

Mac OS X 10.10.4 Yosomite

How to run palisade library on a Mac?

The process is divided into 4 main steps. Namely:-

1. Install brew (uninstall & fix brew)
2. Install gcc latest version
3. Set environment path
4. make clean and make

The current problem with running the palisade on Mac is that gcc regular version on Mac doesn't support the functions used in Source.cpp file of the library.

So which version of gcc are you running?

```
jameslipuma$ gcc --version
Configured with: --prefix=/Applications/Xcode.app/Contents/Developer/usr --with-gxx-include-dir=/Applications/Xcode.app/Contents/Developer/Platforms/MacOSX.platform/Developer/SDKs/MacOSX10.11.sdk/usr/include/c++/4.2.1
Apple LLVM version 7.0.0 (clang-700.0.72)
Target: x86_64-apple-darwin14.5.0
Thread model: posix
jameslipuma$
```

What happens when you run the make file using current 4.2.1 version of gcc on Mac?

Step1: change directory

```
jameslipuma$ ls
Makefile  bin  documents  lbcrypto-doxy-config  spike  test
README    doc  include    lib  src
jameslipuma$ ls -lsa
total 224
0 drwxr-xr-x@ 14 jameslipuma  staff  476 Oct  7 18:41 .
0 drwxr-xr-x@ 19 jameslipuma  staff  646 Oct  7 20:44 ..
0 -rwxr-xr-x@  1 jameslipuma  staff   76 Oct  7 18:41 .gitignore
0 -rwxr-xr-x@  1 jameslipuma  staff 3182 Oct  7 18:41 Makefile
0 -rwxr-xr-x@  1 jameslipuma  staff 1468 Oct  7 18:41 README
0 drwxr-xr-x@  3 jameslipuma  staff  102 Oct  7 18:41 bin
0 drwxr-xr-x@  3 jameslipuma  staff  102 Oct  7 18:41 doc
0 drwxr-xr-x@  7 jameslipuma  staff  238 Oct  7 18:41 documents
0 drwxr-xr-x@  3 jameslipuma  staff  102 Oct  7 18:41 include
200 -rwxr-xr-x@  1 jameslipuma  staff 100331 Oct  7 18:41 lbcrypto-doxy-config
0 drwxr-xr-x@  3 jameslipuma  staff  102 Oct  7 18:41 lib
0 drwxr-xr-x@  3 jameslipuma  staff  102 Oct  7 18:41 spike
0 drwxr-xr-x@  8 jameslipuma  staff  272 Oct  7 18:41 src
0 drwxr-xr-x@  3 jameslipuma  staff  102 Oct  7 18:41 test
```

Step2: run make command

```

james-mbp:palisade-student-edition.git jameslipuma$ make
g++ -Wall -O3 -std=gnu++11 -w -g -I include -c -o build/crypto/lwecrypt.o src/crypto/lwecrypt.cpp
g++ -Wall -O3 -std=gnu++11 -w -g -I include -c -o build/crypto/lwepre.o src/crypto/lwepre.cpp
g++ -Wall -O3 -std=gnu++11 -w -g -I include -c -o build/encoding/ptxtencoding.o src/encoding/ptxtencoding.cpp
g++ -Wall -O3 -std=gnu++11 -w -g -I include -c -o build/lattice/il2n.o src/lattice/il2n.cpp
g++ -Wall -O3 -std=gnu++11 -w -g -I include -c -o build/math/cpu8bit/binint.o src/math/cpu8bit/binint.cpp
g++ -Wall -O3 -std=gnu++11 -w -g -I include -c -o build/math/cpu8bit/binmat.o src/math/cpu8bit/binmat.cpp
g++ -Wall -O3 -std=gnu++11 -w -g -I include -c -o build/math/cpu8bit/binvect.o src/math/cpu8bit/binvect.cpp
g++ -Wall -O3 -std=gnu++11 -w -g -I include -c -o build/math/cpu8bit/dtstruct.o src/math/cpu8bit/dtstruct.cpp
g++ -Wall -O3 -std=gnu++11 -w -g -I include -c -o build/math/cpu8bit/mempool.o src/math/cpu8bit/mempool.cpp
g++ -Wall -O3 -std=gnu++11 -w -g -I include -c -o build/math/distrngen.o src/math/distrngen.cpp
g++ -Wall -O3 -std=gnu++11 -w -g -I include -c -o build/math/nbtheory.o src/math/nbtheory.cpp
g++ -Wall -O3 -std=gnu++11 -w -g -I include -c -o build/math/transfrm.o src/math/transfrm.cpp
g++ -Wall -O3 -std=gnu++11 -w -g -I include -c -o build/Source.o src/Source.cpp
src/Source.cpp:101:55: error: no member named 'to_time_t' in 'std::chrono::steady_clock'
    time_t tnow = std::chrono::high_resolution_clock::to_time_t(now);
                                                    ^
src/Source.cpp:107:21: error: no member named 'from_time_t' in 'std::chrono::steady_clock'; did you mean 'std::chrono::system_clock::from_time_t'?
    auto midnight = std::chrono::high_resolution_clock::from_time_t(mktime(date));
                        ^
src/Source.cpp:107:21: note: 'std::chrono::system_clock::from_time_t'
      std::chrono::system_clock::from_time_t
      ^
/Applications/Xcode.app/Contents/Developer/Toolchains/XcodeDefault.xctoolchain/usr/bin/../include/c++/v1/chrono:926:23: note: 'std::chrono::system_clock::from_time_t'
    declared here
    static time_point from_time_t(time_t __t) _NOEXCEPT;
                        ^
2 errors generated.
make: *** [build/Source.o] Error 1

