC-RLWE、AKCN-SEC-RLWE和AKCN-E8-RLWE三种算法实现给出空间性能分析。

### OKCN-SEC-RLWE算法的空间消耗

在表4.20中我们给出了OKCN-SEC-RLWE算法主要参数一览。

表4.20 OKCN-SEC-RLWE算法主要参数所耗空间一览表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **名称** | **公钥 pk** | **私钥 sk** | **密文ct** | **共享秘密ss** |
| 长度(byte) | 1696 | 640 | 1955 | 95 |

对于具体API接口，针对大赛要求实现的kem\_api，一次密钥封装完整过程包括密钥生成函数（kem\_keygen）， 封装函数（kem\_enc）和解封装函数（kem\_dec）。表4.21给出了这三个函数输入输出参数所需要的空间 并对各个参数进行了简要的介绍。

表4.21 OKCN-SEC-RLWE算法各个接口参数空间性能

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **函数** | **输入** | **长度(byte)** | **含义** | **输出** | **长度(byte)** | **含义** |
| kem\_keygen |  | | | pk | 1696 | 用户公钥 |
| sk | 640 | 用户私钥 |
| kem\_enc | pk | 1696 | 接收方公钥 | ct | 1955 | 密文 |
| ss | 95 | 共享秘密 |
| kem\_dec | ct | 1955 | 密文 | ss | 95 | 共享秘密 |
| sk | 640 | 接收方私钥 |

# 测试总结

1. 算法库各API对异常参数均能正常处理。
2. 验证了OKCN-SEC-RLWE算法在正常流程下实现双方获取共享密钥的功能。
3. 验证了OKCN-SEC-RLWE算法在传输时被篡改密文后解封装应报错的功能。
4. 对OKCN-SEC-RLWE算法进行了完整过程功能验证。
5. 各算法API实现的单次平均耗时收敛值如表5.1所示（性能测试数据详见具体案例）。

表5.1 各算法API实现的性能统计表

|  |  |  |  |
| --- | --- | --- | --- |
| **算法名** | **接口名** | **平均耗时（微秒）** | **平均CPU周期消耗** |
| OKCN-SEC-RLWE | 密钥生成 | 96 | 307000 |
| 封装 | 166 | 530000 |
| 解封装 | 51 | 164600 |