分布式计算大作业报告

1．项目信息

选题：

Project #1：Cloud Backup (Secure Cloud Backup)

成员信息：

张明锐　1110379057
吴通　1110379054
李梦萍　1110379071

项目名称：

SecBox

项目简介：

基于新浪微盘开放 API 实现苹果 Cocoa 平台与跨系统 Java 平台的加密云备份文件系统。

系统架构：

服务端我们使用新浪微盘。微盘的开放 API 可以很好地进行整合。我们使用了 API 中的获得 token、保持 token、获得容量、获得列表、获得文件信息、删除文件、上传文件、重命名文件。

客户端我们同时覆盖 Mac OS/Linux/Windows 三个主流操作系统。Mac 版基于 Cocoa 平台采用 Objective-C 语言编写，提供详细的命令行交互界面。Linux 与 Windows 版使用 Java 编写，提供简单的图形用户界面。

文件加密算法我们选用工业上成熟的 AES128 位算法，同时加密文件的内容与元数据（meta data）（路径信息等）。

项目进度：

现已经按《提案》与《详细设计》中制定的计划，完成了程序的开发、测试，并完成项目文档。

版本控制：

GitHub：https://github.com/ming-rui/SecBox（源代码完全公开）

应用的技术：

AES128、Base64、SHA256、MD5、Cocoa、Objective-C、Java、json

开发工具：

XCode、Eclipse、Git

开源项目的使用：

google-toolbox-for-mac：Google 的开源项目，我们使用了其中的 Base64 算法实现；

json-framework：Cocoa 平台的 json 实现；

CommonCrypto：苹果公司的开源数据加密项目；

2．项目关键技术介绍

数据加密

我们使用了标准的 AES128 作为我们的数据加密的算法。

文件信息映射

文件内容的映射是简单的，普通文件的内容经过上文提到的算法直接加密变成远程文件的内容，文件内容长度没有显著变化。我们把虚拟文件系统中文件的元数据（拥有者、路径）通过以下的方式映射成微盘文件的文件名：

微盘上文件的文件名 = “**[**SecBox**][**文件拥有者**][**文件路径的加密**]**”

其中的“SecBox”作为被 SecBox 系统所管理的文件的标志，用于过滤用户通过其他途径上传的文件；“文件拥有者”为明文的文件拥有者的系统用户名，用于过滤系统同一网盘上不同用户的文件；最重要的是“文件路径的加密”，它以加密的方式记录了文件在虚拟文件系统中的路径，而其加密/解密算法如下：

未加密的路径 $\xleftrightarrow{\text{AES128}}$ 中间数据 $\xleftrightarrow{\text{base64（web safe 版）}}$ 加密的路径

其中必须使用 base64 进行二次编码是为了产生合法的文件名（被这个版本的 base64 [1]编码过后的数据只包括字母、数字、“-”和“_”）。下面是一个例子：

未加密路径：“musics/country_music/carry.mp3”，用户名：“mingrui”，密码“mingrui”
加密的文件名“[SecBox][mingrui][9BVREfGtlRKHBAxM4vTPnqHQwVuVN-5rzn8_32ztGDw=]”

由于使用了这个策略来保存文件的路径信息，必然会使得微盘上文件的文件名很长。已知微盘文件名长度限制为 255，经过计算可以得知加密前的路径必须小于等于 170。

文件同步（备份）逻辑

需要提供的数据包括：上一次同步时文件的 MD5 计算 lastMd5、现在本地文件的 MD5 计算 localMd5、现在远程文件的 MD5 计算 remoteMd5、文件同步的冲突处理参数（同步/上传覆盖/下载覆盖/跳过）。则：

操作	条件（或）
无需操作	跳过 本地文件存在&远程文件存在&localMd5==remoteMd5 本地文件不存在&远程文件不存在
上传	本地文件存在&远程文件存在&上传覆盖 本地文件存在&远程文件存在&同步&lastMd5==remoteMd5

	本地文件存在&远程文件不存在
下载	本地文件存在&远程文件存在&下载覆盖 本地文件存在&远程文件存在&同步&lastMd5==localMd5 本地文件不存在&远程文件存在
提示用户处理	本地文件存在&远程文件存在&同步&（lastMd5、remoteMd5、localMd5 互不相等）

