The program is implemented using MIRACL Core Library in C++. Here is the library link: <https://github.com/miracl/core>. The library is set up in a Docker Container. May use the provided DockerFile and docker-compose.yml to create the Docker Container and also set up the library in the container.

The Docker Container may mount to the local machine’s folder, /app. The /app folder is the place to put all the program files.

After setting up the library, in Docker Bash shell, enter:

1. cd /core/cpp
2. python3 config64.py

*Note: config64.py is a script that will generate the required cryptographic schemes for the program.*

1. Choose BLS12381 from the displayed menu.

*Note: The script will generate all required .cpp and corresponding .h files. The .cpp files will then be compiled and append into core.a. The .cpp files will then be deleted. The corresponding .h files will remain for reference for usage of the selected scheme.*

The program compilation command will be: (must be in Docker bash shell too)

g++ main.cpp main\_2.cpp setup.cpp mpencode.cpp CommitForAuditing.cpp open\_intersection.cpp big\_util.cpp verify\_intersection.cpp open\_difference.cpp verify\_difference.cpp -I /core/cpp/ /core/cpp/core.a -o main

After compilation, the program can be executed with the command below:

./main

Notes:

1. The maximum number of attributes that is entered into the program must be one size larger than the actual number of attributes to be committed. This is because the commitment also needs to include a random value, o.
2. When generating commitment, user will be asked to enter additional attributes other than the file path. Please ensure that the number of additional attributes does not exceed the “maximum number of attributes” that is entered into the system.
3. When generating proof, enter the “additional attributes” or “manual attributes” that are used when generating commitment.
4. The proof cannot be generated using the content in the file, because the entire file is hashed and treated as a single data object in the commitment.
5. When verifying proof, must enter the exact additional attributes/query attributes that are used to generate the proof and the minimum match size when is asked.