Incremental Offline/Online PIR

Yiping Ma and Ke Zhong, *University of Pennsylvania;* Tal Rabin, *University of Pennsylvania and Algorand Foundation;* Sebastian Angel, *University of Pennsylvania and Microsoft Research*

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

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

This implementation contains our incremental PIR protocol as well as two baseline PIR protocols described in the paper. Our implementation requires the dependencies specified in Section A.3. We did our experiments on CloudLab.

A.2 Artifact check-list

- **Compilation:** Follow the standard compilation steps in c++. We include the detailed instructions in `readme.md`.
- **Experiments:** See readme.
- **How much disk space required (approximately)?:** 2GB.
- **How much time is needed to prepare workflow (approximately)?:** 30 minutes.
- **How much time is needed to complete experiments (approximately)?:** 1 hour.
- **Publicly available?:** Yes.

A.3 Description

A.3.1 How to access

See stable version at
`https://github.com/eniac/incpir/tree/a7d1bcf45b1bd5a3e98bcb421276ecd09c6eebdd`.

A.3.2 Hardware dependencies

Hardware should support AES-NI and AVX2.

A.3.3 Software dependencies

Protobuf, OpenSSL, libboost-all-dev, Python3, Matplotlib.

A.4 Installation

We provide a guide for how to install dependencies in `install.md`.

A.5 Experiment workflow

We provided scripts to generate numbers in benchmark table and graphs in the paper. See `readme.md` for more details.

A.6 Evaluation and expected results

We provide scripts to generate the data for the figures in the paper. In each folder (specified by `readme.md`), run `sh run.sh` or the instruction specified.

A.7 Notes

- The timings for some parts of the protocol could be slightly different from the results in the paper, because the client's queries are randomized and the time (for example, for Query) depends on which index it queries for. However, they should be on average close to what is shown in the paper.
- Some scripts will output "TimesNewRoman font not found" (if TimesNewRoman is not installed on the test machine), but you can still get figures without any problem.