Lab 7: The Ekert Protocol

Preliminaries

Refer to the teaching materials in Module 7.

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. In the Lecture 7, we proved the Property 2 of the three basis by assuming that Alice uses the basis consisting of $|\searrow\rangle$ and $|\nwarrow\rangle$, and Bob uses the basis consisting of $|\swarrow\rangle$ and $|\nearrow\rangle$. In this task, you are asked to prove this property by assuming that Alice uses the standard basis, and Bob uses the basis consisting of $|\swarrow\rangle$ and $|\nearrow\rangle$.

2. It is known that measuring a qubit under the $\theta = \frac{2\pi}{3}$ basis of $|\searrow\rangle$ and $|\nwarrow\rangle$ is equivalent to applying the $RY(\frac{4\pi}{3}, qubit)$ gate to this qubit first and then measuring it under the Vertical basis. Please prove this fact in a Markdown cell.
   Hint: It is to prove that, if $|\psi\rangle = a|\searrow\rangle + b|\nwarrow\rangle$, then $RY(\frac{4\pi}{3}, |\psi\rangle) = a|0\rangle + b|1\rangle$ or $-a|0\rangle - b|1\rangle$. In the proof, you need the fact that the $RY(\theta, qubit)$ gate has the following matrix: $\begin{bmatrix} \cos(\frac{\theta}{2}) & -\sin(\frac{\theta}{2}) \\ \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{bmatrix}$. Then, by using distributivity, you can apply this matrix to both $|\searrow\rangle$ and $|\nwarrow\rangle$ for calculating the result.

3. Use the QasmSimulator to implement the following variant of the Ekert Protocol: Steps 1-3 should be the same as described in Lecture 7. In Step 4, Alice and Bob share half of the bits from the string *S*. This half of the bits should be randomly chosen. Let's denote this half of the bits by S_1. If Alice and Bob agree on all the bits in S_1, it means no eavesdropping has happened, and Alice and Bob will use $S - S_1$ as the key. Otherwise, it means eavesdropping has happened, and Alice and Bob should repeat the protocol to generate another key.
   3.1 Implement the protocol for the scenario of no eavesdropping.
   3.2 Implement the protocol for the scenario of eavesdropping.
   3.3 In a Markdown cell, derive the probability for Alice and Bob to agree on a bit in S_1 if Eve overhears. Let's assume that, when eavesdropping, Eve randomly picks the three bases with equal probability. The probability derived in 3.3 should roughly match the agreement percentage you got in 3.2.

   Note: The implementations of 3.1 and 3.2 should roughly follow the structure of the notebook accompanying Lecture 7.