to@toddzhang-NB01:~$ git clone https://github.com/WeDPR-Team/encryptogroup-ABY.git

Cloning into 'encryptogroup-ABY'...

Username for 'https://github.com': zzzztao

Password for 'https://zzzztao@github.com':

remote: Enumerating objects: 3, done.

remote: Counting objects: 100% (3/3), done.

remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0

Unpacking objects: 100% (3/3), done.

to@toddzhang-NB01:~$ cp encryptogroup-ABY /mnt/d/

cp: -r not specified; omitting directory 'encryptogroup-ABY'

to@toddzhang-NB01:~$ cp -r encryptogroup-ABY /mnt/d/

to@toddzhang-NB01:~$ cd

to@toddzhang-NB01:~$ cd ..

to@toddzhang-NB01:/home$ cd

to@toddzhang-NB01:~$ cd /mnt/d

to@toddzhang-NB01:/mnt/d$ cd encryptogroup-ABY/

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git init .

Reinitialized existing Git repository in /mnt/d/encryptogroup-ABY/.git/

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git add

Nothing specified, nothing added.

Maybe you wanted to say 'git add .'?

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git add .

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git status

On branch master

Your branch is up to date with 'origin/master'.

Changes to be committed:

(use "git reset HEAD <file>..." to unstage)

new file: .gitignore

new file: .gitmodules

new file: .travis.yml

new file: CMakeLists.txt

new file: Doxyfile

new file: LICENSE

new file: bin/.gitignore

new file: bin/circ/circuitformat.md

new file: bin/circ/cos\_16.aby

new file: bin/circ/cos\_32.aby

new file: bin/circ/cs\_matrix16\_16.aby

new file: bin/circ/cs\_matrix32\_32.aby

new file: bin/circ/cs\_matrix\_16.aby

new file: bin/circ/cs\_matrix\_32.aby

new file: bin/circ/fp\_ieee\_add\_32.aby

new file: bin/circ/fp\_ieee\_add\_42.aby

new file: bin/circ/fp\_ieee\_add\_64.aby

new file: bin/circ/fp\_ieee\_cos\_32.aby

new file: bin/circ/fp\_ieee\_cos\_42.aby

new file: bin/circ/fp\_ieee\_div\_32.aby

new file: bin/circ/fp\_ieee\_div\_42.aby

new file: bin/circ/fp\_ieee\_div\_64.aby

new file: bin/circ/fp\_ieee\_mult\_32.aby

new file: bin/circ/fp\_ieee\_mult\_42.aby

new file: bin/circ/fp\_ieee\_mult\_64.aby

new file: bin/circ/fp\_ieee\_sin\_32.aby

new file: bin/circ/fp\_ieee\_sin\_42.aby

new file: bin/circ/fp\_ieee\_sqr\_32.aby

new file: bin/circ/fp\_ieee\_sqr\_42.aby

new file: bin/circ/fp\_ieee\_sqr\_64.aby

new file: bin/circ/fp\_ieee\_sqrt\_32.aby

new file: bin/circ/fp\_ieee\_sqrt\_42.aby

new file: bin/circ/fp\_ieee\_sqrt\_64.aby

new file: bin/circ/fp\_ieee\_sub\_32.aby

new file: bin/circ/fp\_ieee\_sub\_42.aby

new file: bin/circ/fp\_ieee\_sub\_64.aby

new file: bin/circ/fp\_nostatus\_add\_32.aby

new file: bin/circ/fp\_nostatus\_add\_42.aby

new file: bin/circ/fp\_nostatus\_add\_64.aby

new file: bin/circ/fp\_nostatus\_cmp\_32.aby

new file: bin/circ/fp\_nostatus\_cmp\_42.aby

new file: bin/circ/fp\_nostatus\_cmp\_64.aby

new file: bin/circ/fp\_nostatus\_div\_32.aby

new file: bin/circ/fp\_nostatus\_div\_42.aby

new file: bin/circ/fp\_nostatus\_div\_64.aby

new file: bin/circ/fp\_nostatus\_exp2\_32.aby

new file: bin/circ/fp\_nostatus\_exp2\_42.aby

new file: bin/circ/fp\_nostatus\_exp2\_64.aby

new file: bin/circ/fp\_nostatus\_exp\_32.aby

new file: bin/circ/fp\_nostatus\_exp\_42.aby

new file: bin/circ/fp\_nostatus\_ln\_32.aby

new file: bin/circ/fp\_nostatus\_ln\_42.aby

new file: bin/circ/fp\_nostatus\_ln\_64.aby

new file: bin/circ/fp\_nostatus\_log2\_32.aby

new file: bin/circ/fp\_nostatus\_log2\_42.aby

new file: bin/circ/fp\_nostatus\_log2\_64.aby

new file: bin/circ/fp\_nostatus\_mult\_32.aby

new file: bin/circ/fp\_nostatus\_mult\_42.aby

new file: bin/circ/fp\_nostatus\_mult\_64.aby

new file: bin/circ/fp\_nostatus\_sqr\_32.aby

new file: bin/circ/fp\_nostatus\_sqr\_42.aby

new file: bin/circ/fp\_nostatus\_sqr\_64.aby

new file: bin/circ/fp\_nostatus\_sqrt\_32.aby

new file: bin/circ/fp\_nostatus\_sqrt\_42.aby

new file: bin/circ/fp\_nostatus\_sqrt\_64.aby

new file: bin/circ/fp\_nostatus\_sub\_32.aby

new file: bin/circ/fp\_nostatus\_sub\_42.aby

new file: bin/circ/fp\_nostatus\_sub\_64.aby

new file: bin/circ/int\_div\_16.aby

new file: bin/circ/int\_div\_32.aby

new file: bin/circ/int\_div\_64.aby

new file: bin/circ/int\_div\_8.aby

new file: bin/circ/rc\_matrix16\_16.aby

new file: bin/circ/rc\_matrix32\_32.aby

new file: bin/circ/rc\_matrix\_16.aby

new file: bin/circ/rc\_matrix\_32.aby

new file: bin/circ/sin\_16.aby

new file: bin/circ/sin\_32.aby

new file: bin/uc/adder\_circ.txt

new file: bin/uc/adder\_prog.txt

new file: bin/uc/dummy\_circ.txt

new file: bin/uc/dummy\_prog.txt

new file: cmake/ABYConfig.cmake.in

new file: cmake/FindGMP.cmake

new file: cmake/FindGMPXX.cmake

new file: runtest\_scr.sh

new file: src/abycore/ABY\_utils/ABYconstants.h

new file: src/abycore/ABY\_utils/convtypes.h

new file: src/abycore/ABY\_utils/yaokey.h

new file: src/abycore/CMakeLists.txt

new file: src/abycore/DGK/dgkparty.cpp

new file: src/abycore/DGK/dgkparty.h

new file: src/abycore/DJN/djnparty.cpp

new file: src/abycore/DJN/djnparty.h

new file: src/abycore/aby/abyparty.cpp

new file: src/abycore/aby/abyparty.h

new file: src/abycore/aby/abysetup.cpp

new file: src/abycore/aby/abysetup.h

new file: src/abycore/circuit/abycircuit.cpp

new file: src/abycore/circuit/abycircuit.h

new file: src/abycore/circuit/arithmeticcircuits.cpp

new file: src/abycore/circuit/arithmeticcircuits.h

new file: src/abycore/circuit/booleancircuits.cpp

new file: src/abycore/circuit/booleancircuits.h

new file: src/abycore/circuit/circuit.cpp

new file: src/abycore/circuit/circuit.h

new file: src/abycore/circuit/share.cpp

new file: src/abycore/circuit/share.h

new file: src/abycore/ot/.gitignore

new file: src/abycore/sharing/arithsharing.cpp

new file: src/abycore/sharing/arithsharing.h

new file: src/abycore/sharing/boolsharing.cpp

new file: src/abycore/sharing/boolsharing.h

new file: src/abycore/sharing/sharing.cpp

new file: src/abycore/sharing/sharing.h

new file: src/abycore/sharing/splut.cpp

new file: src/abycore/sharing/splut.h

new file: src/abycore/sharing/yaoclientsharing.cpp

new file: src/abycore/sharing/yaoclientsharing.h

new file: src/abycore/sharing/yaoserversharing.cpp

new file: src/abycore/sharing/yaoserversharing.h

new file: src/abycore/sharing/yaosharing.cpp

new file: src/abycore/sharing/yaosharing.h

new file: src/examples/CMakeLists.txt

new file: src/examples/aes/CMakeLists.txt

new file: src/examples/aes/aes\_test.cpp

new file: src/examples/aes/common/aescircuit.cpp

new file: src/examples/aes/common/aescircuit.h

new file: src/examples/bench\_operations/CMakeLists.txt

new file: src/examples/bench\_operations/bench\_operations.cpp

new file: src/examples/euclidean\_distance/CMakeLists.txt

new file: src/examples/euclidean\_distance/common/euclidean\_dist.cpp

new file: src/examples/euclidean\_distance/common/euclidean\_dist.h

new file: src/examples/euclidean\_distance/euclidean\_distance\_test.cpp

new file: src/examples/float/CMakeLists.txt

new file: src/examples/float/abyfloat.cpp

new file: src/examples/innerproduct/CMakeLists.txt

new file: src/examples/innerproduct/common/innerproduct.cpp

new file: src/examples/innerproduct/common/innerproduct.h

new file: src/examples/innerproduct/innerproduct\_test.cpp

new file: src/examples/lowmc/CMakeLists.txt

new file: src/examples/lowmc/common/lowmccircuit.cpp

new file: src/examples/lowmc/common/lowmccircuit.h

new file: src/examples/lowmc/lowmc.cpp

new file: src/examples/millionaire\_prob/CMakeLists.txt

new file: src/examples/millionaire\_prob/common/millionaire\_prob.cpp

new file: src/examples/millionaire\_prob/common/millionaire\_prob.h

new file: src/examples/millionaire\_prob/millionaire\_prob\_test.cpp

new file: src/examples/min-euclidean-dist/CMakeLists.txt

new file: src/examples/min-euclidean-dist/common/min-euclidean-dist-circuit.cpp

new file: src/examples/min-euclidean-dist/common/min-euclidean-dist-circuit.h

new file: src/examples/min-euclidean-dist/min-euclidean-dist.cpp

new file: src/examples/psi\_phasing/CMakeLists.txt

new file: src/examples/psi\_phasing/common/hashing/cuckoo.cpp

new file: src/examples/psi\_phasing/common/hashing/cuckoo.h

new file: src/examples/psi\_phasing/common/hashing/hashing\_util.h

new file: src/examples/psi\_phasing/common/hashing/simple\_hashing.cpp

new file: src/examples/psi\_phasing/common/hashing/simple\_hashing.h

new file: src/examples/psi\_phasing/common/hashing\_includes.h

new file: src/examples/psi\_phasing/common/phasing\_circuit.cpp

new file: src/examples/psi\_phasing/common/phasing\_circuit.h

new file: src/examples/psi\_phasing/psi\_phasing.cpp

new file: src/examples/psi\_scs/CMakeLists.txt

new file: src/examples/psi\_scs/common/WaksmanPermutation.cpp

new file: src/examples/psi\_scs/common/WaksmanPermutation.h

new file: src/examples/psi\_scs/common/sort\_compare\_shuffle.cpp

new file: src/examples/psi\_scs/common/sort\_compare\_shuffle.h

new file: src/examples/psi\_scs/psi\_scs.cpp

new file: src/examples/sha1/CMakeLists.txt

new file: src/examples/sha1/common/sha1\_circuit.cpp

new file: src/examples/sha1/common/sha1\_circuit.h

new file: src/examples/sha1/sha1\_test.cpp

new file: src/examples/threshold\_euclidean\_dist\_2d\_simd/CMakeLists.txt

new file: src/examples/threshold\_euclidean\_dist\_2d\_simd/common/threshold-euclidean-dist.cpp

new file: src/examples/threshold\_euclidean\_dist\_2d\_simd/common/threshold-euclidean-dist.h

new file: src/examples/threshold\_euclidean\_dist\_2d\_simd/threshold-euclidean-dist.cpp

new file: src/examples/uc\_circuit/CMakeLists.txt

new file: src/examples/uc\_circuit/common/uc\_circuit.cpp

new file: src/examples/uc\_circuit/common/uc\_circuit.h

new file: src/examples/uc\_circuit/uc\_circuit\_test.cpp

new file: src/test/CMakeLists.txt

new file: src/test/abytest.cpp

new file: src/test/abytest.h

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git commit "init code"

error: pathspec 'init code' did not match any file(s) known to git.

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ gst

Command 'gst' not found, but can be installed with:

sudo apt install gnu-smalltalk

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ ls

CMakeLists.txt LICENSE bin extern src

Doxyfile README.md cmake runtest\_scr.sh

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ ls -a

. .gitignore CMakeLists.txt README.md extern

.. .gitmodules Doxyfile bin runtest\_scr.sh

.git .travis.yml LICENSE cmake src

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ gst

Command 'gst' not found, but can be installed with:

sudo apt install gnu-smalltalk

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git status

On branch master

Your branch is up to date with 'origin/master'.

