Quantum Key Distribution

There is a task in quantum information called quantum key distribution (QKD). Its goal is to have two distance parties, Alice and Bob, follow a protocol in order to end up with a shared random secret string of bits. That is, they would like a list of 0s and 1s that they share and no one else knows. In order to achieve this they use a quantum channel that is public. That means that an eavesdropper, called Eve, could interfere with the signals that pass between Alice and Bob. In fact, we consider the case where Eve can do anything allowed by quantum mechanics. If quantum key distribution succeeds, what can Alice and Bob do with their shared secret key? An obvious application is to do classical cryptography, and in particular use the "one-time pad." This protocol involves Alice adding their key to a message they would like to send. Then Alice sends the encrypted message through a public classical channel (where Eve can see, but can't change, the messages that are sent from Alice to Bob). Since the key bits are random, the encrypted message just looks like a random string to Eve. Then Bob can just add the key to the encrypted message to get the message (see figure).

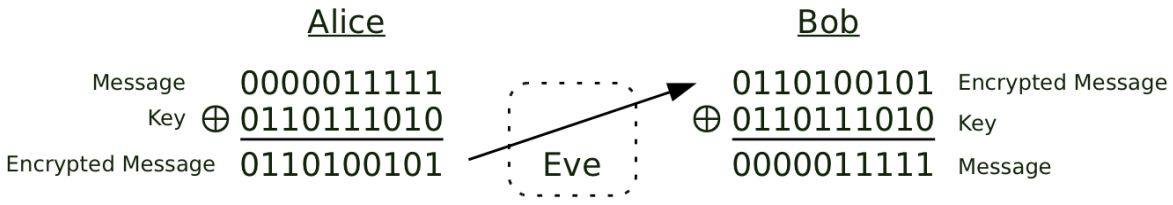

Figure 1: The one-time pad

Let's now look at two examples.

Examples

BB84

The first QKD protocol was invented by Bennet and Brassard in 1984 (hence its name). It involves Alice randomly preparing one of four quantum states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and sending it through a public quantum channel to Bob. Bob then measures the state he receives in either the basis $\{|0\rangle, |1\rangle\}$ or the basis $\{|+\rangle, |-\rangle\}$. Alice and Bob repeat this many, many times. Whenever Bob measures 0 or + he writes down "0", and whenever he measures 1 or − he writes down "1". Similarly, whenever Alice sends a 0 or + she writes "0" and when she sends a 1 or − she writes "1". After this step of distributing quantum states from Alice to Bob, they do the following classical steps (these are usually referred to as post-processing) involving classical communication:

a) *Basis Sifting*: Bob will sometimes measure in the "right" basis: for example measuring the state $|0\rangle$ in the basis $\{|0\rangle, |1\rangle\}$. Bob will always get the 0 outcome in this case. However, Bob may have measured in the "wrong" basis some of the time (*e.g.* Alice may have sent the state $|0\rangle$, but Bob measured in the basis $\{|+\rangle, |-\rangle\}$). It is easy to check that Bob will get a random outcome (*i.e.* equal probability for each outcome) whenever he measures $|0\rangle$ in the basis $\{|+\rangle, |-\rangle\}$ (and similarly for the other such "wrong" combinations of states and bases).

   To compensate for these "wrong" basis choices by Bob, Bob communicates classically to Alice all the bases he measured in. Whenever Alice sees he measured in the "wrong" basis, she tells Bob to discard that measurement result (and Alice discards hers as well).

b) *Parameter Estimation*: Since Eve may have interfered with the quantum signals, Alice and Bob want to see what percentage of their signals are errors. By knowing how many errors they have, they can do the next two steps. One way of doing this is Bob can pick a random subset of his string and communicate it to Alice. Alice can compare Bob's results with what she sent to him, and tell Bob what percentage of those results were errors. In the limit where Alice sent Bob an infinite number of quantum signals, this will give them an estimate of the percentage of errors they have in the remainder of their string. Bob discards all of the bits that he communicated to Alice to do this step, and Alice removes the corresponding bits in her string.

