1. QKD: a scheme between three parties with W states

Notation: In this problem it is more convenient to use the following notations. The computational basis states $|0\rangle$, $|1\rangle$ (or Z basis) are called $|z_+\rangle$, $|z_-\rangle$ and the states $|\pm\rangle = \frac{1}{2}(|0\rangle \pm |-\rangle$ (or X basis) are denoted $|x_+\rangle$ and $|x_-\rangle$. Note that these states are the outcomes of measurements of the observables X and Z (Pauli matrices).

Suppose three parties A, B, C share a number of $|W\rangle$ states,

$$|W\rangle = \frac{1}{\sqrt{3}}(|z_+ z_- z_-\rangle + |z_- z_+ z_-\rangle + |z_- z_- z_+\rangle)$$

One can show that this is a fully entangled state in the sense that it is not equal a product state of the type $A \otimes B \otimes C$ nor of the type $(AB) \otimes C$, $(AC) \otimes B$, $(BC) \otimes A$.

The goal of A, B, C is to generate pairs of secret keys or "one-time pads" (one for AB, one for BC, one for AC) by making appropriate local measurements and using classical communication. Consider the following protocol for each instant of time $t = 1, \ldots N$:

1. A, B, C each choose an X or Z basis at random. Thus they have 8 choices $i - j - k$ with $i, j, k \in \{X, Z\}$. They perform a local measurement and keep the outcome secret.

2. They announce publicly their choice of basis.

3. They keep their measurement outcomes (secret) if the choice of basis are $Z - X - X$, $X - Z - X$, $X - X - Z$. The rest of the outcomes are discarded.

4. For the above choices only one of them choose the Z basis. At each such instant he is called the "decider". The decider looks at his measurement outcome and:

   - if it is $|z_+\rangle$ he announces publicly to A and B to discard their measurement outcomes.
   - if it is $|z_-\rangle$ he announces publicly to A and B to keep their measurement outcomes and turn them into their key bits: $|x_+\rangle \to 1$ and $|x_-\rangle \to 0$. One can show that the key bits of A and B are equal.

5. A, B, C do a security test similar to BB84 by revealing a small fraction of their secret bits. If the test passes they keep their secret pairwise keys. If it fails they abort communication.

Question a: *Check that the W-state can be written as*

$$\begin{aligned} |W\rangle = \frac{1}{\sqrt{3}}\Big(& |z_-\rangle_A \otimes \big(|x_+ x_+\rangle_{BC} - |x_- x_-\rangle_{BC}\big) \\ & + |z_+\rangle_A \otimes \frac{1}{\sqrt{2}}\big(|x_+\rangle_B - |x_-\rangle_B\big) \otimes \frac{1}{\sqrt{2}}\big(|x_+\rangle_C - |x_-\rangle_C\big)\Big) \end{aligned}$$

Deduce that for the three basis choices $Z-X-X$, $X-Z-X$, $X-X-Z$ the possible outcomes of measurements are given by this table (the decider has the Z basis and the two other parties the X basis). Compute also the probabilities for each outcome.

Alice	Bob	Charlie	Decider
z_-	x_-	x_-	
z_-	x_+	x_+	Alice
z_+	x_- or x_+	x_- or x_+	
x_-	z_-	x_-	
x_+	z_-	x_+	Bob
x_- or x_+	z_+	x_- or x_+	
x_-	x_-	z_-	
x_+	x_+	z_-	Charlie
x_- or x_+	x_- or x_+	z_+	

Question b: *Convince yourself that each pair of parties has its own one-time pad. What is then the length of each one-time pad (i.e., what fraction of N) ? On average, to produce one secret-key bit, how many quantum bits are needed in this protocol (compare with the Ekert-91 protocol) ?*

2. Secret sharing: a simple example with three parties and qutrit states

Suppose n distant parties want to share a common secret so that each party gets only a share of the secret. The secret is encoded in a string of n bits, such that any k parties that cooperate together can reconstruct the secret, but any $k-1$ of them (or less) cannot reconstruct it. These are called (k,n) secret sharing schemes in the classical case.

In quantum secret sharing schemes the secret is (typically) a quantum state which is suitably "encoded" into a state state of n qubits (or qutrits, qudits,...). These are distributed to n parties. We require that any k parties that cooperate together can reconstruct the secret, but any $k-1$ of them (or less) cannot reconstruct it. These are called $((k,n))$ quantum secret sharing schemes. One must necessarily have $k > \frac{n}{2}$ otherwise two disjoint groups of users would be able to reconstruct two copies of the secret state, thereby violating the no-cloning theorem.