Changes to be committed:

(use "git reset HEAD <file>..." to unstage)

new file: .gitignore

new file: .gitmodules

new file: .travis.yml

new file: CMakeLists.txt

new file: Doxyfile

new file: LICENSE

new file: bin/.gitignore

new file: bin/circ/circuitformat.md

new file: bin/circ/cos\_16.aby

new file: bin/circ/cos\_32.aby

new file: bin/circ/cs\_matrix16\_16.aby

new file: bin/circ/cs\_matrix32\_32.aby

new file: bin/circ/cs\_matrix\_16.aby

new file: bin/circ/cs\_matrix\_32.aby

new file: bin/circ/fp\_ieee\_add\_32.aby

new file: bin/circ/fp\_ieee\_add\_42.aby

new file: bin/circ/fp\_ieee\_add\_64.aby

new file: bin/circ/fp\_ieee\_cos\_32.aby

new file: bin/circ/fp\_ieee\_cos\_42.aby

new file: bin/circ/fp\_ieee\_div\_32.aby

new file: bin/circ/fp\_ieee\_div\_42.aby

new file: bin/circ/fp\_ieee\_div\_64.aby

new file: bin/circ/fp\_ieee\_mult\_32.aby

new file: bin/circ/fp\_ieee\_mult\_42.aby

new file: bin/circ/fp\_ieee\_mult\_64.aby

new file: bin/circ/fp\_ieee\_sin\_32.aby

new file: bin/circ/fp\_ieee\_sin\_42.aby

new file: bin/circ/fp\_ieee\_sqr\_32.aby

new file: bin/circ/fp\_ieee\_sqr\_42.aby

new file: bin/circ/fp\_ieee\_sqr\_64.aby

new file: bin/circ/fp\_ieee\_sqrt\_32.aby

new file: bin/circ/fp\_ieee\_sqrt\_42.aby

new file: bin/circ/fp\_ieee\_sqrt\_64.aby

new file: bin/circ/fp\_ieee\_sub\_32.aby

new file: bin/circ/fp\_ieee\_sub\_42.aby

new file: bin/circ/fp\_ieee\_sub\_64.aby

new file: bin/circ/fp\_nostatus\_add\_32.aby

new file: bin/circ/fp\_nostatus\_add\_42.aby

new file: bin/circ/fp\_nostatus\_add\_64.aby

new file: bin/circ/fp\_nostatus\_cmp\_32.aby

new file: bin/circ/fp\_nostatus\_cmp\_42.aby

new file: bin/circ/fp\_nostatus\_cmp\_64.aby

new file: bin/circ/fp\_nostatus\_div\_32.aby

new file: bin/circ/fp\_nostatus\_div\_42.aby

new file: bin/circ/fp\_nostatus\_div\_64.aby

new file: bin/circ/fp\_nostatus\_exp2\_32.aby

new file: bin/circ/fp\_nostatus\_exp2\_42.aby

new file: bin/circ/fp\_nostatus\_exp2\_64.aby

new file: bin/circ/fp\_nostatus\_exp\_32.aby

new file: bin/circ/fp\_nostatus\_exp\_42.aby

new file: bin/circ/fp\_nostatus\_ln\_32.aby

new file: bin/circ/fp\_nostatus\_ln\_42.aby

new file: bin/circ/fp\_nostatus\_ln\_64.aby

new file: bin/circ/fp\_nostatus\_log2\_32.aby

new file: bin/circ/fp\_nostatus\_log2\_42.aby

new file: bin/circ/fp\_nostatus\_log2\_64.aby

new file: bin/circ/fp\_nostatus\_mult\_32.aby

new file: bin/circ/fp\_nostatus\_mult\_42.aby

new file: bin/circ/fp\_nostatus\_mult\_64.aby

new file: bin/circ/fp\_nostatus\_sqr\_32.aby

new file: bin/circ/fp\_nostatus\_sqr\_42.aby

new file: bin/circ/fp\_nostatus\_sqr\_64.aby

new file: bin/circ/fp\_nostatus\_sqrt\_32.aby

new file: bin/circ/fp\_nostatus\_sqrt\_42.aby

new file: bin/circ/fp\_nostatus\_sqrt\_64.aby

new file: bin/circ/fp\_nostatus\_sub\_32.aby

new file: bin/circ/fp\_nostatus\_sub\_42.aby

new file: bin/circ/fp\_nostatus\_sub\_64.aby

new file: bin/circ/int\_div\_16.aby

new file: bin/circ/int\_div\_32.aby

new file: bin/circ/int\_div\_64.aby

new file: bin/circ/int\_div\_8.aby

new file: bin/circ/rc\_matrix16\_16.aby

new file: bin/circ/rc\_matrix32\_32.aby

new file: bin/circ/rc\_matrix\_16.aby

new file: bin/circ/rc\_matrix\_32.aby

new file: bin/circ/sin\_16.aby

new file: bin/circ/sin\_32.aby

new file: bin/uc/adder\_circ.txt

new file: bin/uc/adder\_prog.txt

new file: bin/uc/dummy\_circ.txt

new file: bin/uc/dummy\_prog.txt

new file: cmake/ABYConfig.cmake.in

new file: cmake/FindGMP.cmake

new file: cmake/FindGMPXX.cmake

new file: runtest\_scr.sh

new file: src/abycore/ABY\_utils/ABYconstants.h

new file: src/abycore/ABY\_utils/convtypes.h

new file: src/abycore/ABY\_utils/yaokey.h

new file: src/abycore/CMakeLists.txt

new file: src/abycore/DGK/dgkparty.cpp

new file: src/abycore/DGK/dgkparty.h

new file: src/abycore/DJN/djnparty.cpp

new file: src/abycore/DJN/djnparty.h

new file: src/abycore/aby/abyparty.cpp

new file: src/abycore/aby/abyparty.h

new file: src/abycore/aby/abysetup.cpp

new file: src/abycore/aby/abysetup.h

new file: src/abycore/circuit/abycircuit.cpp

new file: src/abycore/circuit/abycircuit.h

new file: src/abycore/circuit/arithmeticcircuits.cpp

new file: src/abycore/circuit/arithmeticcircuits.h

new file: src/abycore/circuit/booleancircuits.cpp

new file: src/abycore/circuit/booleancircuits.h

new file: src/abycore/circuit/circuit.cpp

new file: src/abycore/circuit/circuit.h

new file: src/abycore/circuit/share.cpp

new file: src/abycore/circuit/share.h

new file: src/abycore/ot/.gitignore

new file: src/abycore/sharing/arithsharing.cpp

new file: src/abycore/sharing/arithsharing.h

new file: src/abycore/sharing/boolsharing.cpp

new file: src/abycore/sharing/boolsharing.h

new file: src/abycore/sharing/sharing.cpp

new file: src/abycore/sharing/sharing.h

new file: src/abycore/sharing/splut.cpp

new file: src/abycore/sharing/splut.h

new file: src/abycore/sharing/yaoclientsharing.cpp

new file: src/abycore/sharing/yaoclientsharing.h

new file: src/abycore/sharing/yaoserversharing.cpp

new file: src/abycore/sharing/yaoserversharing.h

new file: src/abycore/sharing/yaosharing.cpp

new file: src/abycore/sharing/yaosharing.h

new file: src/examples/CMakeLists.txt

new file: src/examples/aes/CMakeLists.txt

new file: src/examples/aes/aes\_test.cpp

new file: src/examples/aes/common/aescircuit.cpp

new file: src/examples/aes/common/aescircuit.h

new file: src/examples/bench\_operations/CMakeLists.txt

new file: src/examples/bench\_operations/bench\_operations.cpp

new file: src/examples/euclidean\_distance/CMakeLists.txt

new file: src/examples/euclidean\_distance/common/euclidean\_dist.cpp

new file: src/examples/euclidean\_distance/common/euclidean\_dist.h

new file: src/examples/euclidean\_distance/euclidean\_distance\_test.cpp

new file: src/examples/float/CMakeLists.txt

new file: src/examples/float/abyfloat.cpp

new file: src/examples/innerproduct/CMakeLists.txt

new file: src/examples/innerproduct/common/innerproduct.cpp

new file: src/examples/innerproduct/common/innerproduct.h

new file: src/examples/innerproduct/innerproduct\_test.cpp

new file: src/examples/lowmc/CMakeLists.txt

new file: src/examples/lowmc/common/lowmccircuit.cpp

new file: src/examples/lowmc/common/lowmccircuit.h

new file: src/examples/lowmc/lowmc.cpp

new file: src/examples/millionaire\_prob/CMakeLists.txt

new file: src/examples/millionaire\_prob/common/millionaire\_prob.cpp

new file: src/examples/millionaire\_prob/common/millionaire\_prob.h

new file: src/examples/millionaire\_prob/millionaire\_prob\_test.cpp

new file: src/examples/min-euclidean-dist/CMakeLists.txt

new file: src/examples/min-euclidean-dist/common/min-euclidean-dist-circuit.cpp

new file: src/examples/min-euclidean-dist/common/min-euclidean-dist-circuit.h

new file: src/examples/min-euclidean-dist/min-euclidean-dist.cpp

new file: src/examples/psi\_phasing/CMakeLists.txt

new file: src/examples/psi\_phasing/common/hashing/cuckoo.cpp

new file: src/examples/psi\_phasing/common/hashing/cuckoo.h

new file: src/examples/psi\_phasing/common/hashing/hashing\_util.h

new file: src/examples/psi\_phasing/common/hashing/simple\_hashing.cpp

new file: src/examples/psi\_phasing/common/hashing/simple\_hashing.h

new file: src/examples/psi\_phasing/common/hashing\_includes.h

new file: src/examples/psi\_phasing/common/phasing\_circuit.cpp

new file: src/examples/psi\_phasing/common/phasing\_circuit.h

new file: src/examples/psi\_phasing/psi\_phasing.cpp

new file: src/examples/psi\_scs/CMakeLists.txt

new file: src/examples/psi\_scs/common/WaksmanPermutation.cpp

new file: src/examples/psi\_scs/common/WaksmanPermutation.h

new file: src/examples/psi\_scs/common/sort\_compare\_shuffle.cpp

new file: src/examples/psi\_scs/common/sort\_compare\_shuffle.h

new file: src/examples/psi\_scs/psi\_scs.cpp

new file: src/examples/sha1/CMakeLists.txt

new file: src/examples/sha1/common/sha1\_circuit.cpp

new file: src/examples/sha1/common/sha1\_circuit.h

new file: src/examples/sha1/sha1\_test.cpp

new file: src/examples/threshold\_euclidean\_dist\_2d\_simd/CMakeLists.txt

new file: src/examples/threshold\_euclidean\_dist\_2d\_simd/common/threshold-euclidean-dist.cpp

new file: src/examples/threshold\_euclidean\_dist\_2d\_simd/common/threshold-euclidean-dist.h

new file: src/examples/threshold\_euclidean\_dist\_2d\_simd/threshold-euclidean-dist.cpp

new file: src/examples/uc\_circuit/CMakeLists.txt

new file: src/examples/uc\_circuit/common/uc\_circuit.cpp

new file: src/examples/uc\_circuit/common/uc\_circuit.h

new file: src/examples/uc\_circuit/uc\_circuit\_test.cpp

new file: src/test/CMakeLists.txt

new file: src/test/abytest.cpp

new file: src/test/abytest.h

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git commit "init code"

error: pathspec 'init code' did not match any file(s) known to git.

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ pathspec 'init code' did not match any file(s) known to git

bash: syntax error near unexpected token `('

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git branch -a

\* master

remotes/origin/HEAD -> origin/master

remotes/origin/master

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ grv

Command 'grv' not found, did you mean:

command 'gav' from deb gav

command 'gcv' from deb scotch

command 'gtv' from deb smpeg-gtv

command 'grc' from deb grc

command 'grn' from deb groff

command 'gri' from deb gri

command 'gv' from deb gv

Try: sudo apt install <deb name>

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git remote -v

origin https://github.com/WeDPR-Team/encryptogroup-ABY.git (fetch)

origin https://github.com/WeDPR-Team/encryptogroup-ABY.git (push)

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git remote remove origin

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git remote add origin https://github.com/zzzztao/encryptogroup-ABY.git

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git remote add up https://github.com/WeDPR-Team/encryptogroup-ABY.git

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git remote -v

origin https://github.com/zzzztao/encryptogroup-ABY.git (fetch)

origin https://github.com/zzzztao/encryptogroup-ABY.git (push)

up https://github.com/WeDPR-Team/encryptogroup-ABY.git (fetch)

up https://github.com/WeDPR-Team/encryptogroup-ABY.git (push)

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ gst

Command 'gst' not found, but can be installed with:

sudo apt install gnu-smalltalk

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git status

On branch master

Changes to be committed:

(use "git reset HEAD <file>..." to unstage)