   Alice and Bob only continue to the next steps if the error rate is below some threshold. If the error rate is too high, it means Eve has too much information about the states that were sent, and no amount of privacy amplification (the last step) can create a secret key.

   We outline the next two steps to say what they do, without going into the details of how they accomplish their tasks.

c) *Error Correction*: Now that we know how many errors we have, Alice and Bob would like to remove them from their shared string. There exist ways for them to do this, but at the expense of reducing the length of their shared string (just like they reduced the length of their strings in parameter estimation).

d) *Privacy Amplification*: Once the errors are removed, it's possible that Eve has some information about what their shared string is. At the expense of reducing the length of their string, they can reduce Eve's knowledge about their string to a negligible amount (much less than one bit, for example), with high probability. The amount they need to reduce their shared string can be quantified, and it depends on the error probability that Alice and Bob estimated. At the end of this step, we say that Alice and Bob share a secret string. By 'secret' we mean that Eve has at most a very small amount of information about their string with high probability.

Six-State Protocol

This is another QKD protocol, very similar to BB84, where we add the states $|\circlearrowleft\rangle = (|0\rangle + i|1\rangle)/\sqrt{2}, |\circlearrowright\rangle = (|0\rangle - i|1\rangle)/\sqrt{2}$ to the list of possible states that Alice sends in the BB84 protocol. Also, Bob can choose one of the two bases from BB84, or the basis $\{|\circlearrowleft\rangle, |\circlearrowright\rangle\}$. Each of the three bases are chosen equally at random. Following the same kind of representation as above $|\circlearrowleft\rangle$ represents a "0" and $|\circlearrowright\rangle$ represents a "1". The post-processing steps are similar.

Prepare and Measure vs. Entanglement based schemes

The two examples above are examples of prepare and measure (P+M) schemes. Alice prepares states, and sends them through the channel. Bob performs measurements on the states he receives.

There is another way to do QKD by using entangled states. In this scenario Alice prepares a bipartite quantum state, and sends one half of it to Bob through the quantum channel. Alice and Bob each do measurements on their half of the state. They repeat this procedure many times. Afterwards they perform the same post-processing steps as the P+M schemes.

There is a way to connect a P+M scheme to an entanglement based one. For BB84 Alice selects one of four states to send to Bob. This can be done by Alice starting with the state $|\Psi\rangle = 1/2(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B + |2\rangle_A|+\rangle_B + |3\rangle_A|-\rangle_B)$, and then Alice measures in the standard (orthonormal) basis ($\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$). Note that Alice has a four dimensional space. However,

