Final Year Project Plan

Optimal Measurements for the B92 Protocol

Author: Zhuofei Wu

Supervisor: Dr. Lluis Masanes

1 Aim

The aim of this project is to determine the optimal angle θ between the non-orthogonal quantum states used in the B92 quantum key distribution protocol to maximise security against eavesdropping, given an error rate in Bob's measurements.

2 Objectives

1. Study B92 protocol, Shannon's Information Theory and related quantum theories, which are essential for analysing the optimisation problem.
2. Derive the mutual information between Alice and Bob, I (X ; Y), and the mutual information between Alice and Eve, I (X ; Z) as functions of θ.
3. Compute the key generation rate R = I (X ; Y) – I (X ; Z) and derive the optimal θ that maximises R.
4. Evaluate the relationship between θ, error rate, and key generation rate, and assess the effectiveness of the optimisation method against eavesdropping.
5. Implement a computational model that solves the optimisation problem as a function of the specified error rate.
6. Research other optional related problems:
    a. Explore the optimisation problem for three states setup.
    b. Analyse the BB84 protocol with two arbitrary bases instead of X and Y bases. Alternatively, prove that θ = 90 degrees gives the maximal rate.
    c. Investigate the impact of different cloning strategies on the optimisation problem and whether the derived optimal θ remains valid.
    d. Generalise the optimisation problem for any QKD protocol using non-orthogonal states (e.g., BB84, 6-states protocol, E91) and its respective optimal cloning attack strategy.
    e. Develop an adaptive QKD protocol that adjusts θ based on current environmental conditions (e.g., noise level, error rate) in real time.

3 Deliverables

1. A literature survey summarising previous studies of security of B92 protocol against eavesdropping and motivating the optimisation problem.
2. The key generation rate function of θ and error rate with plots and graphics.
3. The algorithm/formulas to obtain θ value that optimises the key generation rate function.
4. A computational model that simulates the algorithm for solving the optimisation problem.
5. Evaluation and analysis of the results presented as plots and graphics.
6. Research findings for optional related problems.