new file: .gitignore

new file: .gitmodules

new file: .travis.yml

new file: CMakeLists.txt

new file: Doxyfile

new file: LICENSE

new file: bin/.gitignore

new file: bin/circ/circuitformat.md

new file: bin/circ/cos\_16.aby

new file: bin/circ/cos\_32.aby

new file: bin/circ/cs\_matrix16\_16.aby

new file: bin/circ/cs\_matrix32\_32.aby

new file: bin/circ/cs\_matrix\_16.aby

new file: bin/circ/cs\_matrix\_32.aby

new file: bin/circ/fp\_ieee\_add\_32.aby

new file: bin/circ/fp\_ieee\_add\_42.aby

new file: bin/circ/fp\_ieee\_add\_64.aby

new file: bin/circ/fp\_ieee\_cos\_32.aby

new file: bin/circ/fp\_ieee\_cos\_42.aby

new file: bin/circ/fp\_ieee\_div\_32.aby

new file: bin/circ/fp\_ieee\_div\_42.aby

new file: bin/circ/fp\_ieee\_div\_64.aby

new file: bin/circ/fp\_ieee\_mult\_32.aby

new file: bin/circ/fp\_ieee\_mult\_42.aby

new file: bin/circ/fp\_ieee\_mult\_64.aby

new file: bin/circ/fp\_ieee\_sin\_32.aby

new file: bin/circ/fp\_ieee\_sin\_42.aby

new file: bin/circ/fp\_ieee\_sqr\_32.aby

new file: bin/circ/fp\_ieee\_sqr\_42.aby

new file: bin/circ/fp\_ieee\_sqr\_64.aby

new file: bin/circ/fp\_ieee\_sqrt\_32.aby

new file: bin/circ/fp\_ieee\_sqrt\_42.aby

new file: bin/circ/fp\_ieee\_sqrt\_64.aby

new file: bin/circ/fp\_ieee\_sub\_32.aby

new file: bin/circ/fp\_ieee\_sub\_42.aby

new file: bin/circ/fp\_ieee\_sub\_64.aby

new file: bin/circ/fp\_nostatus\_add\_32.aby

new file: bin/circ/fp\_nostatus\_add\_42.aby

new file: bin/circ/fp\_nostatus\_add\_64.aby

new file: bin/circ/fp\_nostatus\_cmp\_32.aby

new file: bin/circ/fp\_nostatus\_cmp\_42.aby

new file: bin/circ/fp\_nostatus\_cmp\_64.aby

new file: bin/circ/fp\_nostatus\_div\_32.aby

new file: bin/circ/fp\_nostatus\_div\_42.aby

new file: bin/circ/fp\_nostatus\_div\_64.aby

new file: bin/circ/fp\_nostatus\_exp2\_32.aby

new file: bin/circ/fp\_nostatus\_exp2\_42.aby

new file: bin/circ/fp\_nostatus\_exp2\_64.aby

new file: bin/circ/fp\_nostatus\_exp\_32.aby

new file: bin/circ/fp\_nostatus\_exp\_42.aby

new file: bin/circ/fp\_nostatus\_ln\_32.aby

new file: bin/circ/fp\_nostatus\_ln\_42.aby

new file: bin/circ/fp\_nostatus\_ln\_64.aby

new file: bin/circ/fp\_nostatus\_log2\_32.aby

new file: bin/circ/fp\_nostatus\_log2\_42.aby

new file: bin/circ/fp\_nostatus\_log2\_64.aby

new file: bin/circ/fp\_nostatus\_mult\_32.aby

new file: bin/circ/fp\_nostatus\_mult\_42.aby

new file: bin/circ/fp\_nostatus\_mult\_64.aby

new file: bin/circ/fp\_nostatus\_sqr\_32.aby

new file: bin/circ/fp\_nostatus\_sqr\_42.aby

new file: bin/circ/fp\_nostatus\_sqr\_64.aby

new file: bin/circ/fp\_nostatus\_sqrt\_32.aby

new file: bin/circ/fp\_nostatus\_sqrt\_42.aby

new file: bin/circ/fp\_nostatus\_sqrt\_64.aby

new file: bin/circ/fp\_nostatus\_sub\_32.aby

new file: bin/circ/fp\_nostatus\_sub\_42.aby

new file: bin/circ/fp\_nostatus\_sub\_64.aby

new file: bin/circ/int\_div\_16.aby

new file: bin/circ/int\_div\_32.aby

new file: bin/circ/int\_div\_64.aby

new file: bin/circ/int\_div\_8.aby

new file: bin/circ/rc\_matrix16\_16.aby

new file: bin/circ/rc\_matrix32\_32.aby

new file: bin/circ/rc\_matrix\_16.aby

new file: bin/circ/rc\_matrix\_32.aby

new file: bin/circ/sin\_16.aby

new file: bin/circ/sin\_32.aby

new file: bin/uc/adder\_circ.txt

new file: bin/uc/adder\_prog.txt

new file: bin/uc/dummy\_circ.txt

new file: bin/uc/dummy\_prog.txt

new file: cmake/ABYConfig.cmake.in

new file: cmake/FindGMP.cmake

new file: cmake/FindGMPXX.cmake

new file: runtest\_scr.sh

new file: src/abycore/ABY\_utils/ABYconstants.h

new file: src/abycore/ABY\_utils/convtypes.h

new file: src/abycore/ABY\_utils/yaokey.h

new file: src/abycore/CMakeLists.txt

new file: src/abycore/DGK/dgkparty.cpp

new file: src/abycore/DGK/dgkparty.h

new file: src/abycore/DJN/djnparty.cpp

new file: src/abycore/DJN/djnparty.h

new file: src/abycore/aby/abyparty.cpp

new file: src/abycore/aby/abyparty.h

new file: src/abycore/aby/abysetup.cpp

new file: src/abycore/aby/abysetup.h

new file: src/abycore/circuit/abycircuit.cpp

new file: src/abycore/circuit/abycircuit.h

new file: src/abycore/circuit/arithmeticcircuits.cpp

new file: src/abycore/circuit/arithmeticcircuits.h

new file: src/abycore/circuit/booleancircuits.cpp

new file: src/abycore/circuit/booleancircuits.h

new file: src/abycore/circuit/circuit.cpp

new file: src/abycore/circuit/circuit.h

new file: src/abycore/circuit/share.cpp

new file: src/abycore/circuit/share.h

new file: src/abycore/ot/.gitignore

new file: src/abycore/sharing/arithsharing.cpp

new file: src/abycore/sharing/arithsharing.h

new file: src/abycore/sharing/boolsharing.cpp

new file: src/abycore/sharing/boolsharing.h

new file: src/abycore/sharing/sharing.cpp

new file: src/abycore/sharing/sharing.h

new file: src/abycore/sharing/splut.cpp

new file: src/abycore/sharing/splut.h

new file: src/abycore/sharing/yaoclientsharing.cpp

new file: src/abycore/sharing/yaoclientsharing.h

new file: src/abycore/sharing/yaoserversharing.cpp

new file: src/abycore/sharing/yaoserversharing.h

new file: src/abycore/sharing/yaosharing.cpp

new file: src/abycore/sharing/yaosharing.h

new file: src/examples/CMakeLists.txt

new file: src/examples/aes/CMakeLists.txt

new file: src/examples/aes/aes\_test.cpp

new file: src/examples/aes/common/aescircuit.cpp

new file: src/examples/aes/common/aescircuit.h

new file: src/examples/bench\_operations/CMakeLists.txt

new file: src/examples/bench\_operations/bench\_operations.cpp

new file: src/examples/euclidean\_distance/CMakeLists.txt

new file: src/examples/euclidean\_distance/common/euclidean\_dist.cpp

new file: src/examples/euclidean\_distance/common/euclidean\_dist.h

new file: src/examples/euclidean\_distance/euclidean\_distance\_test.cpp

new file: src/examples/float/CMakeLists.txt

new file: src/examples/float/abyfloat.cpp

new file: src/examples/innerproduct/CMakeLists.txt

new file: src/examples/innerproduct/common/innerproduct.cpp

new file: src/examples/innerproduct/common/innerproduct.h

new file: src/examples/innerproduct/innerproduct\_test.cpp

new file: src/examples/lowmc/CMakeLists.txt

new file: src/examples/lowmc/common/lowmccircuit.cpp

new file: src/examples/lowmc/common/lowmccircuit.h

new file: src/examples/lowmc/lowmc.cpp

new file: src/examples/millionaire\_prob/CMakeLists.txt

new file: src/examples/millionaire\_prob/common/millionaire\_prob.cpp

new file: src/examples/millionaire\_prob/common/millionaire\_prob.h

new file: src/examples/millionaire\_prob/millionaire\_prob\_test.cpp

new file: src/examples/min-euclidean-dist/CMakeLists.txt

new file: src/examples/min-euclidean-dist/common/min-euclidean-dist-circuit.cpp

new file: src/examples/min-euclidean-dist/common/min-euclidean-dist-circuit.h

new file: src/examples/min-euclidean-dist/min-euclidean-dist.cpp

new file: src/examples/psi\_phasing/CMakeLists.txt

new file: src/examples/psi\_phasing/common/hashing/cuckoo.cpp

new file: src/examples/psi\_phasing/common/hashing/cuckoo.h

new file: src/examples/psi\_phasing/common/hashing/hashing\_util.h

new file: src/examples/psi\_phasing/common/hashing/simple\_hashing.cpp

new file: src/examples/psi\_phasing/common/hashing/simple\_hashing.h

new file: src/examples/psi\_phasing/common/hashing\_includes.h

new file: src/examples/psi\_phasing/common/phasing\_circuit.cpp

new file: src/examples/psi\_phasing/common/phasing\_circuit.h

new file: src/examples/psi\_phasing/psi\_phasing.cpp

new file: src/examples/psi\_scs/CMakeLists.txt

new file: src/examples/psi\_scs/common/WaksmanPermutation.cpp

new file: src/examples/psi\_scs/common/WaksmanPermutation.h

new file: src/examples/psi\_scs/common/sort\_compare\_shuffle.cpp

new file: src/examples/psi\_scs/common/sort\_compare\_shuffle.h

new file: src/examples/psi\_scs/psi\_scs.cpp

new file: src/examples/sha1/CMakeLists.txt

new file: src/examples/sha1/common/sha1\_circuit.cpp

new file: src/examples/sha1/common/sha1\_circuit.h

new file: src/examples/sha1/sha1\_test.cpp

new file: src/examples/threshold\_euclidean\_dist\_2d\_simd/CMakeLists.txt

new file: src/examples/threshold\_euclidean\_dist\_2d\_simd/common/threshold-euclidean-dist.cpp

new file: src/examples/threshold\_euclidean\_dist\_2d\_simd/common/threshold-euclidean-dist.h

new file: src/examples/threshold\_euclidean\_dist\_2d\_simd/threshold-euclidean-dist.cpp

new file: src/examples/uc\_circuit/CMakeLists.txt

new file: src/examples/uc\_circuit/common/uc\_circuit.cpp

new file: src/examples/uc\_circuit/common/uc\_circuit.h

new file: src/examples/uc\_circuit/uc\_circuit\_test.cpp

new file: src/test/CMakeLists.txt

new file: src/test/abytest.cpp

new file: src/test/abytest.h

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git commit "init code"

error: pathspec 'init code' did not match any file(s) known to git.

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ gco .

Command 'gco' not found, but there are 17 similar ones.

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ gst

Command 'gst' not found, but can be installed with:

sudo apt install gnu-smalltalk

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git checkout .

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git status

On branch master

Changes to be committed:

(use "git reset HEAD <file>..." to unstage)