系统功能分解

我们把系统分为五大块：算法、配置系统、虚拟文件系统、新浪微盘驱动、文件同步系统。

系统	类	说明	类接口
算法	SBoxAlgorithms	封装各种算法。	+ encrypt + decrypt + base64wsEncode + base64wsDecode + hmacSHA256 + md5 + descriptionWithNumberOfBytes
配置系统	SBoxConfigs	负责保存程序数据。	- accountType - accountUserName - accountPassword - accountToken - currentRemotePath - encryptionUserName - encryptionPassword - pairs + sharedConfigs - save
虚拟文件系统	SBFSNode	文件和目录的索引节点（index-node）。	- type - isDirectory - isFile - name - path - itemInfo + fileNode + dirNode - childNode - addChildNode - removeChildNode - removeAllChildNodes - allChildNodes - numOfChildNodes
	SBFSTree	索引节点组成的目录树，主	- addFileNode

		要负责目录结构的管理和路径到节点的转换。	- getNode - getDirNode - getFileNode - removeAllData
	SBoxFileSystem	虚拟文件系统，同时管理一个 SBFSTree 目录树和 VDiskManager 新浪微盘驱动，负责两者之间数据的同步、目录树数据的缓存，并且对外提供封装好的接口。	+ sharedSystem - userName - currentPath - setAccountInfo - setEncrytionInfo - saveConfigs - absolutePath - fileMd5InRemote - getFileNode - getNodesInCurrentDirectory - changeDirectory - removeFile - moveFile - putFile - getFile
新浪微盘驱动	VDiskItemInfo	新浪微盘索引节点数据的封装。可以表示文件，也可以表示文件夹，并且文件还分为通过列表 API 和通过信息 API 两种格式。itemID、name 、 creationDate 和 lastModificationDate 域是两种文件和目录都具有的，其他的域不一定。还有些域经过分析系统没有使用。	- itemID - name - creationDate - lastModificationDate - isFile - isDirectory - fileSize - fileType - fileMd5 - fileURL + itemInfo
	VDiskManager	新浪微盘驱动，可以通过上文介绍的 API 登陆系统并增、删、查、改微盘根目录的文件（我们的系统只使用了根目录），提供封装好的接口，并作必要的数据缓存。原则上 VDiskManager 只允许 SBoxFileSystem 访问，不暴露接口给其他类（getQuota 例外）。	- delegate - accountType - userName - password - token + manager - keepTokenAndSync - getQuota - getRootFileList - getRootFileInfo - removeRootFile - renameRootFile - uploadFileToRoot - downloadFileFromRoot

文件同步系统	SBSSPair	本地文件和远程文件的一对映射、同步信息。	- localPath - remotePath - lastMd5 + pair
	SBoxSyncSystem	文件同步系统。实现“本地-远程文件对”信息的管理，并调用 SBoxFileSystem 执行同步操作。对外提供添加、删除文件对的接口，并且提供类似于迭代器的文件同步接口。	+ sharedSystem - saveConfigs - allPairs - addMap - removeMap - initSync - syncOne - stillCanSync