In this problem we scratch the surface of this topic by looking at the following simple example. Suppose the quantum secret is a qutrit state in the Hilbert space $\mathcal{H} = \mathbb{C}^3$ with orthonormal "computational basis" basis $\{|0\rangle, |1\rangle, |2\rangle\}$:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle$$

To distributed the secret among 3 parties we first map it to (this can be done via some unitary transform in $\mathbb{C}^3 \otimes \mathbb{C}^3 \otimes \mathbb{C}^3$ where we add two ancilla qubits):

$$|\Psi\rangle \otimes |0\rangle \otimes |0\rangle \to \frac{\alpha}{\sqrt{3}}\big(|000\rangle + |111\rangle + |222\rangle\big) + \frac{\beta}{\sqrt{3}}\big(|012\rangle + |120\rangle + |201\rangle\big) + \frac{\gamma}{\sqrt{3}}\big(|021\rangle + |102\rangle + |210\rangle\big)$$

This is a "three-particle" state and each "particle" is distributed to Alice, Bob, Charlie. Each of them alone has no information to reconstruct the original state. This can be neatly proved by computing the reduced density matrix: if you know what is a density matrix do the computation.

Question a: *Without using the density matrix convince yourself as follows: what are the measurement outcomes and their respective probabilities, of say A, when she measures in the computational basis ? Same question for B and C ?*

Now we want to show that there exists a $((2,3))$ threshold scheme. Suppose A and B cooperate by doing the following unitary operation (or circuit) $\mathrm{CNOT}_{B\to A}\mathrm{CNOT}_{A\to B}$ defined as (sums are modulo 3)

$$\mathrm{CNOT}_{A\to B}|x\rangle_A \otimes |y\rangle_B = |x\rangle_A \oplus |y \oplus x\rangle_B, \quad \mathrm{CNOT}_{B\to A}|x\rangle_A \otimes |y\rangle_B = |x \oplus y\rangle_A \oplus |y\rangle_B$$

Question b: *What is the resulting state at the output of the circuit ? It turns out that A or B, but not both, gets the initial secret in their Hilbert space: who gets it ?*

Solution for problem 1: a scheme between three parties with W states

Question a: Firstly, one can check that:

$$\frac{1}{\sqrt{2}}\left(|x_+\rangle - |x_-\rangle\right) = |z_-\rangle \implies \frac{1}{\sqrt{2}}\left(|x_+\rangle - |x_-\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|x_+\rangle - |x_-\rangle\right) = |z_-z_-\rangle \tag{1}$$

and:

$$|x_\pm x_\pm\rangle = \frac{1}{\sqrt{2}}(|z_+\rangle \pm |z_-\rangle) \otimes \frac{1}{\sqrt{2}}(|z_+\rangle \pm |z_-\rangle) \tag{2}$$

$$= \frac{1}{2}(|z_+z_+\rangle + |z_-z_-\rangle \pm |z_+z_-\rangle \pm |z_-z_+\rangle) \tag{3}$$

So:

$$\frac{1}{\sqrt{2}}(|x_+x_+\rangle - |x_-x_-\rangle) = \frac{1}{\sqrt{2}}(|z_+z_-\rangle + |z_-z_+\rangle) \tag{4}$$

Therefore:

$$|W\rangle = \frac{1}{\sqrt{3}}\left(|z_-\rangle \otimes (|z_+z_-\rangle + |z_-z_+\rangle) + |z_+\rangle \otimes |z_-z_-\rangle\right) \tag{5}$$

$$= \frac{1}{\sqrt{3}}\left(|z_-\rangle \otimes (|x_+x_+\rangle - |x_-x_-\rangle) + |z_+\rangle \otimes \frac{1}{\sqrt{2}}\left(|x_+\rangle - |x_-\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|x_+\rangle - |x_-\rangle\right)\right) \tag{6}$$

Assume the basis is $Z - X - X$, we get:

$$P(|z_+\rangle_A) = \langle W| \left(|z_+\rangle_A \langle z_+|_A \otimes I_B \otimes I_c\right) |W\rangle = \frac{1}{3} \tag{7}$$

1. Conditional on the outcome $|z_+\rangle_A$ (which happens with probability $\frac{1}{3}$), Bob and Charlie obtain an outcome in the set $\{|x_+x_+\rangle, |x_-x_+\rangle, |x_+x_-\rangle, |x_-x_-\rangle\}$ with uniform probability ($\frac{1}{4}$)

2. Conditional on the outcome $|z_-\rangle_A$ (which happens with probability $\frac{2}{3}$), Bob and Charlie get either $|x_-x_-\rangle_{BC}$ with probability $\frac{1}{2}$ or $|x_+x_+\rangle_{BC}$ with probability $\frac{1}{2}$.

