

Project 1 - Implement the Yao's Millionaire problem using FastGC*

1 Tasks to be Performed

- Read and understand the following paper:

Huang, Y., Evans, D., Katz, J., Malka, L., “Faster secure two-party computation using garbled circuits”, In Proceedings of the 20th USENIX conference on Security (SEC 11), 35–35, 2011.

- Install and setup FastGC on your system.
- Implement the Yao's millionaire problem using FastGC.
- Create a README file to include the set-up instructions regarding FastGC.

2 Deliverables

- README: includes the set-up instructions regarding FastGC, describes the files produced or used related to your implementation, and provides instructions how to use your implementation
- Project report: includes the implementation details of this project

*Your report must be typed, and to receive full credits, please show detailed steps regarding the tasks you performed.