CS523 Project 1 Report

Author 1, Author 2

***Abstract*—Please report your design, implementation details, findings in the first project in this report.**
You can add references if necessary [1].
THE REPORT SHOULD NOT EXCEED 3 PAGES.

I. Introduction

Give a brief introduction about the aim of the project, and your roadmap about the design/implementation.

II. Part I

A. Threat model

Give the corresponding threat model for this part of the project that you implemented.

B. Implementation details

- Give your implementation details
- Detail the circuit you created at the end of the first part

III. Part II

A. Threat model

Give the corresponding threat model for this part of the project that you implemented.

B. Implementation details

Give implementation details

IV. Evaluation

- Give a comprehensive comparison and evaluation about Part1 and Part2 of the project including performance results. Feel free to use charts, tables, plots...

- What changes the efficiency of the executions? Be specific, which types of operations/circuits are directly linked to performance?
- Is there any differences in terms of performance between Part-I and Part-II? Why?

V. Discussion

- Comment on your findings, discuss different outcomes for each part.
- Discuss outcomes from different circuits including your own circuit.
- In your opinion, which model is appropriate to use under which conditions/threat model? Why? Discuss.
- Come up with a scenario for each part of the implementation, discuss why it makes sense to use homomorphic encryption based generation of Beaver triplets?

VI. Conclusion

- Assess your learning outcomes for this project.
- What did you do? What did you learn? Any interesting design ideas?

References

[1] O. Goldreich, "Secure multi-party computation," *Manuscript. Preliminary Version*, 03 1999.