PHYS379 Group 3 Minutes

Date and Time: 07/03/2023 @ 15:00
Location: Library B12 Study Space

1. **Appointment of chair & secretary**

Ana is appointed secretary.

Willow is appointed chair.

2. **Grover Project Progress Update**

The testing was done but Ana is afraid that the code was changed too much, and it does not work now. We have saved the old code so codes are being compared with Willow.

Solved code problems and this week will finish testing.

Decided to meet again this week to share tests.

3. **Cryptography Project Progress Update**

What has each person done?

Sam: week 14 Sam focused on quantum Fourier transform and had it working for two qubits by week 15. The work from then on was corrected by Willow, who will explain what she did this week soon.

Sid: had RSA encryption done by week 16, which worked.

Baby Shor's, written by Sid, his pretty much the same a Shor's but without the actual quantum subroutine (classical). Takes exponential amount of time. Sid said he could run some tests, however, there's not much of an overlap with the quantum Shor's algorithm.

Willow explains Shor's algorithm in detail to explain what had been done wrong in the last weeks. Programme called shor.py implements the algorithm completely when given *N, a, bits, verbose*. Only needs m ancillary bits to factorise N (e.g, for N=15 -> m=4)

RSAbreaker.py: Takes Sid's code from week 16 and with shors.py breaks it. Sid wrote 2^N RSA for N>2. Based on Sid's code we are limited to 8-bit RSA.

Willow also did some testing and explained the group the results obtained.

Testing: varying r and varying n. Also could add the error probability programme created for the Grover programme and test it.

4. **Report Progress Update**

We created two new Gmail accounts so we can all access the overleaf document. Grover's project only needs results to be written. Sam and Sid need to add what they have written so far to the document.

5. **Tasks for this week**

Set time and book a room for next meeting this week.

Ana must do the testing again for Grover's and submit the results.

Sid and Sam must add to the report what they have written so far, with references.

Sid and Sam must do testing for this week for the Shor's project.

Willow will also do some testing for Shor's with the error programme created for Grover project.

6. **AOB**