3．程序截图

Mac 版命令行记录：

```
Mini:SecBoxTest zimmer$ ./secbox help
Examples:
        secbox help : show help
        secbox status : show status
        secbox setacc : set vdisk account
        secbox setenc : set encryption
        secbox ls : list current remote directory
        secbox cd <path> : change current remote directory
        secbox put <local path> <remote path> : put local file to remote
        secbox get <remote path> <local path> : get remote file to local
        secbox rm <remote path> : remove remote file
        secbox mv <remote path 1> <remote path 2> : move remote file
        secbox addmap <local path> <remote path> : map local file with remote
        secbox rmmap <local path> : remove map
        secbox sync : sync files based on the map
Operation Completed.
Mini:SecBoxTest zimmer$ ./secbox status
Status:
 Account Type: weipan, User Name: mingrui.net@gmail.com;
 Encryption User Name: mingrui;
 Server Used:    11.2 MB, Server Total:     2.0 GB.
1 map records for syncronization:
 </Users/zimmer/SecBoxTest/t.jpg, /t.jpg>
Operation Completed.
Mini:SecBoxTest zimmer$ ./secbox setacc
Set Account Type(weibo or weipan):weipan
Set Account User Name:mingrui.net@gmail.com
```

```
Set Account Password:
Operation Completed.
Mini:SecBoxTest zimmer$ ./secbox setenc
Set Encryption User Name:mingrui
Set Encryption Password:
Operation Completed.
Mini:SecBoxTest zimmer$ ./secbox ls
15 items in "/":
 2012-05-24 21:04:23                5.4 MB       Carry You Home.mp3
 2012-05-24 23:43:31              118.6 KB       dtb.jpg
 2012-05-22 08:11:36               16.0 B        file1
 2012-05-22 08:17:31               16.0 B        file3
 2012-05-22 08:17:34               16.0 B        file5
 2012-05-24 23:36:14              298.6 KB       lady.jpg
 2012-05-24 20:30:56              103.7 KB       s.jpg
 2012-05-24 05:09:40              103.7 KB       sync.jpg
  --                     <DIR>                   syncFolder
 2012-05-24 23:45:19              298.6 KB       t.jpg
  --                     <DIR>                   test
 2012-05-23 00:10:23              298.6 KB       test2.jpg
  --                     <DIR>                   ttttttt
Operation Completed.
Mini:SecBoxTest zimmer$ ./secbox cd test
current path: "/test"
Operation Completed.
Mini:SecBoxTest zimmer$ ./secbox ls
4 items in "/test":
 2012-05-22 08:17:35               16.0 B        file1
 2012-05-22 08:17:36               16.0 B        file2
 2012-05-22 08:17:38               16.0 B        file3
  --                     <DIR>                   test
Operation Completed.
Mini:SecBoxTest zimmer$ ./secbox cd ../
current path: "/"
Operation Completed.
Mini:SecBoxTest zimmer$ ./secbox ls
15 items in "/":
 2012-05-24 21:04:23                5.4 MB       Carry You Home.mp3
 2012-05-24 23:43:31              118.6 KB       dtb.jpg
 2012-05-22 08:11:36               16.0 B        file1
 2012-05-22 08:17:31               16.0 B        file3
 2012-05-22 08:17:34               16.0 B        file5
 2012-05-24 23:36:14              298.6 KB       lady.jpg
 2012-05-24 20:30:56              103.7 KB       s.jpg
```

```
 2012-05-24 05:09:40                 103.7 KB        sync.jpg
  --                        <DIR>                    syncFolder
 2012-05-24 23:45:19                 298.6 KB        t.jpg
  --                        <DIR>                    test
 2012-05-23 00:10:23                 298.6 KB        test2.jpg
  --                        <DIR>                    ttttttt
Operation Completed.
Mini:SecBoxTest zimmer$ ls
Carry You Home.mp3                lady.jpg
Carry.mp3                         secbox
dtb.jpg                           sync.jpg
install_flash_player_osx.dmg      t.jpg
Mini:SecBoxTest zimmer$ ./secbox put Carry.mp3 Carry.mp3
Operation Completed.
Mini:SecBoxTest zimmer$ ./secbox ls
16 items in "/":
 2012-05-24 21:04:23                   5.4 MB        Carry You Home.mp3
 2012-05-25 03:24:54                   5.4 MB        Carry.mp3
 2012-05-24 23:43:31                 118.6 KB        dtb.jpg
 2012-05-22 08:11:36                  16.0 B         file1
 2012-05-22 08:17:31                  16.0 B         file3
 2012-05-22 08:17:34                  16.0 B         file5
 2012-05-24 23:36:14                 298.6 KB        lady.jpg
 2012-05-24 20:30:56                 103.7 KB        s.jpg
 2012-05-24 05:09:40                 103.7 KB        sync.jpg
  --                        <DIR>                    syncFolder
 2012-05-24 23:45:19                 298.6 KB        t.jpg
  --                        <DIR>                    test
 2012-05-23 00:10:23                 298.6 KB        test2.jpg
  --                        <DIR>                    ttttttt
Operation Completed.
Mini:SecBoxTest zimmer$ ./secbox get t.jpg t.jpg
Operation Completed.
Mini:SecBoxTest zimmer$ ls
Carry You Home.mp3                lady.jpg
Carry.mp3                         secbox
dtb.jpg                           sync.jpg
install_flash_player_osx.dmg      t.jpg
Mini:SecBoxTest zimmer$ ./secbox rm Carry.mp3
Operation Completed.
Mini:SecBoxTest zimmer$ ./secbox ls
15 items in "/":
 2012-05-24 21:04:23                   5.4 MB        Carry You Home.mp3
 2012-05-24 23:43:31                 118.6 KB        dtb.jpg
```

