# 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，并基本完成项目文档。

**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：

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，主要负责目录结构的管理和路径到节点的转换。 | - addFileNode  - 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**