```

To fix the above issue we need to update gcc to latest version. The Mac version of **apt-get** is called **brew**

If **BREW** is installed the following message will be displayed

```

james-mbp:palisade-student-edition.git jameslipuma$ brew
Example usage:
  brew [info | home | options ] [FORMULA...]
  brew install FORMULA...
  brew uninstall FORMULA...
  brew search [foo]
  brew list [FORMULA...]
  brew update
  brew upgrade [FORMULA...]
  brew pin/unpin [FORMULA...]

Troubleshooting:
  brew doctor
  brew install -vd FORMULA
  brew [--env | config]

Brewing:
  brew create [URL [--no-fetch]]
  brew edit [FORMULA...]
  https://github.com/Homebrew/homebrew/blob/master/share/doc/homebrew/Formula-Cookbook.md

Further help:
  man brew
  brew home
james-mbp:palisade-student-edition.git jameslipuma$

```

If **BREW** is not installed please go to link : <http://brew.sh>
or type in terminal

```
ruby -e "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/master/install)"
```

```
james-mbp:palisade-student-edition.git jameslipuma$ ruby -e "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/master/install)"
==> This script will install:
/usr/local/bin/brew
/usr/local/Library/...
/usr/local/share/man/man1/brew.1

Press RETURN to continue or any other key to abort
==> /usr/bin/sudo /usr/sbin/chown jameslipuma /Library/Caches/Homebrew
Password:
==> Downloading and installing Homebrew...
remote: Counting objects: 3769, done.
remote: Compressing objects: 100% (3608/3608), done.
remote: Total 3769 (delta 43), reused 534 (delta 26), pack-reused 0
Receiving objects: 100% (3769/3769), 3.20 MiB | 0 bytes/s, done.
Resolving deltas: 100% (43/43), done.
From https://github.com/Homebrew/homebrew
* [new branch]      master      -> origin/master
HEAD is now at 3328872 formulae: migrate patches (part 2)
==> Installation successful!
==> Next steps
Run `brew help` to get started
james-mbp:palisade-student-edition.git jameslipuma$
```

If **BREW** is installed and not functioning properly use the below command to uninstall

```
ruby -e "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/master/uninstall)"
```

```
james-mbp:palisade-student-edition.git jameslipuma$ ruby -e "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/master/uninstall)"
Warning: This script will remove:
/Library/Caches/Homebrew/
/Users/jameslipuma/Library/Logs/Homebrew/
/usr/local/.git/
/usr/local/.gitignore
/usr/local/.travis.yml
/usr/local/.yardopts
/usr/local/CODEOFCONDUCT.md
/usr/local/CONTRIBUTING.md
/usr/local/Cellar/
/usr/local/LICENSE.txt
/usr/local/Library/
/usr/local/README.md
/usr/local/SUPPORTERS.md
/usr/local/bin/brew
/usr/local/share/doc/homebrew/
/usr/local/share/man/man1/brew.1
Are you sure you want to uninstall Homebrew? [y/N] y
==> Removing Homebrew installation...
==> Removing empty directories...
==> Homebrew uninstalled!
The following possible Homebrew files were not deleted:
/usr/local/share/
You may consider to remove them by yourself.
You may want to restore /usr/local's original permissions
sudo chmod 0755 /usr/local
sudo chgrp wheel /usr/local
james-mbp:palisade-student-edition.git jameslipuma$
```