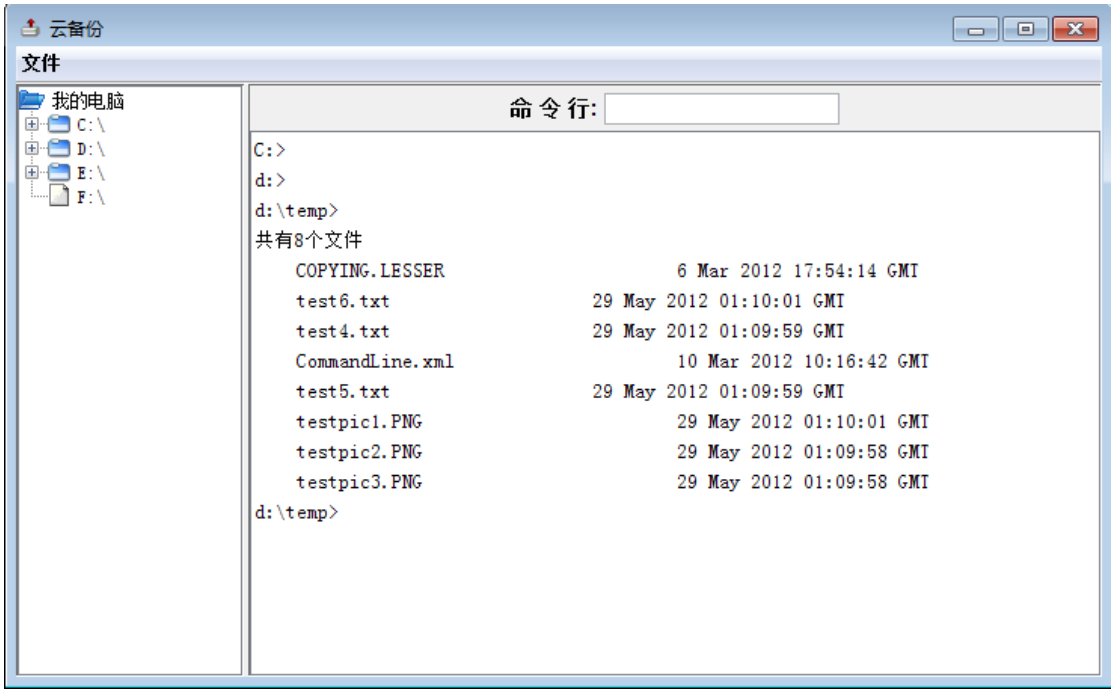
```
 2012-05-22 08:11:36                16.0 B         file1
 2012-05-22 08:17:31                16.0 B         file3
 2012-05-22 08:17:34                16.0 B         file5
 2012-05-24 23:36:14               298.6 KB        lady.jpg
 2012-05-24 20:30:56               103.7 KB        s.jpg
 2012-05-24 05:09:40               103.7 KB        sync.jpg
  --                     <DIR>                     syncFolder
 2012-05-24 23:45:19               298.6 KB        t.jpg
  --                     <DIR>                     test
 2012-05-23 00:10:23               298.6 KB        test2.jpg
  --                     <DIR>                     ttttttt
Operation Completed.
Mini:SecBoxTest zimmer$ ./secbox mv file5 test/file5
Operation Completed.
Mini:SecBoxTest zimmer$ ./secbox cd test
current path: "/test"
Operation Completed.
Mini:SecBoxTest zimmer$ ./secbox ls
5 items in "/test":
 2012-05-22 08:17:35                16.0 B         file1
 2012-05-22 08:17:36                16.0 B         file2
 2012-05-22 08:17:38                16.0 B         file3
 2012-05-25 03:27:23                16.0 B         file5
  --                     <DIR>                     test
Operation Completed.
Mini:SecBoxTest zimmer$ ls
Carry You Home.mp3                lady.jpg
Carry.mp3                         secbox
dtb.jpg                           sync.jpg
install_flash_player_osx.dmg      t.jpg
Mini:SecBoxTest zimmer$ ./secbox addmap file1-local file1
Operation Completed.
Mini:SecBoxTest zimmer$ ./secbox sync
File "/Users/zimmer/SecBoxTest/file1-local" is downloaded.
File "/Users/zimmer/SecBoxTest/t.jpg" is ok.
Operation Completed.
Mini:SecBoxTest zimmer$ ls
Carry You Home.mp3                lady.jpg
Carry.mp3                         secbox
dtb.jpg                           sync.jpg
file1-local                       t.jpg
install_flash_player_osx.dmg
Mini:SecBoxTest zimmer$ ./secbox rmmap file1-local
Operation Completed.
```

```
Mini:SecBoxTest zimmer$ ./secbox sync
File "/Users/zimmer/SecBoxTest/t.jpg" is ok.
Operation Completed.
Mini:SecBoxTest zimmer$
```