new file: .gitignore

new file: .gitmodules

new file: .travis.yml

new file: CMakeLists.txt

new file: Doxyfile

new file: LICENSE

new file: bin/.gitignore

new file: bin/circ/circuitformat.md

new file: bin/circ/cos\_16.aby

new file: bin/circ/cos\_32.aby

new file: bin/circ/cs\_matrix16\_16.aby

new file: bin/circ/cs\_matrix32\_32.aby

new file: bin/circ/cs\_matrix\_16.aby

new file: bin/circ/cs\_matrix\_32.aby

new file: bin/circ/fp\_ieee\_add\_32.aby

new file: bin/circ/fp\_ieee\_add\_42.aby

new file: bin/circ/fp\_ieee\_add\_64.aby

new file: bin/circ/fp\_ieee\_cos\_32.aby

new file: bin/circ/fp\_ieee\_cos\_42.aby

new file: bin/circ/fp\_ieee\_div\_32.aby

new file: bin/circ/fp\_ieee\_div\_42.aby

new file: bin/circ/fp\_ieee\_div\_64.aby

new file: bin/circ/fp\_ieee\_mult\_32.aby

new file: bin/circ/fp\_ieee\_mult\_42.aby

new file: bin/circ/fp\_ieee\_mult\_64.aby

new file: bin/circ/fp\_ieee\_sin\_32.aby

new file: bin/circ/fp\_ieee\_sin\_42.aby

new file: bin/circ/fp\_ieee\_sqr\_32.aby

new file: bin/circ/fp\_ieee\_sqr\_42.aby

new file: bin/circ/fp\_ieee\_sqr\_64.aby

new file: bin/circ/fp\_ieee\_sqrt\_32.aby

new file: bin/circ/fp\_ieee\_sqrt\_42.aby

new file: bin/circ/fp\_ieee\_sqrt\_64.aby

new file: bin/circ/fp\_ieee\_sub\_32.aby

new file: bin/circ/fp\_ieee\_sub\_42.aby

new file: bin/circ/fp\_ieee\_sub\_64.aby

new file: bin/circ/fp\_nostatus\_add\_32.aby

new file: bin/circ/fp\_nostatus\_add\_42.aby

new file: bin/circ/fp\_nostatus\_add\_64.aby

new file: bin/circ/fp\_nostatus\_cmp\_32.aby

new file: bin/circ/fp\_nostatus\_cmp\_42.aby

new file: bin/circ/fp\_nostatus\_cmp\_64.aby

new file: bin/circ/fp\_nostatus\_div\_32.aby

new file: bin/circ/fp\_nostatus\_div\_42.aby

new file: bin/circ/fp\_nostatus\_div\_64.aby

new file: bin/circ/fp\_nostatus\_exp2\_32.aby

new file: bin/circ/fp\_nostatus\_exp2\_42.aby

new file: bin/circ/fp\_nostatus\_exp2\_64.aby

new file: bin/circ/fp\_nostatus\_exp\_32.aby

new file: bin/circ/fp\_nostatus\_exp\_42.aby

new file: bin/circ/fp\_nostatus\_ln\_32.aby

new file: bin/circ/fp\_nostatus\_ln\_42.aby

new file: bin/circ/fp\_nostatus\_ln\_64.aby

new file: bin/circ/fp\_nostatus\_log2\_32.aby

new file: bin/circ/fp\_nostatus\_log2\_42.aby

new file: bin/circ/fp\_nostatus\_log2\_64.aby

new file: bin/circ/fp\_nostatus\_mult\_32.aby

new file: bin/circ/fp\_nostatus\_mult\_42.aby

new file: bin/circ/fp\_nostatus\_mult\_64.aby

new file: bin/circ/fp\_nostatus\_sqr\_32.aby

new file: bin/circ/fp\_nostatus\_sqr\_42.aby

new file: bin/circ/fp\_nostatus\_sqr\_64.aby

new file: bin/circ/fp\_nostatus\_sqrt\_32.aby

new file: bin/circ/fp\_nostatus\_sqrt\_42.aby

new file: bin/circ/fp\_nostatus\_sqrt\_64.aby

new file: bin/circ/fp\_nostatus\_sub\_32.aby

new file: bin/circ/fp\_nostatus\_sub\_42.aby

new file: bin/circ/fp\_nostatus\_sub\_64.aby

new file: bin/circ/int\_div\_16.aby

new file: bin/circ/int\_div\_32.aby

new file: bin/circ/int\_div\_64.aby

new file: bin/circ/int\_div\_8.aby

new file: bin/circ/rc\_matrix16\_16.aby

new file: bin/circ/rc\_matrix32\_32.aby

new file: bin/circ/rc\_matrix\_16.aby

new file: bin/circ/rc\_matrix\_32.aby

new file: bin/circ/sin\_16.aby

new file: bin/circ/sin\_32.aby

new file: bin/uc/adder\_circ.txt

new file: bin/uc/adder\_prog.txt

new file: bin/uc/dummy\_circ.txt

new file: bin/uc/dummy\_prog.txt

new file: cmake/ABYConfig.cmake.in

new file: cmake/FindGMP.cmake

new file: cmake/FindGMPXX.cmake

new file: runtest\_scr.sh

new file: src/abycore/ABY\_utils/ABYconstants.h

new file: src/abycore/ABY\_utils/convtypes.h

new file: src/abycore/ABY\_utils/yaokey.h

new file: src/abycore/CMakeLists.txt

new file: src/abycore/DGK/dgkparty.cpp

new file: src/abycore/DGK/dgkparty.h

new file: src/abycore/DJN/djnparty.cpp

new file: src/abycore/DJN/djnparty.h

new file: src/abycore/aby/abyparty.cpp

new file: src/abycore/aby/abyparty.h

new file: src/abycore/aby/abysetup.cpp

new file: src/abycore/aby/abysetup.h

new file: src/abycore/circuit/abycircuit.cpp

new file: src/abycore/circuit/abycircuit.h

new file: src/abycore/circuit/arithmeticcircuits.cpp

new file: src/abycore/circuit/arithmeticcircuits.h

new file: src/abycore/circuit/booleancircuits.cpp

new file: src/abycore/circuit/booleancircuits.h

new file: src/abycore/circuit/circuit.cpp

new file: src/abycore/circuit/circuit.h

new file: src/abycore/circuit/share.cpp

new file: src/abycore/circuit/share.h

new file: src/abycore/ot/.gitignore

new file: src/abycore/sharing/arithsharing.cpp

new file: src/abycore/sharing/arithsharing.h

new file: src/abycore/sharing/boolsharing.cpp

new file: src/abycore/sharing/boolsharing.h

new file: src/abycore/sharing/sharing.cpp

new file: src/abycore/sharing/sharing.h

new file: src/abycore/sharing/splut.cpp

new file: src/abycore/sharing/splut.h

new file: src/abycore/sharing/yaoclientsharing.cpp

new file: src/abycore/sharing/yaoclientsharing.h

new file: src/abycore/sharing/yaoserversharing.cpp

new file: src/abycore/sharing/yaoserversharing.h

new file: src/abycore/sharing/yaosharing.cpp

new file: src/abycore/sharing/yaosharing.h

new file: src/examples/CMakeLists.txt

new file: src/examples/aes/CMakeLists.txt

new file: src/examples/aes/aes\_test.cpp

new file: src/examples/aes/common/aescircuit.cpp

new file: src/examples/aes/common/aescircuit.h

new file: src/examples/bench\_operations/CMakeLists.txt

new file: src/examples/bench\_operations/bench\_operations.cpp

new file: src/examples/euclidean\_distance/CMakeLists.txt

new file: src/examples/euclidean\_distance/common/euclidean\_dist.cpp

new file: src/examples/euclidean\_distance/common/euclidean\_dist.h

new file: src/examples/euclidean\_distance/euclidean\_distance\_test.cpp

new file: src/examples/float/CMakeLists.txt

new file: src/examples/float/abyfloat.cpp

new file: src/examples/innerproduct/CMakeLists.txt

new file: src/examples/innerproduct/common/innerproduct.cpp

new file: src/examples/innerproduct/common/innerproduct.h

new file: src/examples/innerproduct/innerproduct\_test.cpp

new file: src/examples/lowmc/CMakeLists.txt

new file: src/examples/lowmc/common/lowmccircuit.cpp

new file: src/examples/lowmc/common/lowmccircuit.h

new file: src/examples/lowmc/lowmc.cpp

new file: src/examples/millionaire\_prob/CMakeLists.txt

new file: src/examples/millionaire\_prob/common/millionaire\_prob.cpp

new file: src/examples/millionaire\_prob/common/millionaire\_prob.h

new file: src/examples/millionaire\_prob/millionaire\_prob\_test.cpp

new file: src/examples/min-euclidean-dist/CMakeLists.txt

new file: src/examples/min-euclidean-dist/common/min-euclidean-dist-circuit.cpp

new file: src/examples/min-euclidean-dist/common/min-euclidean-dist-circuit.h

new file: src/examples/min-euclidean-dist/min-euclidean-dist.cpp

new file: src/examples/psi\_phasing/CMakeLists.txt

new file: src/examples/psi\_phasing/common/hashing/cuckoo.cpp

new file: src/examples/psi\_phasing/common/hashing/cuckoo.h

new file: src/examples/psi\_phasing/common/hashing/hashing\_util.h

new file: src/examples/psi\_phasing/common/hashing/simple\_hashing.cpp

new file: src/examples/psi\_phasing/common/hashing/simple\_hashing.h

new file: src/examples/psi\_phasing/common/hashing\_includes.h

new file: src/examples/psi\_phasing/common/phasing\_circuit.cpp

new file: src/examples/psi\_phasing/common/phasing\_circuit.h

new file: src/examples/psi\_phasing/psi\_phasing.cpp

new file: src/examples/psi\_scs/CMakeLists.txt

new file: src/examples/psi\_scs/common/WaksmanPermutation.cpp

new file: src/examples/psi\_scs/common/WaksmanPermutation.h

new file: src/examples/psi\_scs/common/sort\_compare\_shuffle.cpp

new file: src/examples/psi\_scs/common/sort\_compare\_shuffle.h

new file: src/examples/psi\_scs/psi\_scs.cpp

new file: src/examples/sha1/CMakeLists.txt

new file: src/examples/sha1/common/sha1\_circuit.cpp

new file: src/examples/sha1/common/sha1\_circuit.h

new file: src/examples/sha1/sha1\_test.cpp

new file: src/examples/threshold\_euclidean\_dist\_2d\_simd/CMakeLists.txt

new file: src/examples/threshold\_euclidean\_dist\_2d\_simd/common/threshold-euclidean-dist.cpp

new file: src/examples/threshold\_euclidean\_dist\_2d\_simd/common/threshold-euclidean-dist.h

new file: src/examples/threshold\_euclidean\_dist\_2d\_simd/threshold-euclidean-dist.cpp

new file: src/examples/uc\_circuit/CMakeLists.txt

new file: src/examples/uc\_circuit/common/uc\_circuit.cpp

new file: src/examples/uc\_circuit/common/uc\_circuit.h

new file: src/examples/uc\_circuit/uc\_circuit\_test.cpp

new file: src/test/CMakeLists.txt

new file: src/test/abytest.cpp

new file: src/test/abytest.h

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ rm -rf \*

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ ls

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git status

On branch master

Changes to be committed:

(use "git reset HEAD <file>..." to unstage)

new file: .gitignore

new file: .gitmodules

new file: .travis.yml

new file: CMakeLists.txt

new file: Doxyfile

new file: LICENSE

new file: bin/.gitignore

new file: bin/circ/circuitformat.md

new file: bin/circ/cos\_16.aby

new file: bin/circ/cos\_32.aby

new file: bin/circ/cs\_matrix16\_16.aby

new file: bin/circ/cs\_matrix32\_32.aby

new file: bin/circ/cs\_matrix\_16.aby

new file: bin/circ/cs\_matrix\_32.aby

new file: bin/circ/fp\_ieee\_add\_32.aby

new file: bin/circ/fp\_ieee\_add\_42.aby

new file: bin/circ/fp\_ieee\_add\_64.aby

new file: bin/circ/fp\_ieee\_cos\_32.aby

new file: bin/circ/fp\_ieee\_cos\_42.aby

new file: bin/circ/fp\_ieee\_div\_32.aby

new file: bin/circ/fp\_ieee\_div\_42.aby

new file: bin/circ/fp\_ieee\_div\_64.aby

new file: bin/circ/fp\_ieee\_mult\_32.aby

new file: bin/circ/fp\_ieee\_mult\_42.aby

new file: bin/circ/fp\_ieee\_mult\_64.aby

new file: bin/circ/fp\_ieee\_sin\_32.aby

new file: bin/circ/fp\_ieee\_sin\_42.aby

new file: bin/circ/fp\_ieee\_sqr\_32.aby

new file: bin/circ/fp\_ieee\_sqr\_42.aby

new file: bin/circ/fp\_ieee\_sqr\_64.aby

new file: bin/circ/fp\_ieee\_sqrt\_32.aby

new file: bin/circ/fp\_ieee\_sqrt\_42.aby

new file: bin/circ/fp\_ieee\_sqrt\_64.aby

new file: bin/circ/fp\_ieee\_sub\_32.aby

new file: bin/circ/fp\_ieee\_sub\_42.aby

new file: bin/circ/fp\_ieee\_sub\_64.aby

new file: bin/circ/fp\_nostatus\_add\_32.aby

new file: bin/circ/fp\_nostatus\_add\_42.aby

new file: bin/circ/fp\_nostatus\_add\_64.aby

new file: bin/circ/fp\_nostatus\_cmp\_32.aby

new file: bin/circ/fp\_nostatus\_cmp\_42.aby

new file: bin/circ/fp\_nostatus\_cmp\_64.aby

new file: bin/circ/fp\_nostatus\_div\_32.aby

new file: bin/circ/fp\_nostatus\_div\_42.aby

new file: bin/circ/fp\_nostatus\_div\_64.aby

new file: bin/circ/fp\_nostatus\_exp2\_32.aby

new file: bin/circ/fp\_nostatus\_exp2\_42.aby

new file: bin/circ/fp\_nostatus\_exp2\_64.aby

new file: bin/circ/fp\_nostatus\_exp\_32.aby

new file: bin/circ/fp\_nostatus\_exp\_42.aby

new file: bin/circ/fp\_nostatus\_ln\_32.aby

new file: bin/circ/fp\_nostatus\_ln\_42.aby

new file: bin/circ/fp\_nostatus\_ln\_64.aby

new file: bin/circ/fp\_nostatus\_log2\_32.aby

new file: bin/circ/fp\_nostatus\_log2\_42.aby

new file: bin/circ/fp\_nostatus\_log2\_64.aby

new file: bin/circ/fp\_nostatus\_mult\_32.aby

new file: bin/circ/fp\_nostatus\_mult\_42.aby

new file: bin/circ/fp\_nostatus\_mult\_64.aby

new file: bin/circ/fp\_nostatus\_sqr\_32.aby

new file: bin/circ/fp\_nostatus\_sqr\_42.aby

new file: bin/circ/fp\_nostatus\_sqr\_64.aby

new file: bin/circ/fp\_nostatus\_sqrt\_32.aby

new file: bin/circ/fp\_nostatus\_sqrt\_42.aby

new file: bin/circ/fp\_nostatus\_sqrt\_64.aby

new file: bin/circ/fp\_nostatus\_sub\_32.aby

new file: bin/circ/fp\_nostatus\_sub\_42.aby

new file: bin/circ/fp\_nostatus\_sub\_64.aby

new file: bin/circ/int\_div\_16.aby

new file: bin/circ/int\_div\_32.aby

new file: bin/circ/int\_div\_64.aby

new file: bin/circ/int\_div\_8.aby

new file: bin/circ/rc\_matrix16\_16.aby

new file: bin/circ/rc\_matrix32\_32.aby

new file: bin/circ/rc\_matrix\_16.aby

new file: bin/circ/rc\_matrix\_32.aby

new file: bin/circ/sin\_16.aby

new file: bin/circ/sin\_32.aby

new file: bin/uc/adder\_circ.txt

new file: bin/uc/adder\_prog.txt

new file: bin/uc/dummy\_circ.txt

new file: bin/uc/dummy\_prog.txt

new file: cmake/ABYConfig.cmake.in

new file: cmake/FindGMP.cmake

new file: cmake/FindGMPXX.cmake

new file: runtest\_scr.sh

new file: src/abycore/ABY\_utils/ABYconstants.h

new file: src/abycore/ABY\_utils/convtypes.h

new file: src/abycore/ABY\_utils/yaokey.h

new file: src/abycore/CMakeLists.txt

new file: src/abycore/DGK/dgkparty.cpp

new file: src/abycore/DGK/dgkparty.h

new file: src/abycore/DJN/djnparty.cpp

new file: src/abycore/DJN/djnparty.h

new file: src/abycore/aby/abyparty.cpp

new file: src/abycore/aby/abyparty.h

new file: src/abycore/aby/abysetup.cpp

new file: src/abycore/aby/abysetup.h

new file: src/abycore/circuit/abycircuit.cpp

new file: src/abycore/circuit/abycircuit.h

new file: src/abycore/circuit/arithmeticcircuits.cpp

new file: src/abycore/circuit/arithmeticcircuits.h

new file: src/abycore/circuit/booleancircuits.cpp

new file: src/abycore/circuit/booleancircuits.h

new file: src/abycore/circuit/circuit.cpp

new file: src/abycore/circuit/circuit.h

new file: src/abycore/circuit/share.cpp

new file: src/abycore/circuit/share.h

new file: src/abycore/ot/.gitignore

new file: src/abycore/sharing/arithsharing.cpp

new file: src/abycore/sharing/arithsharing.h

new file: src/abycore/sharing/boolsharing.cpp

new file: src/abycore/sharing/boolsharing.h

new file: src/abycore/sharing/sharing.cpp

new file: src/abycore/sharing/sharing.h

new file: src/abycore/sharing/splut.cpp

new file: src/abycore/sharing/splut.h

new file: src/abycore/sharing/yaoclientsharing.cpp

new file: src/abycore/sharing/yaoclientsharing.h

new file: src/abycore/sharing/yaoserversharing.cpp

new file: src/abycore/sharing/yaoserversharing.h

new file: src/abycore/sharing/yaosharing.cpp

new file: src/abycore/sharing/yaosharing.h

new file: src/examples/CMakeLists.txt

new file: src/examples/aes/CMakeLists.txt

new file: src/examples/aes/aes\_test.cpp

new file: src/examples/aes/common/aescircuit.cpp

new file: src/examples/aes/common/aescircuit.h

new file: src/examples/bench\_operations/CMakeLists.txt

new file: src/examples/bench\_operations/bench\_operations.cpp

new file: src/examples/euclidean\_distance/CMakeLists.txt

new file: src/examples/euclidean\_distance/common/euclidean\_dist.cpp

new file: src/examples/euclidean\_distance/common/euclidean\_dist.h

new file: src/examples/euclidean\_distance/euclidean\_distance\_test.cpp

new file: src/examples/float/CMakeLists.txt

new file: src/examples/float/abyfloat.cpp

new file: src/examples/innerproduct/CMakeLists.txt

new file: src/examples/innerproduct/common/innerproduct.cpp

new file: src/examples/innerproduct/common/innerproduct.h

new file: src/examples/innerproduct/innerproduct\_test.cpp

new file: src/examples/lowmc/CMakeLists.txt

new file: src/examples/lowmc/common/lowmccircuit.cpp

new file: src/examples/lowmc/common/lowmccircuit.h

new file: src/examples/lowmc/lowmc.cpp

new file: src/examples/millionaire\_prob/CMakeLists.txt

new file: src/examples/millionaire\_prob/common/millionaire\_prob.cpp

new file: src/examples/millionaire\_prob/common/millionaire\_prob.h

new file: src/examples/millionaire\_prob/millionaire\_prob\_test.cpp

new file: src/examples/min-euclidean-dist/CMakeLists.txt

new file: src/examples/min-euclidean-dist/common/min-euclidean-dist-circuit.cpp

new file: src/examples/min-euclidean-dist/common/min-euclidean-dist-circuit.h

new file: src/examples/min-euclidean-dist/min-euclidean-dist.cpp

new file: src/examples/psi\_phasing/CMakeLists.txt

new file: src/examples/psi\_phasing/common/hashing/cuckoo.cpp

new file: src/examples/psi\_phasing/common/hashing/cuckoo.h

new file: src/examples/psi\_phasing/common/hashing/hashing\_util.h

new file: src/examples/psi\_phasing/common/hashing/simple\_hashing.cpp

new file: src/examples/psi\_phasing/common/hashing/simple\_hashing.h

new file: src/examples/psi\_phasing/common/hashing\_includes.h

new file: src/examples/psi\_phasing/common/phasing\_circuit.cpp

new file: src/examples/psi\_phasing/common/phasing\_circuit.h

new file: src/examples/psi\_phasing/psi\_phasing.cpp

new file: src/examples/psi\_scs/CMakeLists.txt

new file: src/examples/psi\_scs/common/WaksmanPermutation.cpp

new file: src/examples/psi\_scs/common/WaksmanPermutation.h

new file: src/examples/psi\_scs/common/sort\_compare\_shuffle.cpp

new file: src/examples/psi\_scs/common/sort\_compare\_shuffle.h

new file: src/examples/psi\_scs/psi\_scs.cpp

new file: src/examples/sha1/CMakeLists.txt

new file: src/examples/sha1/common/sha1\_circuit.cpp

new file: src/examples/sha1/common/sha1\_circuit.h

new file: src/examples/sha1/sha1\_test.cpp

new file: src/examples/threshold\_euclidean\_dist\_2d\_simd/CMakeLists.txt

new file: src/examples/threshold\_euclidean\_dist\_2d\_simd/common/threshold-euclidean-dist.cpp

