Final Year Project Interim Report

Optimal Measurements for the B92 Protocol

Author: Zhuofei Wu

Supervisor: Dr. Lluis Masanes

1 Progress Made to Date

To date, I have worked on the optimal measurements for the B92 protocol under collective attack and individual attack, and obtained results respectively. The collective attack is more powerful, since it assumes that Eve has a quantum machine with quantum memory. The individual attack is less powerful, since it assumes that Eve intercepts qubits and measures them individually with the Helstrom measurement without storing in a quantum memory.

For each attack, the following key results have been obtained:

1. H(X|Y) as a function of error rate.
2. H(X|Z) as a function of θ.
3. R as a function of error rate and θ, where R = (proportion of raw key formed from distributed bits) x (proportion of raw key retained)).
4. Solution to the optimal θ that maximises R given an arbitrary error rate.
5. The corresponding key rate R.
6. Upper bound of Eve's information gain I(X;Z).
7. Analysis of Eve's cloning strategy.
8. Graphs and plots of optimal θ, corresponding R, H(X|Z), and H(X|Y) for varying error rate.

After obtaining results for collective and individual attack, comparison and evaluation were done to analyse the security of the B92 protocol against different eavesdropping strategies, and whether the optimal θ stays in reasonable range for the same error rate under different attacks.

All results were obtained using computational models implemented in Jupyter Notebook. The algorithms and formulas used in the models were derived from theoretical calculations documented in the project's written notes. To ensure accuracy and consistency, mathematical checks and visual sanity checks were performed at each stage where necessary.

2 Remaining Work to Be Done

In summary, all compulsory objectives outlined in the project plan have been achieved. An additional optional research problem can be studied: analyse the BB84 protocol with two arbitrary bases instead of X and Y bases. The expected result is that θ = 90 degrees gives the maximal R rate. This objective is secondary to the final report and will be addressed if time permits.

The compulsory work to be done is listed as follows:

1. A literature survey summarising previous studies of security of B92 protocol against eavesdropping and other related research in the field.
2. The final report.