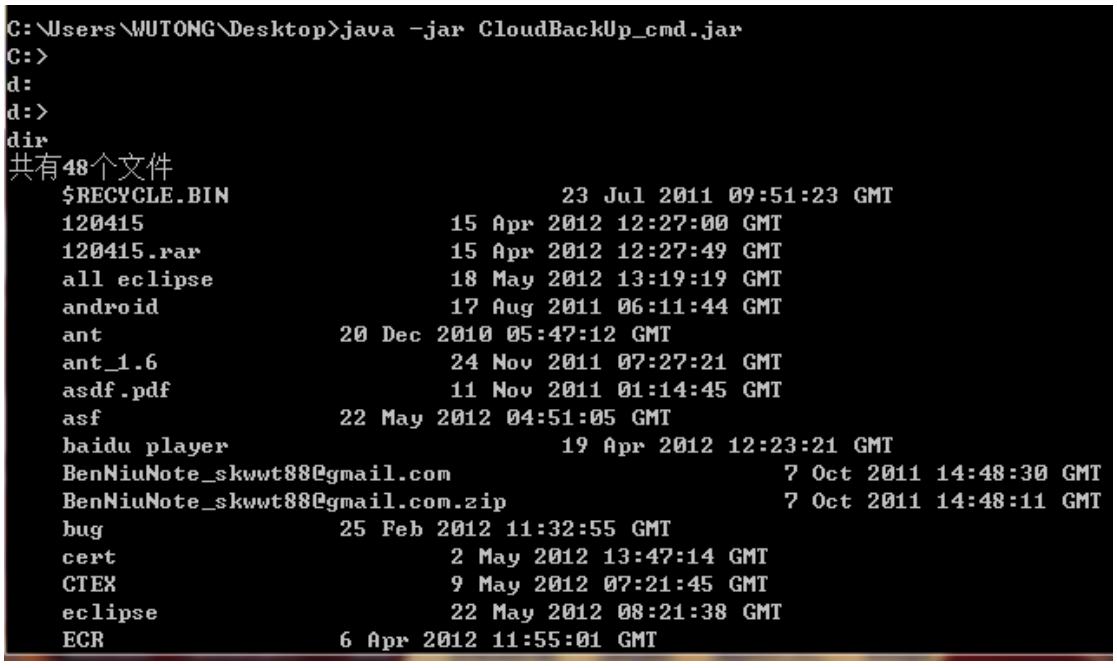
Java 版用户界面

1. Java 版提供了两种控制台下的界面和窗口界面，下面是运行截图：

   Gui 截图：



   命令行截图：



2. 命令说明：

   cd: 转换当前目录位置。

dir: 列出当前路径下文件列表

del: 删除文件，仅删除本地文件，不删除云端文件

del –cloud: 删除文件，本地云端都删除

update: 和云端同步，把云端的文件和本地的进行同步。

update –cloud: 使用云端文件覆盖本地文件，本地原有文件会被删除。

update –client: 使用本地文件覆盖云端文件，云端原有文件会被删除。

exit: 退出系统。

3. Java 版命令行记录

```
C:\Users\WUTONG\Desktop>java -jar CloudBackUp_cmd.jar
C:>
d:
d:>
cd temp
d:\temp>
dir
共有 9 个文件
    test1.txt                   28 May 2012 13:29:29 GMT
    test2.txt                   28 May 2012 12:55:45 GMT
    test3.txt                   28 May 2012 12:55:45 GMT
    test4.txt                   28 May 2012 12:55:45 GMT
    test5.txt                   28 May 2012 12:55:45 GMT
    test6.txt                   28 May 2012 12:55:45 GMT
    testpic1.PNG                        17 Sep 2011 05:54:11 GMT
    testpic2.PNG                        17 Sep 2011 05:54:11 GMT
    testpic3.PNG                        17 Sep 2011 05:54:11 GMT
d:\temp>
update
同步完成
d:\temp>
del test1.txt
文件删除成功!
d:\temp>
dir
共有 8 个文件
    test2.txt                   28 May 2012 12:55:45 GMT
    test3.txt                   28 May 2012 12:55:45 GMT
    test4.txt                   28 May 2012 12:55:45 GMT
    test5.txt                   28 May 2012 12:55:45 GMT
    test6.txt                   28 May 2012 12:55:45 GMT
    testpic1.PNG                        17 Sep 2011 05:54:11 GMT
    testpic2.PNG                        17 Sep 2011 05:54:11 GMT
    testpic3.PNG                        17 Sep 2011 05:54:11 GMT
d:\temp>
update
```

