CS-523 SMCompiler Report

Author 1, Author 2

Abstract—**Please report your design, implementation details, findings of the first project in this report.**
You can add references if necessary [1].
THE REPORT SHOULD NOT EXCEED 2 PAGES. This is me testing

I. INTRODUCTION

Give a brief introduction about the project and its aims.

II. THREAT MODEL

Describe the threat model for the SMC framework that you have implemented.

III. IMPLEMENTATION DETAILS

Provide any useful details about your implementation.

IV. PERFORMANCE EVALUATION

Report the computation and communication cost of the framework for different circuit and protocol parameters.

V. APPLICATION

Detail the use case of SMC and a circuit for this use case. Discuss possible privacy leakage not covered by SMC. Discuss a mitigation if needed.

REFERENCES

[1] O. Goldreich, S. Micali, and A. Wigderson, "A completeness theorem for protocols with honest majority," *Conference Proceedings of the Annual ACM Symposium on Theory of Computing*, 01 1987.