new file: src/examples/threshold\_euclidean\_dist\_2d\_simd/common/threshold-euclidean-dist.h

new file: src/examples/threshold\_euclidean\_dist\_2d\_simd/threshold-euclidean-dist.cpp

new file: src/examples/uc\_circuit/CMakeLists.txt

new file: src/examples/uc\_circuit/common/uc\_circuit.cpp

new file: src/examples/uc\_circuit/common/uc\_circuit.h

new file: src/examples/uc\_circuit/uc\_circuit\_test.cpp

new file: src/test/CMakeLists.txt

new file: src/test/abytest.cpp

new file: src/test/abytest.h

Changes not staged for commit:

(use "git add/rm <file>..." to update what will be committed)

(use "git checkout -- <file>..." to discard changes in working directory)

deleted: CMakeLists.txt

deleted: Doxyfile

deleted: LICENSE

deleted: README.md

deleted: bin/.gitignore

deleted: bin/circ/circuitformat.md

deleted: bin/circ/cos\_16.aby

deleted: bin/circ/cos\_32.aby

deleted: bin/circ/cs\_matrix16\_16.aby

deleted: bin/circ/cs\_matrix32\_32.aby

deleted: bin/circ/cs\_matrix\_16.aby

deleted: bin/circ/cs\_matrix\_32.aby

deleted: bin/circ/fp\_ieee\_add\_32.aby

deleted: bin/circ/fp\_ieee\_add\_42.aby

deleted: bin/circ/fp\_ieee\_add\_64.aby

deleted: bin/circ/fp\_ieee\_cos\_32.aby

deleted: bin/circ/fp\_ieee\_cos\_42.aby

deleted: bin/circ/fp\_ieee\_div\_32.aby

deleted: bin/circ/fp\_ieee\_div\_42.aby

deleted: bin/circ/fp\_ieee\_div\_64.aby

deleted: bin/circ/fp\_ieee\_mult\_32.aby

deleted: bin/circ/fp\_ieee\_mult\_42.aby

deleted: bin/circ/fp\_ieee\_mult\_64.aby

deleted: bin/circ/fp\_ieee\_sin\_32.aby

deleted: bin/circ/fp\_ieee\_sin\_42.aby

deleted: bin/circ/fp\_ieee\_sqr\_32.aby

deleted: bin/circ/fp\_ieee\_sqr\_42.aby

deleted: bin/circ/fp\_ieee\_sqr\_64.aby

deleted: bin/circ/fp\_ieee\_sqrt\_32.aby

deleted: bin/circ/fp\_ieee\_sqrt\_42.aby

deleted: bin/circ/fp\_ieee\_sqrt\_64.aby

deleted: bin/circ/fp\_ieee\_sub\_32.aby

deleted: bin/circ/fp\_ieee\_sub\_42.aby

deleted: bin/circ/fp\_ieee\_sub\_64.aby

deleted: bin/circ/fp\_nostatus\_add\_32.aby

deleted: bin/circ/fp\_nostatus\_add\_42.aby

deleted: bin/circ/fp\_nostatus\_add\_64.aby

deleted: bin/circ/fp\_nostatus\_cmp\_32.aby

deleted: bin/circ/fp\_nostatus\_cmp\_42.aby

deleted: bin/circ/fp\_nostatus\_cmp\_64.aby

deleted: bin/circ/fp\_nostatus\_div\_32.aby

deleted: bin/circ/fp\_nostatus\_div\_42.aby

deleted: bin/circ/fp\_nostatus\_div\_64.aby

deleted: bin/circ/fp\_nostatus\_exp2\_32.aby

deleted: bin/circ/fp\_nostatus\_exp2\_42.aby

deleted: bin/circ/fp\_nostatus\_exp2\_64.aby

deleted: bin/circ/fp\_nostatus\_exp\_32.aby

deleted: bin/circ/fp\_nostatus\_exp\_42.aby

deleted: bin/circ/fp\_nostatus\_ln\_32.aby

deleted: bin/circ/fp\_nostatus\_ln\_42.aby

deleted: bin/circ/fp\_nostatus\_ln\_64.aby

deleted: bin/circ/fp\_nostatus\_log2\_32.aby

deleted: bin/circ/fp\_nostatus\_log2\_42.aby

deleted: bin/circ/fp\_nostatus\_log2\_64.aby

deleted: bin/circ/fp\_nostatus\_mult\_32.aby

deleted: bin/circ/fp\_nostatus\_mult\_42.aby

deleted: bin/circ/fp\_nostatus\_mult\_64.aby

deleted: bin/circ/fp\_nostatus\_sqr\_32.aby

deleted: bin/circ/fp\_nostatus\_sqr\_42.aby

deleted: bin/circ/fp\_nostatus\_sqr\_64.aby

deleted: bin/circ/fp\_nostatus\_sqrt\_32.aby

deleted: bin/circ/fp\_nostatus\_sqrt\_42.aby

deleted: bin/circ/fp\_nostatus\_sqrt\_64.aby

deleted: bin/circ/fp\_nostatus\_sub\_32.aby

deleted: bin/circ/fp\_nostatus\_sub\_42.aby

deleted: bin/circ/fp\_nostatus\_sub\_64.aby

deleted: bin/circ/int\_div\_16.aby

deleted: bin/circ/int\_div\_32.aby

deleted: bin/circ/int\_div\_64.aby

deleted: bin/circ/int\_div\_8.aby

deleted: bin/circ/rc\_matrix16\_16.aby

deleted: bin/circ/rc\_matrix32\_32.aby

deleted: bin/circ/rc\_matrix\_16.aby

deleted: bin/circ/rc\_matrix\_32.aby

deleted: bin/circ/sin\_16.aby

deleted: bin/circ/sin\_32.aby

deleted: bin/uc/adder\_circ.txt

deleted: bin/uc/adder\_prog.txt

deleted: bin/uc/dummy\_circ.txt

deleted: bin/uc/dummy\_prog.txt

deleted: cmake/ABYConfig.cmake.in

deleted: cmake/FindGMP.cmake

deleted: cmake/FindGMPXX.cmake

deleted: runtest\_scr.sh

deleted: src/abycore/ABY\_utils/ABYconstants.h

deleted: src/abycore/ABY\_utils/convtypes.h

deleted: src/abycore/ABY\_utils/yaokey.h

deleted: src/abycore/CMakeLists.txt

deleted: src/abycore/DGK/dgkparty.cpp

deleted: src/abycore/DGK/dgkparty.h

deleted: src/abycore/DJN/djnparty.cpp

deleted: src/abycore/DJN/djnparty.h

deleted: src/abycore/aby/abyparty.cpp

deleted: src/abycore/aby/abyparty.h

deleted: src/abycore/aby/abysetup.cpp

deleted: src/abycore/aby/abysetup.h

deleted: src/abycore/circuit/abycircuit.cpp

deleted: src/abycore/circuit/abycircuit.h

deleted: src/abycore/circuit/arithmeticcircuits.cpp

deleted: src/abycore/circuit/arithmeticcircuits.h

deleted: src/abycore/circuit/booleancircuits.cpp

deleted: src/abycore/circuit/booleancircuits.h

deleted: src/abycore/circuit/circuit.cpp

deleted: src/abycore/circuit/circuit.h

deleted: src/abycore/circuit/share.cpp

deleted: src/abycore/circuit/share.h

deleted: src/abycore/ot/.gitignore

deleted: src/abycore/sharing/arithsharing.cpp

deleted: src/abycore/sharing/arithsharing.h

deleted: src/abycore/sharing/boolsharing.cpp

deleted: src/abycore/sharing/boolsharing.h

deleted: src/abycore/sharing/sharing.cpp

deleted: src/abycore/sharing/sharing.h

deleted: src/abycore/sharing/splut.cpp

deleted: src/abycore/sharing/splut.h

deleted: src/abycore/sharing/yaoclientsharing.cpp

deleted: src/abycore/sharing/yaoclientsharing.h

deleted: src/abycore/sharing/yaoserversharing.cpp

deleted: src/abycore/sharing/yaoserversharing.h

deleted: src/abycore/sharing/yaosharing.cpp

deleted: src/abycore/sharing/yaosharing.h

deleted: src/examples/CMakeLists.txt

deleted: src/examples/aes/CMakeLists.txt

deleted: src/examples/aes/aes\_test.cpp

deleted: src/examples/aes/common/aescircuit.cpp

deleted: src/examples/aes/common/aescircuit.h

deleted: src/examples/bench\_operations/CMakeLists.txt

deleted: src/examples/bench\_operations/bench\_operations.cpp

deleted: src/examples/euclidean\_distance/CMakeLists.txt

deleted: src/examples/euclidean\_distance/common/euclidean\_dist.cpp

deleted: src/examples/euclidean\_distance/common/euclidean\_dist.h

deleted: src/examples/euclidean\_distance/euclidean\_distance\_test.cpp

deleted: src/examples/float/CMakeLists.txt

deleted: src/examples/float/abyfloat.cpp

deleted: src/examples/innerproduct/CMakeLists.txt

deleted: src/examples/innerproduct/common/innerproduct.cpp

deleted: src/examples/innerproduct/common/innerproduct.h

deleted: src/examples/innerproduct/innerproduct\_test.cpp

deleted: src/examples/lowmc/CMakeLists.txt

deleted: src/examples/lowmc/common/lowmccircuit.cpp

deleted: src/examples/lowmc/common/lowmccircuit.h

deleted: src/examples/lowmc/lowmc.cpp

deleted: src/examples/millionaire\_prob/CMakeLists.txt

deleted: src/examples/millionaire\_prob/common/millionaire\_prob.cpp

deleted: src/examples/millionaire\_prob/common/millionaire\_prob.h

deleted: src/examples/millionaire\_prob/millionaire\_prob\_test.cpp

deleted: src/examples/min-euclidean-dist/CMakeLists.txt

deleted: src/examples/min-euclidean-dist/common/min-euclidean-dist-circuit.cpp

deleted: src/examples/min-euclidean-dist/common/min-euclidean-dist-circuit.h

deleted: src/examples/min-euclidean-dist/min-euclidean-dist.cpp

deleted: src/examples/psi\_phasing/CMakeLists.txt

deleted: src/examples/psi\_phasing/common/hashing/cuckoo.cpp

deleted: src/examples/psi\_phasing/common/hashing/cuckoo.h

deleted: src/examples/psi\_phasing/common/hashing/hashing\_util.h

deleted: src/examples/psi\_phasing/common/hashing/simple\_hashing.cpp

deleted: src/examples/psi\_phasing/common/hashing/simple\_hashing.h

deleted: src/examples/psi\_phasing/common/hashing\_includes.h

deleted: src/examples/psi\_phasing/common/phasing\_circuit.cpp

deleted: src/examples/psi\_phasing/common/phasing\_circuit.h

deleted: src/examples/psi\_phasing/psi\_phasing.cpp

deleted: src/examples/psi\_scs/CMakeLists.txt

deleted: src/examples/psi\_scs/common/WaksmanPermutation.cpp

deleted: src/examples/psi\_scs/common/WaksmanPermutation.h

deleted: src/examples/psi\_scs/common/sort\_compare\_shuffle.cpp

deleted: src/examples/psi\_scs/common/sort\_compare\_shuffle.h

deleted: src/examples/psi\_scs/psi\_scs.cpp

deleted: src/examples/sha1/CMakeLists.txt

deleted: src/examples/sha1/common/sha1\_circuit.cpp

deleted: src/examples/sha1/common/sha1\_circuit.h

deleted: src/examples/sha1/sha1\_test.cpp

deleted: src/examples/threshold\_euclidean\_dist\_2d\_simd/CMakeLists.txt

deleted: src/examples/threshold\_euclidean\_dist\_2d\_simd/common/threshold-euclidean-dist.cpp

deleted: src/examples/threshold\_euclidean\_dist\_2d\_simd/common/threshold-euclidean-dist.h

deleted: src/examples/threshold\_euclidean\_dist\_2d\_simd/threshold-euclidean-dist.cpp

deleted: src/examples/uc\_circuit/CMakeLists.txt

deleted: src/examples/uc\_circuit/common/uc\_circuit.cpp

deleted: src/examples/uc\_circuit/common/uc\_circuit.h

deleted: src/examples/uc\_circuit/uc\_circuit\_test.cpp

deleted: src/test/CMakeLists.txt

deleted: src/test/abytest.cpp

deleted: src/test/abytest.h

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ cd ..

to@toddzhang-NB01:/mnt/d$ rm -rf encryptogroup-ABY/

to@toddzhang-NB01:/mnt/d$ git clone https://github.com/zzzztao/encryptogroup-ABY.git

Cloning into 'encryptogroup-ABY'...