下载文件　d:\temp\test1.txt
同步完成
d:\temp>
dir
共有 9 个文件
test1.txt　28 May 2012 13:33:11 GMT
test2.txt　28 May 2012 12:55:45 GMT
test3.txt　28 May 2012 12:55:45 GMT
test4.txt　28 May 2012 12:55:45 GMT
test5.txt　28 May 2012 12:55:45 GMT
test6.txt　28 May 2012 12:55:45 GMT
testpic1.PNG　17 Sep 2011 05:54:11 GMT
testpic2.PNG　17 Sep 2011 05:54:11 GMT
testpic3.PNG　17 Sep 2011 05:54:11 GMT
d:\temp>
del -cloud test1.txt
文件删除成功!
d:\temp>
update
同步完成
d:\temp>
dir
共有 8 个文件
test2.txt　28 May 2012 12:55:45 GMT
test3.txt　28 May 2012 12:55:45 GMT
test4.txt　28 May 2012 12:55:45 GMT
test5.txt　28 May 2012 12:55:45 GMT
test6.txt　28 May 2012 12:55:45 GMT
testpic1.PNG　17 Sep 2011 05:54:11 GMT
testpic2.PNG　17 Sep 2011 05:54:11 GMT
testpic3.PNG　17 Sep 2011 05:54:11 GMT
d:\temp>
del test2.txt
文件删除成功!
d:\temp>
update -client
删除文件　[SecBox][wutong][542Js3N1te65BYqyPaL2RyMCDGCltIsmgHErvJLlpgQ=]。。。
删除文件　[SecBox][wutong][QA-QCMXNIyC0lwcGnR9uDS4oukLDFZ1qKdWkuIO2LXs=]。。。
删除文件　[SecBox][wutong][TjvLL97i-aCOweMfCj37Zy4oukLDFZ1qKdWkuIO2LXs=]。。。
删除文件　[SecBox][wutong][u-j77CJRPjnIfuPUyV5umSMCDGCltIsmgHErvJLlpgQ=]。。。
删除文件　[SecBox][wutong][Y-lvl5gxhoa9HwQLZtBjeSMCDGCltIsmgHErvJLlpgQ=]。。。
删除文件　[SecBox][wutong][mXvRCm4FSZpwYDgGD8gvXi4oukLDFZ1qKdWkuIO2LXs=]。。。
删除文件　[SecBox][wutong][q_t1tnQEADbcKdzRIEeYcSMCDGCltIsmgHErvJLlpgQ=]。。。
删除文件　[SecBox][wutong][S0M5etXdkAne42aYUHrHZSMCDGCltIsmgHErvJLlpgQ=]。。。

上传文件　test3.txt。。。
上传文件　test4.txt。。。
上传文件　test5.txt。。。
上传文件　test6.txt。。。
上传文件　testpic1.PNG。。。
上传文件　testpic2.PNG。。。
上传文件　testpic3.PNG。。。
同步完成
d:\temp>
update -cloud
删除文件　test3.txt。。。
删除文件　test4.txt。。。
删除文件　test5.txt。。。
删除文件　test6.txt。。。
删除文件　testpic1.PNG。。。
删除文件　testpic2.PNG。。。
删除文件　testpic3.PNG。。。
下载文件　[SecBox][wutong][QA-QCMXNIyC0lwcGnR9uDS4oukLDFZ1qKdWkuIO2LXs=]。。。
下载文件　[SecBox][wutong][TjvLL97i-aCOweMfCj37Zy4oukLDFZ1qKdWkuIO2LXs=]。。。
下载文件　[SecBox][wutong][u-j77CJRPjnIfuPUyV5umSMCDGCltIsmgHErvJLlpgQ=]。。。
下载文件　[SecBox][wutong][Y-lvl5gxhoa9HwQLZtBjeSMCDGCltIsmgHErvJLlpgQ=]。。。
下载文件　[SecBox][wutong][mXvRCm4FSZpwYDgGD8gvXi4oukLDFZ1qKdWkuIO2LXs=]。。。
下载文件　[SecBox][wutong][q_t1tnQEADbcKdzRIEeYcSMCDGCltIsmgHErvJLlpgQ=]。。。
下载文件　[SecBox][wutong][S0M5etXdkAne42aYUHrHZSMCDGCltIsmgHErvJLlpgQ=]。。。
同步完成

4. 引用

[1] "RFC4648," 2006. [Online]. Available: http://www.ietf.org/rfc/rfc4648.txt.