**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:
   1. Explore the optimisation problem for three states setup.
   2. Analyse the BB84 protocol with two arbitrary bases instead of X and Y bases. Alternatively, prove that 𝜃 = 90 degrees gives the maximal rate.
   3. Investigate the impact of different cloning strategies on the optimisation problem and whether the derived optimal 𝜃 remains valid.
   4. 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.
   5. 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.

Problem Setup

1. Alice and Bob communicate using a flawed optical fibre (fidelity Fb < 1) and the B92 protocol. Alice has key X (x1, x2, …, xm) and Bob has key Y (y1, y2, …, ym).
2. Eve wants to eavesdrop. She replaces the flawed optical fibre with a perfect one (fidelity = 1). She attacks Alice and Bob’s setup with an asymmetric phase-covariant cloning machine, which produces clones for Bob with fidelity = Fb. Therefore, Bob cannot find out if Eve has replaced his flawed optical fibre while Eve has more (but still partial) information about Alice’s preparations.
3. Alice and Bob assume the worst case, that is there is always an adversary who has replaced their flawed optical fibre. i.e., the discrepancies are introduced by eavesdropping instead of the flawed optical fibre. These discrepancies are quantified as the error rate, defined as the proportion of incorrectly received measurements in the communication between Alice and Bob. Alice and Bob decide what value of error rate is acceptable based on security requirements.
4. To counter eavesdropping, at reconciliation phase, Alice and Bob first perform error correction which requires Alice to broadcast message R (r1, r2, …, rn), where n=mH(X|Y), which is received by both Bob and Eve. In this step, they correct discrepancies to ensure both measurements match.
5. However, Eve’s ignorance also decreases given R. To strengthen security, Alice and Bob perform privacy amplification which maps the agreed measurements (acting as their raw key) to a shorter key K (k1, k2, …, km’ where m’ < m). If the key generating rate Rk = m’/m = H(X|Z) – H(X|Y) is greater than zero, meaning that Bob has more information than Eve, then they accept K as their secure key.
6. Given an acceptable error rate on Bob’s measurements, can write Rk as a function of 𝜃. The optimisation problem is to find 𝜃 such that it maximises Rk.