Username for 'https://github.com': zzzztao

Password for 'https://zzzztao@github.com':

remote: Enumerating objects: 3, done.

remote: Counting objects: 100% (3/3), done.

remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0

Unpacking objects: 100% (3/3), done.

to@toddzhang-NB01:/mnt/d$ cd encryptogroup-ABY/

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git status

On branch master

Your branch is up to date with 'origin/master'.

nothing to commit, working tree clean

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ ls

README.md

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git status

On branch master

Your branch is up to date with 'origin/master'.

Changes not staged for commit:

(use "git add <file>..." to update what will be committed)

(use "git checkout -- <file>..." to discard changes in working directory)

modified: README.md

Untracked files:

(use "git add <file>..." to include in what will be committed)

.gitignore

.gitmodules

.travis.yml

CMakeLists.txt

Doxyfile

LICENSE

bin/

cmake/

runtest\_scr.sh

src/

no changes added to commit (use "git add" and/or "git commit -a")

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ ga .

ga: command not found

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git add .

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git commit "init code"

error: pathspec 'init code' did not match any file(s) known to git.

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git status

On branch master

Your branch is up to date with 'origin/master'.

Changes to be committed:

(use "git reset HEAD <file>..." to unstage)

new file: .gitignore

new file: .gitmodules

new file: .travis.yml

new file: CMakeLists.txt

new file: Doxyfile

new file: LICENSE

modified: README.md

new file: bin/.gitignore

new file: bin/circ/circuitformat.md

new file: bin/circ/cos\_16.aby

new file: bin/circ/cos\_32.aby

new file: bin/circ/cs\_matrix16\_16.aby

new file: bin/circ/cs\_matrix32\_32.aby

new file: bin/circ/cs\_matrix\_16.aby

new file: bin/circ/cs\_matrix\_32.aby

new file: bin/circ/fp\_ieee\_add\_32.aby

new file: bin/circ/fp\_ieee\_add\_42.aby

new file: bin/circ/fp\_ieee\_add\_64.aby

new file: bin/circ/fp\_ieee\_cos\_32.aby

new file: bin/circ/fp\_ieee\_cos\_42.aby

new file: bin/circ/fp\_ieee\_div\_32.aby

new file: bin/circ/fp\_ieee\_div\_42.aby

new file: bin/circ/fp\_ieee\_div\_64.aby

new file: bin/circ/fp\_ieee\_mult\_32.aby

new file: bin/circ/fp\_ieee\_mult\_42.aby

new file: bin/circ/fp\_ieee\_mult\_64.aby

new file: bin/circ/fp\_ieee\_sin\_32.aby

new file: bin/circ/fp\_ieee\_sin\_42.aby

new file: bin/circ/fp\_ieee\_sqr\_32.aby

new file: bin/circ/fp\_ieee\_sqr\_42.aby

new file: bin/circ/fp\_ieee\_sqr\_64.aby

new file: bin/circ/fp\_ieee\_sqrt\_32.aby

new file: bin/circ/fp\_ieee\_sqrt\_42.aby

new file: bin/circ/fp\_ieee\_sqrt\_64.aby

new file: bin/circ/fp\_ieee\_sub\_32.aby

new file: bin/circ/fp\_ieee\_sub\_42.aby

new file: bin/circ/fp\_ieee\_sub\_64.aby

new file: bin/circ/fp\_nostatus\_add\_32.aby

new file: bin/circ/fp\_nostatus\_add\_42.aby

new file: bin/circ/fp\_nostatus\_add\_64.aby

new file: bin/circ/fp\_nostatus\_cmp\_32.aby

new file: bin/circ/fp\_nostatus\_cmp\_42.aby

new file: bin/circ/fp\_nostatus\_cmp\_64.aby

new file: bin/circ/fp\_nostatus\_div\_32.aby

new file: bin/circ/fp\_nostatus\_div\_42.aby

new file: bin/circ/fp\_nostatus\_div\_64.aby

new file: bin/circ/fp\_nostatus\_exp2\_32.aby

new file: bin/circ/fp\_nostatus\_exp2\_42.aby

new file: bin/circ/fp\_nostatus\_exp2\_64.aby

new file: bin/circ/fp\_nostatus\_exp\_32.aby

new file: bin/circ/fp\_nostatus\_exp\_42.aby

new file: bin/circ/fp\_nostatus\_ln\_32.aby

new file: bin/circ/fp\_nostatus\_ln\_42.aby

new file: bin/circ/fp\_nostatus\_ln\_64.aby

new file: bin/circ/fp\_nostatus\_log2\_32.aby

new file: bin/circ/fp\_nostatus\_log2\_42.aby

new file: bin/circ/fp\_nostatus\_log2\_64.aby

new file: bin/circ/fp\_nostatus\_mult\_32.aby

new file: bin/circ/fp\_nostatus\_mult\_42.aby

new file: bin/circ/fp\_nostatus\_mult\_64.aby

new file: bin/circ/fp\_nostatus\_sqr\_32.aby

new file: bin/circ/fp\_nostatus\_sqr\_42.aby

new file: bin/circ/fp\_nostatus\_sqr\_64.aby

new file: bin/circ/fp\_nostatus\_sqrt\_32.aby

new file: bin/circ/fp\_nostatus\_sqrt\_42.aby

new file: bin/circ/fp\_nostatus\_sqrt\_64.aby

new file: bin/circ/fp\_nostatus\_sub\_32.aby

new file: bin/circ/fp\_nostatus\_sub\_42.aby

new file: bin/circ/fp\_nostatus\_sub\_64.aby

new file: bin/circ/int\_div\_16.aby

new file: bin/circ/int\_div\_32.aby

new file: bin/circ/int\_div\_64.aby

new file: bin/circ/int\_div\_8.aby

new file: bin/circ/rc\_matrix16\_16.aby

new file: bin/circ/rc\_matrix32\_32.aby

new file: bin/circ/rc\_matrix\_16.aby

new file: bin/circ/rc\_matrix\_32.aby

new file: bin/circ/sin\_16.aby

new file: bin/circ/sin\_32.aby

new file: bin/uc/adder\_circ.txt

new file: bin/uc/adder\_prog.txt

new file: bin/uc/dummy\_circ.txt

new file: bin/uc/dummy\_prog.txt

new file: cmake/ABYConfig.cmake.in

new file: cmake/FindGMP.cmake

new file: cmake/FindGMPXX.cmake

new file: runtest\_scr.sh

new file: src/abycore/ABY\_utils/ABYconstants.h

new file: src/abycore/ABY\_utils/convtypes.h

new file: src/abycore/ABY\_utils/yaokey.h

new file: src/abycore/CMakeLists.txt

new file: src/abycore/DGK/dgkparty.cpp

new file: src/abycore/DGK/dgkparty.h

new file: src/abycore/DJN/djnparty.cpp

new file: src/abycore/DJN/djnparty.h

new file: src/abycore/aby/abyparty.cpp

new file: src/abycore/aby/abyparty.h

new file: src/abycore/aby/abysetup.cpp

new file: src/abycore/aby/abysetup.h

new file: src/abycore/circuit/abycircuit.cpp

new file: src/abycore/circuit/abycircuit.h

new file: src/abycore/circuit/arithmeticcircuits.cpp

new file: src/abycore/circuit/arithmeticcircuits.h

new file: src/abycore/circuit/booleancircuits.cpp

new file: src/abycore/circuit/booleancircuits.h

new file: src/abycore/circuit/circuit.cpp

new file: src/abycore/circuit/circuit.h

new file: src/abycore/circuit/share.cpp

new file: src/abycore/circuit/share.h

new file: src/abycore/ot/.gitignore

new file: src/abycore/sharing/arithsharing.cpp

new file: src/abycore/sharing/arithsharing.h

new file: src/abycore/sharing/boolsharing.cpp

new file: src/abycore/sharing/boolsharing.h

new file: src/abycore/sharing/sharing.cpp

new file: src/abycore/sharing/sharing.h

new file: src/abycore/sharing/splut.cpp

new file: src/abycore/sharing/splut.h

new file: src/abycore/sharing/yaoclientsharing.cpp

new file: src/abycore/sharing/yaoclientsharing.h

new file: src/abycore/sharing/yaoserversharing.cpp

new file: src/abycore/sharing/yaoserversharing.h

new file: src/abycore/sharing/yaosharing.cpp

new file: src/abycore/sharing/yaosharing.h

new file: src/examples/CMakeLists.txt

new file: src/examples/aes/CMakeLists.txt

new file: src/examples/aes/aes\_test.cpp

new file: src/examples/aes/common/aescircuit.cpp

new file: src/examples/aes/common/aescircuit.h

new file: src/examples/bench\_operations/CMakeLists.txt

new file: src/examples/bench\_operations/bench\_operations.cpp

new file: src/examples/euclidean\_distance/CMakeLists.txt

new file: src/examples/euclidean\_distance/common/euclidean\_dist.cpp

new file: src/examples/euclidean\_distance/common/euclidean\_dist.h

new file: src/examples/euclidean\_distance/euclidean\_distance\_test.cpp

new file: src/examples/float/CMakeLists.txt

new file: src/examples/float/abyfloat.cpp

new file: src/examples/innerproduct/CMakeLists.txt

new file: src/examples/innerproduct/common/innerproduct.cpp

new file: src/examples/innerproduct/common/innerproduct.h

new file: src/examples/innerproduct/innerproduct\_test.cpp

new file: src/examples/lowmc/CMakeLists.txt

new file: src/examples/lowmc/common/lowmccircuit.cpp

new file: src/examples/lowmc/common/lowmccircuit.h

new file: src/examples/lowmc/lowmc.cpp

new file: src/examples/millionaire\_prob/CMakeLists.txt

new file: src/examples/millionaire\_prob/common/millionaire\_prob.cpp

new file: src/examples/millionaire\_prob/common/millionaire\_prob.h

new file: src/examples/millionaire\_prob/millionaire\_prob\_test.cpp

new file: src/examples/min-euclidean-dist/CMakeLists.txt

new file: src/examples/min-euclidean-dist/common/min-euclidean-dist-circuit.cpp

new file: src/examples/min-euclidean-dist/common/min-euclidean-dist-circuit.h

new file: src/examples/min-euclidean-dist/min-euclidean-dist.cpp

new file: src/examples/psi\_phasing/CMakeLists.txt

new file: src/examples/psi\_phasing/common/hashing/cuckoo.cpp

new file: src/examples/psi\_phasing/common/hashing/cuckoo.h

new file: src/examples/psi\_phasing/common/hashing/hashing\_util.h

new file: src/examples/psi\_phasing/common/hashing/simple\_hashing.cpp

new file: src/examples/psi\_phasing/common/hashing/simple\_hashing.h

new file: src/examples/psi\_phasing/common/hashing\_includes.h

new file: src/examples/psi\_phasing/common/phasing\_circuit.cpp

new file: src/examples/psi\_phasing/common/phasing\_circuit.h

new file: src/examples/psi\_phasing/psi\_phasing.cpp

new file: src/examples/psi\_scs/CMakeLists.txt

new file: src/examples/psi\_scs/common/WaksmanPermutation.cpp

new file: src/examples/psi\_scs/common/WaksmanPermutation.h

new file: src/examples/psi\_scs/common/sort\_compare\_shuffle.cpp

new file: src/examples/psi\_scs/common/sort\_compare\_shuffle.h

new file: src/examples/psi\_scs/psi\_scs.cpp

new file: src/examples/sha1/CMakeLists.txt

new file: src/examples/sha1/common/sha1\_circuit.cpp

new file: src/examples/sha1/common/sha1\_circuit.h

new file: src/examples/sha1/sha1\_test.cpp

new file: src/examples/threshold\_euclidean\_dist\_2d\_simd/CMakeLists.txt

new file: src/examples/threshold\_euclidean\_dist\_2d\_simd/common/threshold-euclidean-dist.cpp

new file: src/examples/threshold\_euclidean\_dist\_2d\_simd/common/threshold-euclidean-dist.h

new file: src/examples/threshold\_euclidean\_dist\_2d\_simd/threshold-euclidean-dist.cpp

new file: src/examples/uc\_circuit/CMakeLists.txt

new file: src/examples/uc\_circuit/common/uc\_circuit.cpp

new file: src/examples/uc\_circuit/common/uc\_circuit.h

new file: src/examples/uc\_circuit/uc\_circuit\_test.cpp

new file: src/test/CMakeLists.txt

new file: src/test/abytest.cpp

new file: src/test/abytest.h

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git status

On branch master

Your branch is up to date with 'origin/master'.

Changes to be committed:

(use "git reset HEAD <file>..." to unstage)

new file: .gitignore

new file: .gitmodules

new file: .travis.yml

new file: CMakeLists.txt

new file: Doxyfile

new file: LICENSE

modified: README.md

new file: bin/.gitignore

new file: bin/circ/circuitformat.md

new file: bin/circ/cos\_16.aby

new file: bin/circ/cos\_32.aby

new file: bin/circ/cs\_matrix16\_16.aby

new file: bin/circ/cs\_matrix32\_32.aby

new file: bin/circ/cs\_matrix\_16.aby

new file: bin/circ/cs\_matrix\_32.aby

new file: bin/circ/fp\_ieee\_add\_32.aby

new file: bin/circ/fp\_ieee\_add\_42.aby

new file: bin/circ/fp\_ieee\_add\_64.aby

new file: bin/circ/fp\_ieee\_cos\_32.aby

new file: bin/circ/fp\_ieee\_cos\_42.aby

new file: bin/circ/fp\_ieee\_div\_32.aby

new file: bin/circ/fp\_ieee\_div\_42.aby

new file: bin/circ/fp\_ieee\_div\_64.aby

new file: bin/circ/fp\_ieee\_mult\_32.aby

new file: bin/circ/fp\_ieee\_mult\_42.aby

new file: bin/circ/fp\_ieee\_mult\_64.aby

new file: bin/circ/fp\_ieee\_sin\_32.aby

new file: bin/circ/fp\_ieee\_sin\_42.aby

new file: bin/circ/fp\_ieee\_sqr\_32.aby

new file: bin/circ/fp\_ieee\_sqr\_42.aby

new file: bin/circ/fp\_ieee\_sqr\_64.aby

new file: bin/circ/fp\_ieee\_sqrt\_32.aby

new file: bin/circ/fp\_ieee\_sqrt\_42.aby

new file: bin/circ/fp\_ieee\_sqrt\_64.aby

new file: bin/circ/fp\_ieee\_sub\_32.aby

new file: bin/circ/fp\_ieee\_sub\_42.aby

new file: bin/circ/fp\_ieee\_sub\_64.aby

new file: bin/circ/fp\_nostatus\_add\_32.aby

new file: bin/circ/fp\_nostatus\_add\_42.aby

new file: bin/circ/fp\_nostatus\_add\_64.aby

new file: bin/circ/fp\_nostatus\_cmp\_32.aby

new file: bin/circ/fp\_nostatus\_cmp\_42.aby

new file: bin/circ/fp\_nostatus\_cmp\_64.aby

new file: bin/circ/fp\_nostatus\_div\_32.aby

new file: bin/circ/fp\_nostatus\_div\_42.aby

new file: bin/circ/fp\_nostatus\_div\_64.aby

new file: bin/circ/fp\_nostatus\_exp2\_32.aby

new file: bin/circ/fp\_nostatus\_exp2\_42.aby

new file: bin/circ/fp\_nostatus\_exp2\_64.aby

new file: bin/circ/fp\_nostatus\_exp\_32.aby

new file: bin/circ/fp\_nostatus\_exp\_42.aby

new file: bin/circ/fp\_nostatus\_ln\_32.aby

new file: bin/circ/fp\_nostatus\_ln\_42.aby

new file: bin/circ/fp\_nostatus\_ln\_64.aby

new file: bin/circ/fp\_nostatus\_log2\_32.aby

new file: bin/circ/fp\_nostatus\_log2\_42.aby

new file: bin/circ/fp\_nostatus\_log2\_64.aby

new file: bin/circ/fp\_nostatus\_mult\_32.aby

new file: bin/circ/fp\_nostatus\_mult\_42.aby

new file: bin/circ/fp\_nostatus\_mult\_64.aby

new file: bin/circ/fp\_nostatus\_sqr\_32.aby

new file: bin/circ/fp\_nostatus\_sqr\_42.aby

new file: bin/circ/fp\_nostatus\_sqr\_64.aby

new file: bin/circ/fp\_nostatus\_sqrt\_32.aby

new file: bin/circ/fp\_nostatus\_sqrt\_42.aby

new file: bin/circ/fp\_nostatus\_sqrt\_64.aby

new file: bin/circ/fp\_nostatus\_sub\_32.aby

new file: bin/circ/fp\_nostatus\_sub\_42.aby

new file: bin/circ/fp\_nostatus\_sub\_64.aby

new file: bin/circ/int\_div\_16.aby

new file: bin/circ/int\_div\_32.aby

new file: bin/circ/int\_div\_64.aby

new file: bin/circ/int\_div\_8.aby

new file: bin/circ/rc\_matrix16\_16.aby

new file: bin/circ/rc\_matrix32\_32.aby

new file: bin/circ/rc\_matrix\_16.aby

new file: bin/circ/rc\_matrix\_32.aby

new file: bin/circ/sin\_16.aby

new file: bin/circ/sin\_32.aby

new file: bin/uc/adder\_circ.txt

new file: bin/uc/adder\_prog.txt

new file: bin/uc/dummy\_circ.txt

new file: bin/uc/dummy\_prog.txt

new file: cmake/ABYConfig.cmake.in

new file: cmake/FindGMP.cmake

new file: cmake/FindGMPXX.cmake

new file: runtest\_scr.sh

new file: src/abycore/ABY\_utils/ABYconstants.h

new file: src/abycore/ABY\_utils/convtypes.h

new file: src/abycore/ABY\_utils/yaokey.h

new file: src/abycore/CMakeLists.txt

new file: src/abycore/DGK/dgkparty.cpp

new file: src/abycore/DGK/dgkparty.h

new file: src/abycore/DJN/djnparty.cpp

new file: src/abycore/DJN/djnparty.h

new file: src/abycore/aby/abyparty.cpp

new file: src/abycore/aby/abyparty.h

new file: src/abycore/aby/abysetup.cpp

new file: src/abycore/aby/abysetup.h

new file: src/abycore/circuit/abycircuit.cpp

new file: src/abycore/circuit/abycircuit.h

new file: src/abycore/circuit/arithmeticcircuits.cpp

new file: src/abycore/circuit/arithmeticcircuits.h

new file: src/abycore/circuit/booleancircuits.cpp

new file: src/abycore/circuit/booleancircuits.h

new file: src/abycore/circuit/circuit.cpp

new file: src/abycore/circuit/circuit.h

new file: src/abycore/circuit/share.cpp

new file: src/abycore/circuit/share.h

new file: src/abycore/ot/.gitignore

new file: src/abycore/sharing/arithsharing.cpp

new file: src/abycore/sharing/arithsharing.h

new file: src/abycore/sharing/boolsharing.cpp

new file: src/abycore/sharing/boolsharing.h

new file: src/abycore/sharing/sharing.cpp

new file: src/abycore/sharing/sharing.h

new file: src/abycore/sharing/splut.cpp

new file: src/abycore/sharing/splut.h

new file: src/abycore/sharing/yaoclientsharing.cpp

new file: src/abycore/sharing/yaoclientsharing.h

new file: src/abycore/sharing/yaoserversharing.cpp

new file: src/abycore/sharing/yaoserversharing.h

new file: src/abycore/sharing/yaosharing.cpp

new file: src/abycore/sharing/yaosharing.h

new file: src/examples/CMakeLists.txt

new file: src/examples/aes/CMakeLists.txt

new file: src/examples/aes/aes\_test.cpp

new file: src/examples/aes/common/aescircuit.cpp

new file: src/examples/aes/common/aescircuit.h

new file: src/examples/bench\_operations/CMakeLists.txt

new file: src/examples/bench\_operations/bench\_operations.cpp

new file: src/examples/euclidean\_distance/CMakeLists.txt

new file: src/examples/euclidean\_distance/common/euclidean\_dist.cpp

new file: src/examples/euclidean\_distance/common/euclidean\_dist.h

new file: src/examples/euclidean\_distance/euclidean\_distance\_test.cpp

new file: src/examples/float/CMakeLists.txt

new file: src/examples/float/abyfloat.cpp

new file: src/examples/innerproduct/CMakeLists.txt

new file: src/examples/innerproduct/common/innerproduct.cpp

new file: src/examples/innerproduct/common/innerproduct.h

new file: src/examples/innerproduct/innerproduct\_test.cpp

new file: src/examples/lowmc/CMakeLists.txt

new file: src/examples/lowmc/common/lowmccircuit.cpp

new file: src/examples/lowmc/common/lowmccircuit.h

new file: src/examples/lowmc/lowmc.cpp

new file: src/examples/millionaire\_prob/CMakeLists.txt

new file: src/examples/millionaire\_prob/common/millionaire\_prob.cpp

new file: src/examples/millionaire\_prob/common/millionaire\_prob.h

new file: src/examples/millionaire\_prob/millionaire\_prob\_test.cpp

new file: src/examples/min-euclidean-dist/CMakeLists.txt

new file: src/examples/min-euclidean-dist/common/min-euclidean-dist-circuit.cpp

new file: src/examples/min-euclidean-dist/common/min-euclidean-dist-circuit.h

new file: src/examples/min-euclidean-dist/min-euclidean-dist.cpp

new file: src/examples/psi\_phasing/CMakeLists.txt

new file: src/examples/psi\_phasing/common/hashing/cuckoo.cpp

new file: src/examples/psi\_phasing/common/hashing/cuckoo.h

new file: src/examples/psi\_phasing/common/hashing/hashing\_util.h

new file: src/examples/psi\_phasing/common/hashing/simple\_hashing.cpp

new file: src/examples/psi\_phasing/common/hashing/simple\_hashing.h

new file: src/examples/psi\_phasing/common/hashing\_includes.h

new file: src/examples/psi\_phasing/common/phasing\_circuit.cpp

new file: src/examples/psi\_phasing/common/phasing\_circuit.h

new file: src/examples/psi\_phasing/psi\_phasing.cpp

new file: src/examples/psi\_scs/CMakeLists.txt

new file: src/examples/psi\_scs/common/WaksmanPermutation.cpp

new file: src/examples/psi\_scs/common/WaksmanPermutation.h

new file: src/examples/psi\_scs/common/sort\_compare\_shuffle.cpp

new file: src/examples/psi\_scs/common/sort\_compare\_shuffle.h

new file: src/examples/psi\_scs/psi\_scs.cpp

new file: src/examples/sha1/CMakeLists.txt

new file: src/examples/sha1/common/sha1\_circuit.cpp

new file: src/examples/sha1/common/sha1\_circuit.h

new file: src/examples/sha1/sha1\_test.cpp

new file: src/examples/threshold\_euclidean\_dist\_2d\_simd/CMakeLists.txt

new file: src/examples/threshold\_euclidean\_dist\_2d\_simd/common/threshold-euclidean-dist.cpp

new file: src/examples/threshold\_euclidean\_dist\_2d\_simd/common/threshold-euclidean-dist.h

new file: src/examples/threshold\_euclidean\_dist\_2d\_simd/threshold-euclidean-dist.cpp

new file: src/examples/uc\_circuit/CMakeLists.txt

new file: src/examples/uc\_circuit/common/uc\_circuit.cpp

new file: src/examples/uc\_circuit/common/uc\_circuit.h

new file: src/examples/uc\_circuit/uc\_circuit\_test.cpp

new file: src/test/CMakeLists.txt

new file: src/test/abytest.cpp

new file: src/test/abytest.h

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git commit "init code"

error: pathspec 'init code' did not match any file(s) known to git.

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git commit "first code" error: pathspec 'first code' did not match any file(s) known to git.

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git commit "add"

error: pathspec 'add' did not match any file(s) known to git.

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git commit -m "init code"

[master b5409d1] init code

184 files changed, 2274449 insertions(+), 1 deletion(-)

create mode 100644 .gitignore

create mode 100644 .gitmodules

create mode 100644 .travis.yml

create mode 100644 CMakeLists.txt

create mode 100644 Doxyfile

create mode 100644 LICENSE

rewrite README.md (100%)

