Estimating Incidental Collection in Foreign Intelligence Surveillance: Large-Scale Multiparty Private Set Intersection with Union and Sum

Anunay Kulshrestha and Jonathan Mayer, *Princeton University*

https://www.usenix.org/conference/usenixsecurity22/presentation/kulshrestha

This artifact appendix is included in the Artifact Appendices to the Proceedings of the 31st USENIX Security Symposium and appends to the paper of the same name that appears in the Proceedings of the 31st USENIX Security Symposium.

August 10–12, 2022 • Boston, MA, USA

978-1-939133-31-1

A Artifact Appendix

A.1 Abstract

Multiparty Private Set Operations is a software program that implements the protocols that we present in the main publication. The program enables multiple parties to privately compute the intersection of sets that they hold (MPSI) or the intersection of one set with the union of all other sets (MPSIU). If set elements have associated values, the library supports privately aggregating those values (MPSI-Sum or MPSIU-Sum). A delegated party learns the result of the set operation, and the parties learn no other information. The library implementation is in Go and supports execution in a Docker container.

A.2 Checklist

- **Algorithm:** Multiparty Private Set Operations implements the MPSI, MPSIU, MPSI-Sum, and MPSIU-Sum protocols in the main publication.
- **Compilation:** Compiling the program requires Go version 1.18 or more recent.
- **Data set:** The program generates random data to simulate protocol input in the user-specified `data` directory.
- **Metrics:** The program appends timing results to `bench.csv` in the user-specified `results` folder.
- **Output:** The program prints output to `stdout` and appends to `bench.csv`.
- **Experiments:** Please see the `README` file for guidance on replicating results in the main publication. The program reads protocol configuration parameters from `config.yml`.
- **How much disk space required (approximately)?:** Disk space requirements are proportional to the number of parties and set sizes, which are specified in `config.yml`.
- **How much time is needed to prepare workflow (approximately)?:** Both native and Docker builds take less than a minute on commodity hardware.
- **How much time is needed to complete experiments (approximately)?:** Please refer to Table 3 of the main publication.
- **Publicly available (explicitly provide evolving version reference)?:** https://github.com/citp/mps-operations
- **Code licenses (if publicly available)?:** We provide the program with the MIT License.
- **Archived (explicitly provide DOI or stable reference)?:** https://github.com/citp/mps-operations/releases/tag/usenix22

A.3 Description

A.3.1 How to access

Multiparty Private Set Operations is available in the Git repository at https://github.com/citp/mps-operations. The current version (as of publication) is https://github.com/citp/mps-operations/releases/tag/usenix22.

A.3.2 Software dependencies

Go (for native build) or Docker (for containerized build).

A.4 Installation

Native. Install Go (at least version 1.18) and run

```
go build -o mps_operations
./mps_operations
```

Docker. Install Docker (at least version 20.10.12) and run

```
docker build -t mps_operations .
docker run -it -rm -name mps_operations
mps_operations
```

A.5 Evaluation and expected results

Table 3 of the main publication provides execution times using large input set sizes. These benchmarks ran on a server using 128 cores. On personal computers, the execution times will be longer. In order to reproduce the benchmarks in Table 3, set the specified values for set sizes $|X_0|$ and $|X_i|$ in `config.yml`. Please refer to the `README` for build instructions.

A.6 Experiment customization

Please refer to `config.yml`.

A.7 Notes

- The number of parties n in `config.yml` does not include the delegated party.
- The program ignores the upper bound on associated values l in `config.yml` if the protocol is MPSI or MPSIU, because l is only necessary for value aggregation in MPSI-Sum and MPSIU-Sum.

A.8 Version

This artifact appendix is based on the LaTeX template for Artifact Evaluation V20220119.