Third Party Private Set Operations - Third-Party Software and License Acknowledgment

This project includes or is based on the following third-party software, which is

subject to their respective license(s):

1. \*\*PSI From Lightweight OPRF\*\* (Permission from the author- Peihan Miao to be used and modified)

- License: N/A

- URL: <https://github.com/peihanmiao/OPRF-PSI>

- Description: This is the implementation of the paper Private Set Intersection in the Internet Setting From Lightweight Oblivious PRF published in CRYPTO 2020.

- Modifications: The following modifications were made:

- Removed main function and PSI functionality. Added functions to set appropriate parameters for the ORPF based on the size of the input set. Modified code to return OPRF result and total communication.

2. \*\* Tangent Graeffe root finding\*\* (Permission from the author- Joris van der Hoeven and Michael Monagan to be used and modified)

- License: N/A

- Joris van der Hoeven and Michael Monagan

Implementing the tangent Graeffe root finding algorithm.

In Mathematical Software -- ICMS 2020.

LNCS 12097:482--492, Springer, 2020.

- URL: [http://www.cecm.sfu.ca/CAG/code/TangentGraeffe](http://www.cecm.sfu.ca/CAG/code/TangentGraeffe" \t "_blank).

- Description: This is the implementation of the paper Implementing the tangent Graeffe root finding algorithm published in ICMS 2020.

- Modifications: The following modifications were made:

- Removed main function and added header file for roots64s function.

3. \*\*GMP Multiple Precision Arithmetic Library\*\*

- License: LGPL v3 / GPL v2

- License URL: https://gmplib.org/

- Description: The GMP library is used for high-precision arithmetic operations.

- Modifications: None (no changes were made to GMP).

4. \*\*NTL Library\*\*

- License: LGPL v2.1 or later

- License URL: https://libntl.org/

- Description: The NTL library is used for number-theoretic algorithms and cryptographic computations.

- Modifications: None (no changes were made to NTL).

5. \*\*Asio C++ Library\*\*

- License: Boost Software License 1.0

- License URL: https://www.boost.org/LICENSE\_1\_0.txt

- Description: Asio provides an asynchronous input/output library that is used for network programming.

- Modifications: None (no changes were made to Asio).

6. \*\*Coproto\*\*

- License: MIT License

- License URL: https://github.com/Visa-Research/coproto

- Description: Coproto is used for secure multi-party computation protocols.

- Modifications: None (no changes were made to Coproto).

7. \*\*cryptoTools\*\*

- License: MIT or Unlicense

- License URL: https://github.com/ladnir/cryptoTools

- Description: cryptoTools provides cryptographic protocols used for secure computations.

- Modifications: None (no changes were made to cryptoTools).

8. \*\*libOTe\*\*

- License: See License URL

- License URL: https://github.com/osu-crypto/libOTe?tab=License-1-ov-file

- Description: libOTe is used for Oblivious Transfer protocols in secure computation.

- Modifications: None (no changes were made to libOTe).

9. \*\*HElib\*\*

- License: Apache License 2.0

- License URL: https://github.com/homenc/HElib/blob/master/LICENSE.md

- Description: HElib is a software library that implements homomorphic encryption.

- Modifications: None (no changes were made to HElib).

============================================================================

For more information about the licenses or to access the full text of the licenses for third-party components, visit the provided URLs or refer to the third-party software packages themselves.