USENIX Security '25 Artifact Appendix: DFS: Delegation-friendly zkSNARK and Private Delegation of Provers

Yuncong Hu [*] Pratyush Mishra [†] Xiao Wang [‡] Jie Xie [§] Kang Yang [¶] Yu Yu [‖]
Yuwen Zhang [**]

A Artifact Appendix

A.1 Abstract

This artifact appendix provides a roadmap for evaluators to test the functionality of our implementation. The artifact is based on the Arkworks framework and offers both single-prover and distributed setups.

A.2 Description & Requirements

A.2.1 Security, privacy, and ethical concerns

We attest that we have thoroughly reviewed the ethics considerations as outlined in the conference call for papers, the detailed submission instructions, and the ethics guidelines document provided by the conference organizers. The research team has carefully evaluated the ethical implications of our work on DFS, ensuring that the research has been conducted in accordance with the highest ethical standards.

Our team has considered all potential ethical issues arising from this research, including the responsible disclosure of findings, the privacy implications of the technologies developed, and the potential for both positive and negative impacts on stakeholders. We have also proactively assessed the possible risks and mitigated them where necessary. We believe that our research was conducted ethically and in a manner that aligns with both the principles of beneficence and respect for persons as described in the Menlo Report.

Additionally, our next steps following publication have been carefully planned with ethical considerations in mind. We commit to following responsible procedures for the further dissemination and application of our findings, particularly in terms of sharing data and code in compliance with the conference's open science policy. We are prepared to engage with the broader community to address any ethical concerns that may arise as the research progresses.

Finally, we have also provided this additional Ethics Considerations and Compliance with the Open Science Policy section to ensure that all relevant ethical issues are transparent and addressed appropriately.

A.2.2 How to access

The artifact can be found in DOI 10.5281/zenodo.14677896.

A.2.3 Hardware dependencies

A local machine with the following specifications is sufficient for functionality testing:

- At least 10-core CPU
- 16 GB RAM

A.2.4 Software dependencies

- **Operating System:** Ubuntu 20.04+ (recommended) or MacOS
- **Rust Compiler:** nightly toolchain (v1.75+)
- **GNU Bash:** Required for running scripts

A.2.5 Benchmarks

None.

A.3 Set-up

A.3.1 Installation

Follow the instructions in the `README.md` file to set up the environment and dependencies. Note that we are using nightly toolchain for Rust.

[*] Shanghai Jiao Tong University, huyuncong@sjtu.edu.cn
[†] University of Pennsylvania, prat@seas.upenn.edu
[‡] Northwestern University, wangxiao@northwestern.edu
[§] Shanghai Jiao Tong University, xiejie1006@gmail.com
[¶] State Key Laboratory of Cryptology, yangk@sklc.org
[‖] Shanghai Jiao Tong University & Shanghai Qi Zhi Institute, yyuu@sjtu.edu.cn
[**] UC Berkeley, yuwen01@berkeley.edu

A.3.2 Basic Test

To verify the basic functionality of the artifact, follow these steps:
Setup and Compilation.

```
cargo build --release --examples
```

Running Functional Tests. Execute the following commands:

```
cargo test --release
```

A.4 Evaluation workflow

A.4.1 Major Claims

(C1): For public delegations, DFS achieves logarithimic communication overheads.
(C2): For private delegations, DFS achieves logarithimic communication overheads for RSS-based implementations, and linear communication overheads for AddSS-based implementations.

A.4.2 Experiments

To run the experiments for example/rss_snark, example/ass_snark and example/snark, use the following commands:

```
./setup.sh
./work.sh
```

Before running the setup.sh, inst_folder folder must be created in the corresponding directory to store the generated files. The work.sh script will then run the tests.

mpirun $-$ n$*$ can be used to specify the number of cores to run. If it is changed, other parameters such as log-num-parties must also be changed accordingly.

A.5 Version

Based on the LaTeX template for Artifact Evaluation V20231005. Submission, reviewing and badging methodology followed for the evaluation of this artifact can be found at https://secartifacts.github.io/usenixsec2025/.