and reinstall using above step

To update gcc run the following command in terminal

```
brew home
james-mbp:palisade-student-edition.git jameslipuma$ brew install gcc
```

```
james-mbp:palisade-student-edition.git jameslipuma$ brew update
Already up-to-date.
james-mbp:palisade-student-edition.git jameslipuma$ brew upgrade
james-mbp:palisade-student-edition.git jameslipuma$ brew install gcc
==> Installing dependencies for gcc: gmp, mpfr, libmpc, isl
==> Installing gcc dependency: gmp
==> Downloading https://homebrew.bintray.com/bottles/gmp-6.0.0a.yosemite.bottle.tar.gz
##### 100.0%
==> Pouring gmp-6.0.0a.yosemite.bottle.tar.gz
📦 /usr/local/Cellar/gmp/6.0.0a: 15 files, 3.2M
==> Installing gcc dependency: mpfr
==> Downloading https://homebrew.bintray.com/bottles/mpfr-3.1.3.yosemite.bottle.tar.gz
##### 100.0%
==> Pouring mpfr-3.1.3.yosemite.bottle.tar.gz
📦 /usr/local/Cellar/mpfr/3.1.3: 24 files, 3.6M
==> Installing gcc dependency: libmpc
==> Downloading https://homebrew.bintray.com/bottles/libmpc-1.0.3.yosemite.bottle.tar.gz
##### 100.0%
==> Pouring libmpc-1.0.3.yosemite.bottle.tar.gz
📦 /usr/local/Cellar/libmpc/1.0.3: 10 files, 380K
==> Installing gcc dependency: isl
==> Downloading https://homebrew.bintray.com/bottles/isl-0.14.1.yosemite.bottle.3.tar.gz
##### 100.0%
==> Pouring isl-0.14.1.yosemite.bottle.3.tar.gz
📦 /usr/local/Cellar/isl/0.14.1: 60 files, 3.2M
```

Might take a while, so relax and have a cup of tea. It took 1hr or more on my personal Mac.

If incase brew isnt able to install gcc latest version well and it throws some error. Fix **Brew** by running the following 2 commands

```
brew doctor
xcode-select --install
```

and click install



The "xcode-select" command requires the command line developer tools. Would you like to install the tools now?

Choose Install to continue. Choose Get Xcode to install Xcode and the command line developer tools from the App Store.

Get Xcode

Not Now

Install

```
james-mbp:Cellar jameslipuma$ brew doctor
```

Please note that these warnings are just used to help the Homebrew maintainers with debugging if you file an issue. If everything you use Homebrew for is working fine: please don't worry and just ignore them. Thanks!

Warning: Xcode 7 lacks the 10.10 SDK which can cause some builds to fail.

We recommend installing the Command Line Tools with:

```
xcode-select --install
```

to resolve this issue.

```
james-mbp:Cellar jameslipuma$ xcode-select --install
```

```
xcode-select: note: install requested for command line developer tools
```

```
james-mbp:Cellar jameslipuma$
```

once done, run again

```
brew install gcc
```

the output screen should show more or less the same result.

```
james-mbp:Cellar jameslipuma$ brew install gcc
```

```
==> Downloading https://homebrew.bintray.com/bottles/gcc-5.2.0.yosemite.bottle.2.tar.gz
```

```
##### 100.0%
```

```
==> Pouring gcc-5.2.0.yosemite.bottle.2.tar.gz
```

```
==> Caveats
```

GCC has been built with multilib support. Notably, OpenMP may not work:

https://gcc.gnu.org/bugzilla/show_bug.cgi?id=60670

If you need OpenMP support you may want to

```
brew reinstall gcc --without-multilib
```

```
==> Summary
```

```
📁 /usr/local/Cellar/gcc/5.2.0: 1353 files, 248M
```

```
james-mbp:Cellar jameslipuma$
```

The latest version of gcc 5.2.0 is installed at:

/usr/local/Cellar/gcc/5.2.0/bin

all compiler related programs should be available by default at:

/usr/bin

The last step is to update the path

```
cd /usr/bin
```

```
sudo rm cc gcc c++ g++
```

```
sudo ln -s /usr/local/Cellar/gcc/5.2.0/bin/gcc-5 cc
```

```
sudo ln -s /usr/local/Cellar/gcc/5.2.0/bin/gcc-5 gcc
```

```
sudo ln -s /usr/local/Cellar/gcc/5.2.0/bin/c++-5 c++
```

```
sudo ln -s /usr/local/Cellar/gcc/5.2.0/bin/g++-5 g++
```

Once executed correctly the following command should display the following output screen

<<Its preferred to manually type the above command instead of copying from the above>>

```
james-mbp:palisade jameslipuma$ gcc --version
gcc (Homebrew gcc 5.2.0) 5.2.0
Copyright (C) 2015 Free Software Foundation, Inc.
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
```

```
james-mbp:palisade jameslipuma$ g++ --version
g++ (Homebrew gcc 5.2.0) 5.2.0
Copyright (C) 2015 Free Software Foundation, Inc.
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
```

```
james-mbp:palisade jameslipuma$ c++ --version
c++ (Homebrew gcc 5.2.0) 5.2.0
Copyright (C) 2015 Free Software Foundation, Inc.
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
```

```
james-mbp:palisade jameslipuma$ cc --version
cc (Homebrew gcc 5.2.0) 5.2.0
Copyright (C) 2015 Free Software Foundation, Inc.
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
```

Finally to test the palisade student library again run the make command in the palisade folder

Always run a

make clean

command before running make at this stage

```
james-mbp:palisade jameslipuma$ make clean
Cleaning...
rm -f -r build bin/NTRU-PRE
james-mbp:palisade jameslipuma$ make
g++ -Wall -O3 -std=gnu++11 -w -g -I include -c -o build/crypto/lwecrypt.o src/crypto/lwecrypt.cpp
g++ -Wall -O3 -std=gnu++11 -w -g -I include -c -o build/crypto/lwepre.o src/crypto/lwepre.cpp
g++ -Wall -O3 -std=gnu++11 -w -g -I include -c -o build/encoding/ptxtencoding.o src/encoding/ptxtencoding.cpp
g++ -Wall -O3 -std=gnu++11 -w -g -I include -c -o build/lattice/il2n.o src/lattice/il2n.cpp
g++ -Wall -O3 -std=gnu++11 -w -g -I include -c -o build/math/cpu8bit/binint.o src/math/cpu8bit/binint.cpp
g++ -Wall -O3 -std=gnu++11 -w -g -I include -c -o build/math/cpu8bit/binmat.o src/math/cpu8bit/binmat.cpp
g++ -Wall -O3 -std=gnu++11 -w -g -I include -c -o build/math/cpu8bit/binvect.o src/math/cpu8bit/binvect.cpp
g++ -Wall -O3 -std=gnu++11 -w -g -I include -c -o build/math/cpu8bit/dtstruct.o src/math/cpu8bit/dtstruct.cpp
g++ -Wall -O3 -std=gnu++11 -w -g -I include -c -o build/math/cpu8bit/mempool.o src/math/cpu8bit/mempool.cpp
g++ -Wall -O3 -std=gnu++11 -w -g -I include -c -o build/math/distrngen.o src/math/distrngen.cpp
g++ -Wall -O3 -std=gnu++11 -w -g -I include -c -o build/math/nbtheory.o src/math/nbtheory.cpp
g++ -Wall -O3 -std=gnu++11 -w -g -I include -c -o build/math/transfrm.o src/math/transfrm.cpp
g++ -Wall -O3 -std=gnu++11 -w -g -I include -c -o build/Source.o src/Source.cpp
g++ -Wall -O3 -std=gnu++11 -w -g -I include -c -o build/utls/utilities.o src/utls/utilities.cpp
Linking...
g++ build/crypto/lwecrypt.o build/crypto/lwepre.o build/encoding/ptxtencoding.o build/lattice/il2n.o build/math/cpu8bit/binint.o build/math/cpu8bit/binmat.o build/math/cpu8bit/binvect.o build/math/cpu8bit/dtstruct.o build/math/cpu8bit/mempool.o build/math/distrngen.o build/math/nbtheory.o build/math/transfrm.o build/Source.o build/utls/utilities.o -o bin/NTRU-PRE
```