Lab 6: The BB84 Protocol

Preliminaries

Refer to the teaching materials in Module 6.

Tasks

Run 'jupyter notebook', and create a notebook for this lab. Write your answers for all tasks into this notebook, and then convert it to pdf for submission to vUWS.

1. Suppose a qubit $q_0 = |-\rangle$. It is measured under a basis with the following two ordered vectors $\begin{bmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{bmatrix}$ and $\begin{bmatrix} -\frac{\sqrt{3}}{2} \\ \frac{1}{2} \end{bmatrix}$.

   1.1 Show that this basis is an orthogonal basis.

   1.2 If $q_0 = c\begin{bmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{bmatrix} + d\begin{bmatrix} -\frac{\sqrt{3}}{2} \\ \frac{1}{2} \end{bmatrix}$, then give the steps for calculating *c* and *d* manually.

2. It is known that measuring a qubit under the Horizontal basis is equivalent to applying H gate to this qubit first and then then measuring it under the Vertical basis. Please prove this fact in a Markdown cell.
   Hint: It is to prove that, if $|\psi\rangle = a|+\rangle + b|-\rangle$, then $H(|\psi\rangle) = a|0\rangle + b|1\rangle$.

3. In the BB84 Protocol, the bits where Alice and Bob choose different bases are not considered. Let's use *D* to denote the set of these bits. In this task, you should use both manual calculation and Quantum Circuit simulation to show the following:
   3.1 If Eve doesn't eavesdrop, the probability for Alice and Bob to agree on a bit in *D* is 1/2.
   3.2 If Eve eavesdrops all bits, the probability for Alice and Bob to agree on a bit in *D* is still 1/2.

   Note: In the Quantum Circuit simulation, you can generate 100 random bits first, and then choose Vertical or Horizontal basis for Alice randomly and meanwhile assign Bob the basis that is different from Alice's. In the end, the simulation should show Alice and Bob roughly agree on half of the bits in *D* in both 3.1 and 3.2.