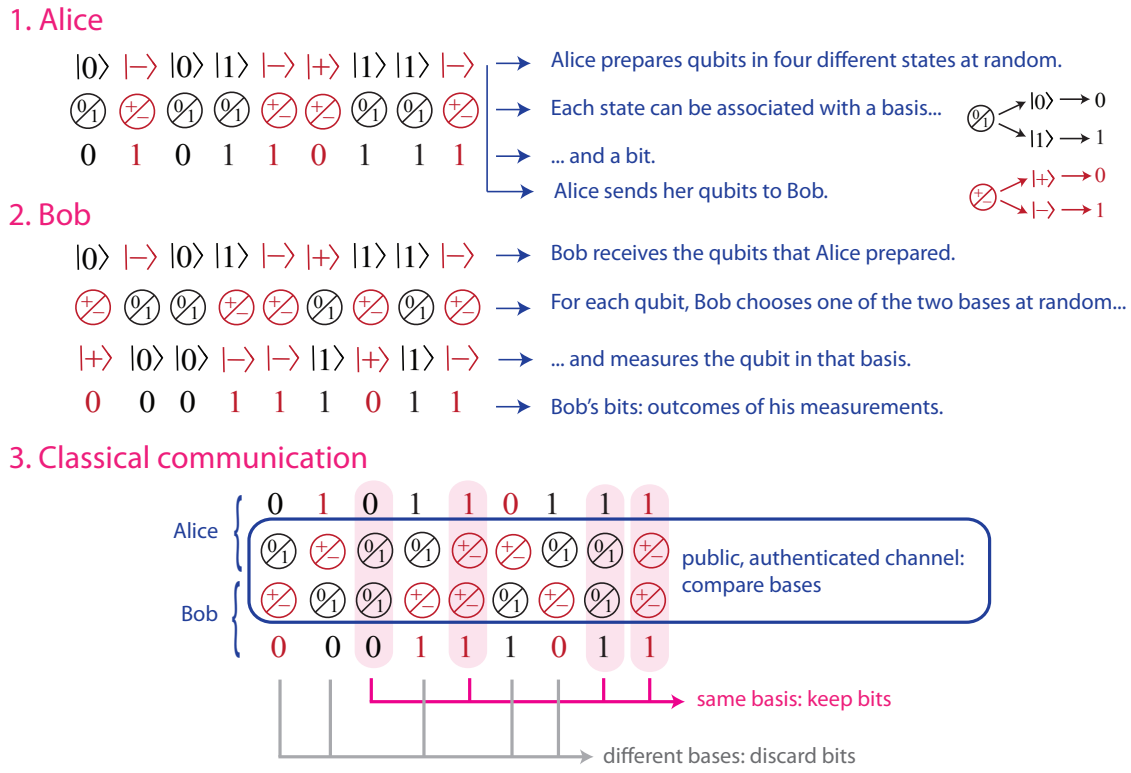

Figure 2: The BB84 protocol

we can rewrite $|\Psi\rangle$ as:

$$|\Psi\rangle = \frac{1}{2}(|0\rangle|0\rangle + |1\rangle|1\rangle + |2\rangle|+\rangle + |3\rangle|-\rangle) \tag{1}$$

$$= \frac{1}{2}\left(|0\rangle|0\rangle + |1\rangle|1\rangle + |2\rangle\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) + |3\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\right) \tag{2}$$

$$= \frac{1}{2}\left(\left(|0\rangle + \frac{|2\rangle + |3\rangle}{\sqrt{2}}\right)|0\rangle + \left(|1\rangle + \frac{|2\rangle - |3\rangle}{\sqrt{2}}\right)|1\rangle\right) \tag{3}$$

$$= \frac{1}{\sqrt{2}}\left(|\tilde{0}\rangle|0\rangle + |\tilde{1}\rangle|1\rangle\right), \tag{4}$$

where $|\tilde{0}\rangle$ and $|\tilde{1}\rangle$ are orthonormal states that are linear combinations of the basis vectors in Alice's four-dimensional space.
What this means is that Alice has a two-dimensional space imbedded in the four-dimensional space where Alice can perform her measurement. If Alice were to measure in the basis $\{|\tilde{0}\rangle, |\tilde{1}\rangle\}$, and get the outcome $|\tilde{0}\rangle$, she sends the state $|0\rangle$ to Bob. If she measures $|\tilde{1}\rangle$ in this basis, she sends $|1\rangle$. It can be easily checked that if she measures in the diagonal basis $\{|\tilde{+}\rangle, |\tilde{-}\rangle\}$, where $|\tilde{+}\rangle = (|\tilde{0}\rangle + |\tilde{1}\rangle)/\sqrt{2}$, she sends $|+\rangle$ to Bob. Similarly for measuring $|\tilde{-}\rangle$, she sends $|-\rangle$. This means that the description for the P+M scheme can be turned into an equivalent entanglement based scheme, where Alice randomly chooses to measure in one of these two tilde bases. Note that this is the exact same measurement that Bob performs on his half of the state.

Eve's Attacks

Typically Eve's attacks have been categorized into three types:

Individual Attacks: Eve attacks each signal sent by Alice individually, and in the same way.

Eve measures any quantum systems she has before Alice and Bob do their post-processing (except basis sifting).

Collective Attacks: Eve attacks each signal sent by Alice individually, and in the same way. Eve doesn't measure her quantum systems until some later time after all of QKD is completed.

Coherent Attacks: Eve attacks in an arbitrary way on each of Alice's signals, possibly in different ways. Eve doesn't measure her quantum systems until some later time after all of QKD is completed.

