

# AKCN-MLWE：基于模格 MLWE 的通用和模块化的密钥封装机制

对于 基于 MLWE 的通用和模块化的密钥封装协议， 我们给出了 AKCN-MLWE-KT-Recommended 和 AKCN-MLWE-PKE-Recommended 算法程序 在 Windows 和 Linux 系统下的实现， 实现代码保存在 参考实现\MLWE-KEM 文件夹中。 下面我们针对基于 MLWE 的通用和模块化的密钥封装协议 算法程序的安装方法和目录结构进行介绍。

## Windows 版本程序 及目录结构

---

Windows 版本程序 为 mlwe-kem-win.zip，解压缩后进入 mlwe-kem-win 文件夹

### 测试程序文件结构说明

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分为两部分，分别是：

- AKCN-MLWE-KT 子目录，包含了 AKCN-MLWE-KT-Recommended 算法实现及其测试程序；
- AKCN-MLWE-PKE 子目录，包含了 AKCN-MLWE-PKE-Recommended 算法实现及其测试程序；

使用 vs2010 打开 MLWE.sln。然后编译所有过程，会在 build 目录下生成两个可执行程序，分别是 AKCN-MLWE-KT.exe、AKCN-MLWE-PKE.exe。 所有测试程序均采用列表菜单方式提供不同项目的测试，使用时双击对应的可执行文件即可进入测试菜单。

### 代码文件

- kem\_test.c 功能测试代码
- kem\_benchmark.c 基准性能测试代码
- test.h 测试文件头文件

### 安装

请先安装 vs2010,进行目录，双击 MLWE 自动打开工程。

### 依赖

本库依赖 openssl 库，请至官网下载最新 32 位版本。

## 辅助脚本

- run\_benchmark.bat 执行基准性能测试。
- run\_case.bat 生成测试案例文件
- report.sh 协助抽取基准测试的日志数据，生成报告文件,依赖于 Linux 环境。

## 可执行文件

可执行程序位于 build 目录下，主要有以下两个可执行程序 - AKCN-MLWE-KT.exe  
AKCN-MLWE-KT 算法测试程序 - AKCN-MLWE-PKE.exe AKCN-MLWE-PKE 算法测试程序

## Linux 版本程序 及目录结构

---

Linux 版本程序 为 mlwe-kem-linux.tar，解压缩后进入 mlwe-kem-linux 文件夹

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分为两部分，分别是：

- AKCN-MLWE-KT 子目录，包含了 AKCN-MLWE-KT-Recommended 算法实现及其测试程序；
- AKCN-MLWE-PKE 子目录，包含了 AKCN-MLWE-PKE-Recommended 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 mlwe-kem-linux.tar
- ./makeall.sh

编译生成以下两个可执行程序

- ./AKCN-MLWE-PKE/kem\_test
- ./AKCN-MLWE-KT/kem\_test

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。

## 代码文件

- `kem_test.c` 功能测试代码
- `kem_benchmark.c` 基准性能测试代码
- `test.h` 测试文件头文件

## 辅助脚本

- `run_benchmark.sh` 执行基准性能测试。
- `run_case.sh` 生成测试案例的脚本
- `report.sh` 协助抽取基准测试的日志数据，生成报告文件。

## 安装

进行目录下执行 `makeall.sh`，可执行文件 `kex_test` 分别生成于子目录 `AKCN-MLWE-KT`、`AKCN-MLWE-PKE` 下。

```
./makeall.sh
```

## 依赖

本库依赖 `openssl` 库，请至官网下载最新 32 位版本。

## 可执行文件

可执行程序位于 `build` 目录下，主要有以下两个可执行程序

- `AKCN-MLWE-KT/kex_test` `AKCN-MLWE-KT` 算法测试程序
- `AKCN-MLWE-PKE/kex_test` `AKCN-MLWE-PKE` 算法测试程序