

OKCN-SEC：基于理想格 RLWE 的通用和模块化的密钥协商协议

算法实现代码在“参考实现文件夹”下。具体来说我们 针对基于理想格的 OKCN-SEC 密钥封装算法给出了软件实现。 针对以上实现， 我们又分别给出了 Windows 和 Linux 系统下的软件实现。 下面我们给出 不同系统下的安装部署和目录及文件结构的说明。

Windows 软件实现 安装部署说明

算法库组成

整个算法库实现在 `rlwe` 解决方案中：

1.rlwe 解决方案

`rlwe` 解决方案打包在 `rlwe-win.zip` 文件中，解压后的得到 `rlwe` 文件夹。 `rlwe` 解决方案给出了 AKCN-SEC 密钥封装算法 和 OKCN-SEC 密钥封装算法的实现。 整个算法库的解决方案名为 `rlwe`，其中包含 4 个项目，分别是：

- `libokcn`，包含了 OKCN-SEC-RLWE 算法实现；
- `testokcnkem`，包含了 OKCN-SEC-RLWE 算法的测试程序；

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基于 `visual studio 2010 pro` 开发工具使用 `c` 语言开发。 因代码涉及对 `openssl` 库的调用，为简化编译流程， 在工程代码的 `x64\release` 目录下已集成了编译好的 `openssl` 库文件（`libcrypto-1_1-x64.dll`）。编译时使用 `visual studio 2010pro` 打开相应目录下的算法解决方案后先编译算法库再编译算法测试程序。

安装运行说明

- 对 `rlwe` 解决方案，可以看到里面包含 2 个项目，分别是算法库 `libokcn`，算法测试程序 `testokcnkem`。 在 `rlwe-win\rlwe\x64\Release` 文件夹下， 编译生成的 `libakcn.lib` 和 `libokcn.lib` 即为算法库， `testakcnkem.exe` 和 `testokcnkem.exe` 即为算法测试程序。

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。

Linux 软件实现 安装部署说明

算法库组成

Linux 软件实现 软件实现 打包在 `rlwe.tar` 文件中，解压后的得到 `rlwe` 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如下：

- `okcn-sec` 子目录，包含了 OKCN-SEC-RLWE 密钥封装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`

安装运行说明

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`

完成以上命令后：

- 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。