Question b: Let's compute for instance the probability that Charlie and Bob get the same one-time-pad:

1. First of all, there are 3 interesting basis among $2^3 = 8$ possible basis, so $\frac{3}{8}$ chances to have a correct basis.

2. Conditional on the previous event, Alice is chosen as the decider with probability $\frac{1}{3}$

3. Conditional on the previous events, Alice measures the outcome $|z_-\rangle$ with probability $\frac{2}{3}$

Therefore, in total, the probability to generate a common key-bit between Charlie and Bob is $\frac{3}{8}\frac{1}{3}\frac{2}{3} = \frac{1}{12}$ for each shared W state (so 3 qubits shared). Thus with 36 qubits BC generate 1 key-bit, but at the same time also AB and AC have generated 1 key-bit each (when the third person was a decider). Thus with 36 qubits the trio generates 3 key bits (associated to the couples AB,, BC, AC). On average this protocol consumes 12 qubits to generate one key bit.

Remark: In the Ekert-91 protocol (see the book Nielsen and Chuang for example) there are 9 basis choices out of which 2 are good to generate a common key-bit between the two parties A and B. So for 9 EPR pairs, i.e., 18 qubits we have 2 key-bits. On average the Ekert-91 protocol consumes 9 qubits to generate 1 key-bit.

Solution for problem 2: Asimple example of secret sharing with three parties and qutrit states

Question a: Let

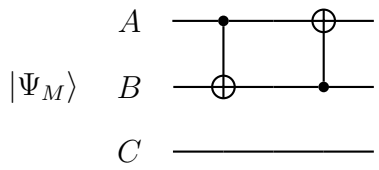
$$|\Psi_M\rangle = \frac{\alpha}{\sqrt{3}}(|000\rangle + |111\rangle + |222\rangle) + \frac{\beta}{\sqrt{3}}(|012\rangle + |120\rangle + |201\rangle) + \frac{\gamma}{\sqrt{3}}(|021\rangle + |102\rangle + |210\rangle).$$

If A does a measurement of her qubit in the basis$\{|0\rangle, |1\rangle, |2\rangle\}$, the probabilities of obtaining $0, 1, 2$, are:

$$\begin{aligned}
\text{Probability[outcome 0]} &= \langle\Psi_M| \left(|0\rangle\langle 0| \otimes 1_B \otimes 1_c\right) |\Psi_M\rangle \\
&= \langle\Psi_M| \left(\frac{\alpha}{\sqrt{3}}|000\rangle + \frac{\beta}{\sqrt{3}}|012\rangle + \frac{\gamma}{\sqrt{3}}|021\rangle\right) \\
&= \frac{|\alpha|^2}{3} + \frac{|\beta|^2}{3} + \frac{|\gamma|^2}{3} \\
&= \frac{1}{3}(\text{ since } |\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1).
\end{aligned}$$

Similarly, Probability[outcome 1] = Probability[outcome 2] $=\frac{1}{3}$. This means that A gets a purely random information and will not be able to reconstruct the secret $|\Psi\rangle$.

Question b: A and B get together and apply the following circuit



After the first $\text{CNOT}_{A\to B}|\Psi_M\rangle$, we find

$$\frac{\alpha}{\sqrt{3}}(|000\rangle + |121\rangle + |212\rangle) + \frac{\beta}{\sqrt{3}}(|012\rangle + |100\rangle + |221\rangle) + \frac{\gamma}{\sqrt{3}}(|021\rangle + |112\rangle + |200\rangle).$$

After the second $\text{CNOT}_{B\to A}$, we find that the state is

$$\begin{aligned}
&\frac{\alpha}{\sqrt{3}}(|000\rangle + |021\rangle + |012\rangle) + \frac{\beta}{\sqrt{3}}(|112\rangle + |100\rangle + |121\rangle) + \frac{\gamma}{\sqrt{3}}(|221\rangle + |212\rangle + |200\rangle) \\
&= \frac{\alpha}{\sqrt{3}}|0\rangle \otimes (|00\rangle + |21\rangle + |12\rangle) + \frac{\beta}{\sqrt{3}}|1\rangle \otimes (|12\rangle + |00\rangle + |21\rangle) + \frac{\gamma}{\sqrt{3}}|2\rangle \otimes (|21\rangle + |12\rangle + |00\rangle) \\
&= (\alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle)_A \otimes \frac{1}{\sqrt{3}}(|00\rangle + |21\rangle + |12\rangle)_{BC}
\end{aligned}$$

Thus A gets the secret state $|\Psi\rangle$.