

Zero-Knowledge Shuffle Improvement in Ethereum Single Secret Leader Election

Anders Malta Jakobsen*, Oliver Holmgaard†



Abstract—This is the abstract Zero-Knowledge Proof (ZKP) [1].

Index Terms—Ethereum, Proof of Shuffle, Distributed Systems, Inner Product Arguments, Zero-Knowledge Proof

1 INTRODUCTION

This is the introduction

Related Work

This is related work

2 BACKGROUND

This is the background/preliminaries section

3 EXPERIMENTAL PROTOCOL

This is the experiment.

4 RESULTS

These are the results

5 DISCUSSION

This is the discussion

6 CONCLUSION

This is the conclusion

7 FUTURE WORK

This is the future work.

8 ACKNOWLEDGEMENTS

We want to express our sincere gratitude to Daniele Dell’Aglio and Michele Albano for their supervision and guidance throughout this thesis.

We also acknowledge the usage of AI tools such as ChatGPT, GitHub Copilot, and Grammarly. These have been used for clarification and implementation purposes.

- All authors are affiliated with the Dept. of Computer Science, Aalborg University, Aalborg, Denmark
- E-mails: *amja23, †oholmg20@student.aau.dk

REFERENCES

- [1] G. D. Greenwade, “The Comprehensive Tex Archive Network (CTAN),” *TUGBoat*, vol. 14, no. 3, pp. 342–351, 1993.

APPENDIX A

APPENDIX

This is the appendix