PHYS379 Group 3 Minutes

Date and Time: 10/03/2023 @ 11:00
Location: Library A2 Study Space

1. **Appointment of chair & secretary**
   Sid is appointed secretary.
   Sam is appointed chair.
   Willow could not attend today due to ill health.

2. **Testing update**
   a. **Sam –** Testing the maximum number that Shor's algorithm, quick test of the inverse QFT – successful.
   b. **Sid –** Testing the classical factorization algorithm for a range of different (degenerate) semiprimes and plotting the algorithm run-time against the number of qubits that *would* be required *if* one were to use Shor's algorithm on a quantum computer. Graph shows the exponential nature of the classical factorization algorithm.
   c. **Ana –** Tested Grover's Adaptive search programme. Did two tests. One for the error probability vs the runtime and another for range of values vs runtime. Results were as expected.
   d. Willow (Gave report remotely) - Tested varying errorp and the error_size for shor's algorithm as discussed. Also restructured the report somewhat and written a few more pages to the "introduction" section to discuss how our simulation works in both halves of the project. Also added the option of including the ESI database to our report as a collection of tables in the appendix. Added a table of commonly used quantum gates to the appendix. However, this table is just taken from wikipedia and is really just a placeholder.

3. **Report writing**

Sid included his graph on report and an explanation of what it is, and more on security (mostly in the conclusion). Security is why this project is important and why we are doing it as the results in this paper show how a quantum algorithm

can be used to crack classical cryptosystems. Sam wrote some more on QFT. Willow reconstructed the report somewhat and written a few more pages to the "introduction" section to discuss how our simulation works in both halves of the project. Also added the option of including the ESI database to our report as a collection of tables in the appendix. Added a table of commonly used quantum gates to the appendix. However, this table is just taken from wikipedia and is really just a placeholder.

4. **Tasks for this week**
   Start writing results in report – Ana for Grover's and Sid and Sam for Shor's
5. **AOB**