Clearly coherent attacks are the most general. To prove security against collective attacks, we can use the Devetak-Winter security bound (see section below). It was shown by Prof. Renner that this actually implies security for coherent attacks, provided some particular symmetry in the QKD protocol (which the BB84 and six-state protocols have).
One example of individual attacks is the intercept resend attack, where Eve performs the same measurement that Bob does, and conditioned on her measurement outcome, tries to resend the correct state to Bob.

Finding ρ_{AB}

Alice and Bob would like to share many copies of an entangled state in an entanglement based protocol. However, Eve has interfered with the states and so really, Alice, Bob and Eve share a state $|\Psi\rangle_{ABE}$. This state is pure, because we assume that Eve holds the purification of the state that Alice and Bob share. This gives the most information to Eve (i.e. even if the state is mixed, we can purify this state, and give the purifying system to Eve, since this only gives her more information: we do this to simplify the analysis).
Let's focus on the state that Alice and Bob share many copies of the reduced state of $|\Psi\rangle_{ABE}$: ρ_{AB}. Alice and Bob get particular error rates from their measurements (which Alice and Bob discover from their parameter estimation). That means that:

$$\langle 01|\rho_{AB}|01\rangle = Q/2, \quad \langle 10|\rho_{AB}|10\rangle = Q/2, \quad \langle + - |\rho_{AB}| + -\rangle = Q/2, \quad \text{etc.}$$

where Q is the error rate. Here we make the assumption that the error rate is the same in each basis (this assumption can be justified, but you don't need to show this).
In addition to knowing these restrictions on ρ_{AB}, since we assume that Alice starts with the entangled state, and Eve doesn't have access to Alice's part of the system, the reduced state for Alice, ρ_A, is fully known.
The following points may be useful to you:

1. You should apply all the restrictions on a general ρ_{AB} with unknown entries (using the fact that ρ_{AB} is hermitian and has trace 1) and then write it in the Bell Basis. You also want to ensure that $\rho_{AB} \geq 0$.

2. The Bell basis for two qubits is $\{|\psi^+\rangle, |\psi^-\rangle, |\phi^+\rangle, |\phi^-\rangle\}$, where

$$|\psi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \quad |\psi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}, |\phi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \quad |\phi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}.$$

3. To change bases for the representation of a two-qubit state from the standard basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ to any other basis, you can apply $B^{-1}\rho B$, where B is a matrix whose columns are the basis vectors represented in the standard basis. This is just linear algebra. It is highly recommended you do this part of the question in Mathematica, Matlab, or Maple.

If you're having trouble, see page 115 of Renato Renner's PhD thesis if you're stuck.

Devetak-Winter Security Bound

Now that we have a description for the quantum state that Alice and Bob share, we can find a lower-bound on the rate at which Alice and Bob can extract a key. That is, the number of key bits Alice and Bob can extract on average from each signal Alice sends Bob. Devetak and Winter found a lower bound for this key rate in the limit of an infinite number of signals sent from Alice to Bob. It is given by:

$$K = I(A:B) - \chi(A:E),$$

where χ is the Holevo quantity: $\chi(A:E) = H(E) - \sum_a p_a H(E|A=a)$, where p_a is the probability that Alice measures an outcome denoted by a, and $H(E|A=a)$ is the von Neumann entropy of E given that Alice had the outcome a from her measurement. Also, we know from Exercise 9 that: $I(A:B) = H(A) + H(B) - H(AB)$. From Exercise 9, we also have that $\chi(A:E) = I(A:E)$ since A is classical for this term in the key rate.
In addition, we know that the state shared between Alice, Bob and Eve $|\Psi\rangle_{ABE}$ is pure (see Finding ρ_{AB} section above). This means that the reduced state ρ_{AB} has the same eigenvalues as ρ_E, and therefore $H(E) = H(AB)$.
Also, once Alice has the measurement outcome a, the state that Bob and Eve share is pure, since we can assume Eve holds a purification of Bob's state: $|\Psi^a\rangle_{BE}$ (see Finding ρ_{AB} section above). Therefore we have that $H(E|A=a) = H(B|A=a)$.
To summarize, we can say that $\chi(A:E) = H(AB) - \sum_a p_a H(B|A=a)$, so the key rate can be calculated just from the knowledge of ρ_{AB}.