create mode 100644 bin/.gitignore

create mode 100644 bin/circ/circuitformat.md

create mode 100644 bin/circ/cos\_16.aby

create mode 100644 bin/circ/cos\_32.aby

create mode 100644 bin/circ/cs\_matrix16\_16.aby

create mode 100644 bin/circ/cs\_matrix32\_32.aby

create mode 100644 bin/circ/cs\_matrix\_16.aby

create mode 100644 bin/circ/cs\_matrix\_32.aby

create mode 100644 bin/circ/fp\_ieee\_add\_32.aby

create mode 100644 bin/circ/fp\_ieee\_add\_42.aby

create mode 100644 bin/circ/fp\_ieee\_add\_64.aby

create mode 100644 bin/circ/fp\_ieee\_cos\_32.aby

create mode 100644 bin/circ/fp\_ieee\_cos\_42.aby

create mode 100644 bin/circ/fp\_ieee\_div\_32.aby

create mode 100644 bin/circ/fp\_ieee\_div\_42.aby

create mode 100644 bin/circ/fp\_ieee\_div\_64.aby

create mode 100644 bin/circ/fp\_ieee\_mult\_32.aby

create mode 100644 bin/circ/fp\_ieee\_mult\_42.aby

create mode 100644 bin/circ/fp\_ieee\_mult\_64.aby

create mode 100644 bin/circ/fp\_ieee\_sin\_32.aby

create mode 100644 bin/circ/fp\_ieee\_sin\_42.aby

create mode 100644 bin/circ/fp\_ieee\_sqr\_32.aby

create mode 100644 bin/circ/fp\_ieee\_sqr\_42.aby

create mode 100644 bin/circ/fp\_ieee\_sqr\_64.aby

create mode 100644 bin/circ/fp\_ieee\_sqrt\_32.aby

create mode 100644 bin/circ/fp\_ieee\_sqrt\_42.aby

create mode 100644 bin/circ/fp\_ieee\_sqrt\_64.aby

create mode 100644 bin/circ/fp\_ieee\_sub\_32.aby

create mode 100644 bin/circ/fp\_ieee\_sub\_42.aby

create mode 100644 bin/circ/fp\_ieee\_sub\_64.aby

create mode 100644 bin/circ/fp\_nostatus\_add\_32.aby

create mode 100644 bin/circ/fp\_nostatus\_add\_42.aby

create mode 100644 bin/circ/fp\_nostatus\_add\_64.aby

create mode 100644 bin/circ/fp\_nostatus\_cmp\_32.aby

create mode 100644 bin/circ/fp\_nostatus\_cmp\_42.aby

create mode 100644 bin/circ/fp\_nostatus\_cmp\_64.aby

create mode 100644 bin/circ/fp\_nostatus\_div\_32.aby

create mode 100644 bin/circ/fp\_nostatus\_div\_42.aby

create mode 100644 bin/circ/fp\_nostatus\_div\_64.aby

create mode 100644 bin/circ/fp\_nostatus\_exp2\_32.aby

create mode 100644 bin/circ/fp\_nostatus\_exp2\_42.aby

create mode 100644 bin/circ/fp\_nostatus\_exp2\_64.aby

create mode 100644 bin/circ/fp\_nostatus\_exp\_32.aby

create mode 100644 bin/circ/fp\_nostatus\_exp\_42.aby

create mode 100644 bin/circ/fp\_nostatus\_ln\_32.aby

create mode 100644 bin/circ/fp\_nostatus\_ln\_42.aby

create mode 100644 bin/circ/fp\_nostatus\_ln\_64.aby

create mode 100644 bin/circ/fp\_nostatus\_log2\_32.aby

create mode 100644 bin/circ/fp\_nostatus\_log2\_42.aby

create mode 100644 bin/circ/fp\_nostatus\_log2\_64.aby

create mode 100644 bin/circ/fp\_nostatus\_mult\_32.aby

create mode 100644 bin/circ/fp\_nostatus\_mult\_42.aby

create mode 100644 bin/circ/fp\_nostatus\_mult\_64.aby

create mode 100644 bin/circ/fp\_nostatus\_sqr\_32.aby

create mode 100644 bin/circ/fp\_nostatus\_sqr\_42.aby

create mode 100644 bin/circ/fp\_nostatus\_sqr\_64.aby

create mode 100644 bin/circ/fp\_nostatus\_sqrt\_32.aby

create mode 100644 bin/circ/fp\_nostatus\_sqrt\_42.aby

create mode 100644 bin/circ/fp\_nostatus\_sqrt\_64.aby

create mode 100644 bin/circ/fp\_nostatus\_sub\_32.aby

create mode 100644 bin/circ/fp\_nostatus\_sub\_42.aby

create mode 100644 bin/circ/fp\_nostatus\_sub\_64.aby

create mode 100644 bin/circ/int\_div\_16.aby

create mode 100644 bin/circ/int\_div\_32.aby

create mode 100644 bin/circ/int\_div\_64.aby

create mode 100644 bin/circ/int\_div\_8.aby

create mode 100644 bin/circ/rc\_matrix16\_16.aby

create mode 100644 bin/circ/rc\_matrix32\_32.aby

create mode 100644 bin/circ/rc\_matrix\_16.aby

create mode 100644 bin/circ/rc\_matrix\_32.aby

create mode 100644 bin/circ/sin\_16.aby

create mode 100644 bin/circ/sin\_32.aby

create mode 100644 bin/uc/adder\_circ.txt

create mode 100644 bin/uc/adder\_prog.txt

create mode 100644 bin/uc/dummy\_circ.txt

create mode 100644 bin/uc/dummy\_prog.txt

create mode 100644 cmake/ABYConfig.cmake.in

create mode 100644 cmake/FindGMP.cmake

create mode 100644 cmake/FindGMPXX.cmake

create mode 100644 runtest\_scr.sh

create mode 100644 src/abycore/ABY\_utils/ABYconstants.h

create mode 100644 src/abycore/ABY\_utils/convtypes.h

create mode 100644 src/abycore/ABY\_utils/yaokey.h

create mode 100644 src/abycore/CMakeLists.txt

create mode 100644 src/abycore/DGK/dgkparty.cpp

create mode 100644 src/abycore/DGK/dgkparty.h

create mode 100644 src/abycore/DJN/djnparty.cpp

create mode 100644 src/abycore/DJN/djnparty.h

create mode 100644 src/abycore/aby/abyparty.cpp

create mode 100644 src/abycore/aby/abyparty.h

create mode 100644 src/abycore/aby/abysetup.cpp

create mode 100644 src/abycore/aby/abysetup.h

create mode 100644 src/abycore/circuit/abycircuit.cpp

create mode 100644 src/abycore/circuit/abycircuit.h

create mode 100644 src/abycore/circuit/arithmeticcircuits.cpp

create mode 100644 src/abycore/circuit/arithmeticcircuits.h

create mode 100644 src/abycore/circuit/booleancircuits.cpp

create mode 100644 src/abycore/circuit/booleancircuits.h

create mode 100644 src/abycore/circuit/circuit.cpp

create mode 100644 src/abycore/circuit/circuit.h

create mode 100644 src/abycore/circuit/share.cpp

create mode 100644 src/abycore/circuit/share.h

create mode 100644 src/abycore/ot/.gitignore

create mode 100644 src/abycore/sharing/arithsharing.cpp

create mode 100644 src/abycore/sharing/arithsharing.h

create mode 100644 src/abycore/sharing/boolsharing.cpp

create mode 100644 src/abycore/sharing/boolsharing.h

create mode 100644 src/abycore/sharing/sharing.cpp

create mode 100644 src/abycore/sharing/sharing.h

create mode 100644 src/abycore/sharing/splut.cpp

create mode 100644 src/abycore/sharing/splut.h

create mode 100644 src/abycore/sharing/yaoclientsharing.cpp

create mode 100644 src/abycore/sharing/yaoclientsharing.h

create mode 100644 src/abycore/sharing/yaoserversharing.cpp

create mode 100644 src/abycore/sharing/yaoserversharing.h

create mode 100644 src/abycore/sharing/yaosharing.cpp

create mode 100644 src/abycore/sharing/yaosharing.h

create mode 100644 src/examples/CMakeLists.txt

create mode 100644 src/examples/aes/CMakeLists.txt

create mode 100644 src/examples/aes/aes\_test.cpp

create mode 100644 src/examples/aes/common/aescircuit.cpp

create mode 100644 src/examples/aes/common/aescircuit.h

create mode 100644 src/examples/bench\_operations/CMakeLists.txt

create mode 100644 src/examples/bench\_operations/bench\_operations.cpp

create mode 100644 src/examples/euclidean\_distance/CMakeLists.txt

create mode 100644 src/examples/euclidean\_distance/common/euclidean\_dist.cpp

create mode 100644 src/examples/euclidean\_distance/common/euclidean\_dist.h

create mode 100644 src/examples/euclidean\_distance/euclidean\_distance\_test.cpp

create mode 100644 src/examples/float/CMakeLists.txt

create mode 100644 src/examples/float/abyfloat.cpp

create mode 100644 src/examples/innerproduct/CMakeLists.txt

create mode 100644 src/examples/innerproduct/common/innerproduct.cpp

create mode 100644 src/examples/innerproduct/common/innerproduct.h

create mode 100644 src/examples/innerproduct/innerproduct\_test.cpp

create mode 100644 src/examples/lowmc/CMakeLists.txt

create mode 100644 src/examples/lowmc/common/lowmccircuit.cpp

create mode 100644 src/examples/lowmc/common/lowmccircuit.h

create mode 100644 src/examples/lowmc/lowmc.cpp

create mode 100644 src/examples/millionaire\_prob/CMakeLists.txt

create mode 100644 src/examples/millionaire\_prob/common/millionaire\_prob.cpp

create mode 100644 src/examples/millionaire\_prob/common/millionaire\_prob.h

create mode 100644 src/examples/millionaire\_prob/millionaire\_prob\_test.cpp

create mode 100644 src/examples/min-euclidean-dist/CMakeLists.txt

create mode 100644 src/examples/min-euclidean-dist/common/min-euclidean-dist-circuit.cpp

create mode 100644 src/examples/min-euclidean-dist/common/min-euclidean-dist-circuit.h

create mode 100644 src/examples/min-euclidean-dist/min-euclidean-dist.cpp

create mode 100644 src/examples/psi\_phasing/CMakeLists.txt

create mode 100644 src/examples/psi\_phasing/common/hashing/cuckoo.cpp

create mode 100644 src/examples/psi\_phasing/common/hashing/cuckoo.h

create mode 100644 src/examples/psi\_phasing/common/hashing/hashing\_util.h

create mode 100644 src/examples/psi\_phasing/common/hashing/simple\_hashing.cpp

create mode 100644 src/examples/psi\_phasing/common/hashing/simple\_hashing.h

create mode 100644 src/examples/psi\_phasing/common/hashing\_includes.h

create mode 100644 src/examples/psi\_phasing/common/phasing\_circuit.cpp

create mode 100644 src/examples/psi\_phasing/common/phasing\_circuit.h

create mode 100644 src/examples/psi\_phasing/psi\_phasing.cpp

create mode 100644 src/examples/psi\_scs/CMakeLists.txt

create mode 100644 src/examples/psi\_scs/common/WaksmanPermutation.cpp

create mode 100644 src/examples/psi\_scs/common/WaksmanPermutation.h

create mode 100644 src/examples/psi\_scs/common/sort\_compare\_shuffle.cpp

create mode 100644 src/examples/psi\_scs/common/sort\_compare\_shuffle.h

create mode 100644 src/examples/psi\_scs/psi\_scs.cpp

create mode 100644 src/examples/sha1/CMakeLists.txt

create mode 100644 src/examples/sha1/common/sha1\_circuit.cpp

create mode 100644 src/examples/sha1/common/sha1\_circuit.h

create mode 100644 src/examples/sha1/sha1\_test.cpp

create mode 100644 src/examples/threshold\_euclidean\_dist\_2d\_simd/CMakeLists.txt

create mode 100644 src/examples/threshold\_euclidean\_dist\_2d\_simd/common/threshold-euclidean-dist.cpp

create mode 100644 src/examples/threshold\_euclidean\_dist\_2d\_simd/common/threshold-euclidean-dist.h

create mode 100644 src/examples/threshold\_euclidean\_dist\_2d\_simd/threshold-euclidean-dist.cpp

create mode 100644 src/examples/uc\_circuit/CMakeLists.txt

create mode 100644 src/examples/uc\_circuit/common/uc\_circuit.cpp

create mode 100644 src/examples/uc\_circuit/common/uc\_circuit.h

create mode 100644 src/examples/uc\_circuit/uc\_circuit\_test.cpp

create mode 100644 src/test/CMakeLists.txt

create mode 100644 src/test/abytest.cpp

create mode 100644 src/test/abytest.h

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git status

On branch master

Your branch is ahead of 'origin/master' by 1 commit.

(use "git push" to publish your local commits)

nothing to commit, working tree clean

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ gp

Command 'gp' not found, but can be installed with:

sudo apt install pari-gp

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git push

Username for 'https://github.com': zzztao

Password for 'https://zzztao@github.com':

remote: Invalid username or password.

fatal: Authentication failed for 'https://github.com/zzzztao/encryptogroup-ABY.git/'

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git push

Username for 'https://github.com': zzztao^[[D^[[D

Password for 'https://zzzt@github.com':

remote: Invalid username or password.

fatal: Authentication failed for 'https://github.com/zzzztao/encryptogroup-ABY.git/'

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git push

Username for 'https://github.com': zzzztao

Password for 'https://zzzztao@github.com':

Counting objects: 222, done.

Delta compression using up to 8 threads.

Compressing objects: 100% (219/219), done.

Writing objects: 100% (222/222), 10.21 MiB | 504.00 KiB/s, done.

Total 222 (delta 21), reused 0 (delta 0)

remote: Resolving deltas: 100% (21/21), done.

To https://github.com/zzzztao/encryptogroup-ABY.git

6c6b8fb..b5409d1 master -> master

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git remote add up https://github.com/WeDPR-Team/encryptogroup-ABY.git

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git remote -v

origin https://github.com/zzzztao/encryptogroup-ABY.git (fetch)

origin https://github.com/zzzztao/encryptogroup-ABY.git (push)

up https://github.com/WeDPR-Team/encryptogroup-ABY.git (fetch)

up https://github.com/WeDPR-Team/encryptogroup-ABY.git (push)

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git fetch up master

Username for 'https://github.com': zzzztao

Password for 'https://zzzztao@github.com':

remote: Enumerating objects: 224, done.

remote: Counting objects: 100% (224/224), done.

remote: Compressing objects: 100% (198/198), done.

Receiving objects: 21% (47/222), 4.47 MiB | 124.00 KiB/s

^C

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git fetch up master

Username for 'https://github.com': zzzztao

Password for 'https://zzzztao@github.com':

fatal: unable to access 'https://github.com/WeDPR-Team/encryptogroup-ABY.git/': gnutls\_handshake() failed: The TLS connection was non-properly terminated.

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git fetch up master

Username for 'https://github.com': zzzztao

Password for 'https://zzzztao@github.com':

remote: Enumerating objects: 224, done.

remote: Counting objects: 100% (224/224), done.

remote: Compressing objects: 100% (198/198), done.

remote: Total 222 (delta 21), reused 221 (delta 21), pack-reused 0

Receiving objects: 100% (222/222), 10.21 MiB | 85.00 KiB/s, done.

Resolving deltas: 100% (21/21), done.

From https://github.com/WeDPR-Team/encryptogroup-ABY

\* branch master -> FETCH\_HEAD

\* [new branch] master -> up/master

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git rebase up/master

First, rewinding head to replay your work on top of it...

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git status

On branch master

Your branch and 'origin/master' have diverged,

and have 1 and 1 different commits each, respectively.

(use "git pull" to merge the remote branch into yours)

nothing to commit, working tree clean

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git push -f

Username for 'https://github.com': zzzztao

Password for 'https://zzzztao @github.com':

remote: Invalid username or password.

fatal: Authentication failed for 'https://github.com/zzzztao/encryptogroup-ABY.git/'

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git push -f

Username for 'https://github.com': zzzztao

Password for 'https://zzzztao @github.com':

remote: Invalid username or password.

fatal: Authentication failed for 'https://github.com/zzzztao/encryptogroup-ABY.git/'

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git push -f

Username for 'https://github.com': zzzztao

Password for 'https://zzzztao@github.com':

Total 0 (delta 0), reused 0 (delta 0)

To https://github.com/zzzztao/encryptogroup-ABY.git

+ b5409d1...7fe6702 master -> master (forced update)

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git branch -a

\* master

remotes/origin/HEAD -> origin/master

remotes/origin/master

remotes/up/master

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git pull

Username for 'https://github.com': zzzztao

Password for 'https://zzzztao@github.com':

Already up to date.

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git branch -a

\* master

remotes/origin/HEAD -> origin/master

remotes/origin/master

remotes/up/master

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git fetch up

Username for 'https://github.com': zzzztao

Password for 'https://zzzztao@github.com':

From https://github.com/WeDPR-Team/encryptogroup-ABY

\* [new branch] dev -> up/dev

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git checkout up/dev

Note: checking out 'up/dev'.

You are in 'detached HEAD' state. You can look around, make experimental

changes and commit them, and you can discard any commits you make in this

state without impacting any branches by performing another checkout.

If you want to create a new branch to retain commits you create, you may

do so (now or later) by using -b with the checkout command again. Example:

git checkout -b <new-branch-name>

HEAD is now at 7fe6702 init code

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git branch -a

\* (HEAD detached at up/dev)

master

remotes/origin/HEAD -> origin/master

remotes/origin/master

remotes/up/dev

remotes/up/master

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git checkout -b dev

Switched to a new branch 'dev'

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git branch -a

\* dev

master

remotes/origin/HEAD -> origin/master

remotes/origin/master

remotes/up/dev

remotes/up/master

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git push

fatal: The current branch dev has no upstream branch.

To push the current branch and set the remote as upstream, use

git push --set-upstream origin dev

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git push --set-upstream origin dev

Username for 'https://github.com': zzzztao

Password for 'https://zzzztao@github.com':

Total 0 (delta 0), reused 0 (delta 0)

remote:

remote: Create a pull request for 'dev' on GitHub by visiting:

remote: https://github.com/zzzztao/encryptogroup-ABY/pull/new/dev

remote:

To https://github.com/zzzztao/encryptogroup-ABY.git

\* [new branch] dev -> dev

Branch 'dev' set up to track remote branch 'dev' from 'origin'.

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git add .

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git commit -m "add Binary exponent double"

[dev af6d334] add Binary exponent double

3 files changed, 351 insertions(+)

create mode 100644 src/examples/Binary\_exponent\_Double/Binary\_exponent\_Double.cpp

create mode 100644 src/examples/Binary\_exponent\_Double/Binary\_exponent\_Double.h

create mode 100644 src/examples/Binary\_exponent\_Double/CMakeLists.txt

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git pull

Username for 'https://github.com': Binary\_exponent^C

to@toddzhang-NB01:/mnt/d/encryptogroup-ABY$ git push