Exercise 12.1 BB84

The first QKD protocol was invented by Bennet and Brassard in 1984 (hence its name). In its entanglement based version (called Ekert91), Eve, an adversary, prepares many copies of a two-qubit state ρ_{AB} that she distributes to Alice and Bob (part A goes to Alice, part B goes to Bob). For each entangled state Alice and Bob have, they each randomly choose one of two bases to measure their part of their state in. These bases are: $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$. Whenever Alice measures 0 or + she writes down "0", and whenever she measures 1 or − she writes down "1". Similarly, whenever Bob measures a 0 or + he writes "0" and when he measures a 1 or − he writes "1". After this step of Eve distributing quantum states from Alice to Bob, they do the following classical steps (these are usually referred to as post-processing) involving classical communication.

i) *Basis Sifting*: Alice and Bob will sometimes measure in the same basis, in which case they will keep their measurement outcomes. If they measure in different bases they will throw away their measurement outcomes. To determine when they have measured in the same or different bases, Bob communicates classically to Alice all the bases he measured in. Whenever Alice sees he measured in a different basis, she tells Bob to discard that measurement result (and Alice discards hers as well).

ii) *Parameter Estimation*: Since Eve may give any state to Alice and Bob, Alice and Bob want to see what percentage of their signals are errors, which will help them 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.

iii) *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.

iv) *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.

a) Show that the optimal state ρ_{AB} for Alice and Bob to be sent by Eve is the maximally entangled state: $|\phi^+\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$.

b) Show that the optimal strategy for Eve (given that she has to send i.i.d. states to Alice and Bob) is to keep a purification of ρ_{AB}, namely $|\phi\rangle_{ABE}$.

c) Show that the entanglement based scheme is the same as a prepare and measure scheme outlined in Figure 1. In a prepare and measure scheme, Alice randomly prepares one of the quantum states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and then sends them through an insecure quantum channel, where Eve can influence the quantum states as she wants, as long as she obeys quantum mechanics. Bob receives the states from Eve and performs the same measurement he did in the entanglement based version.

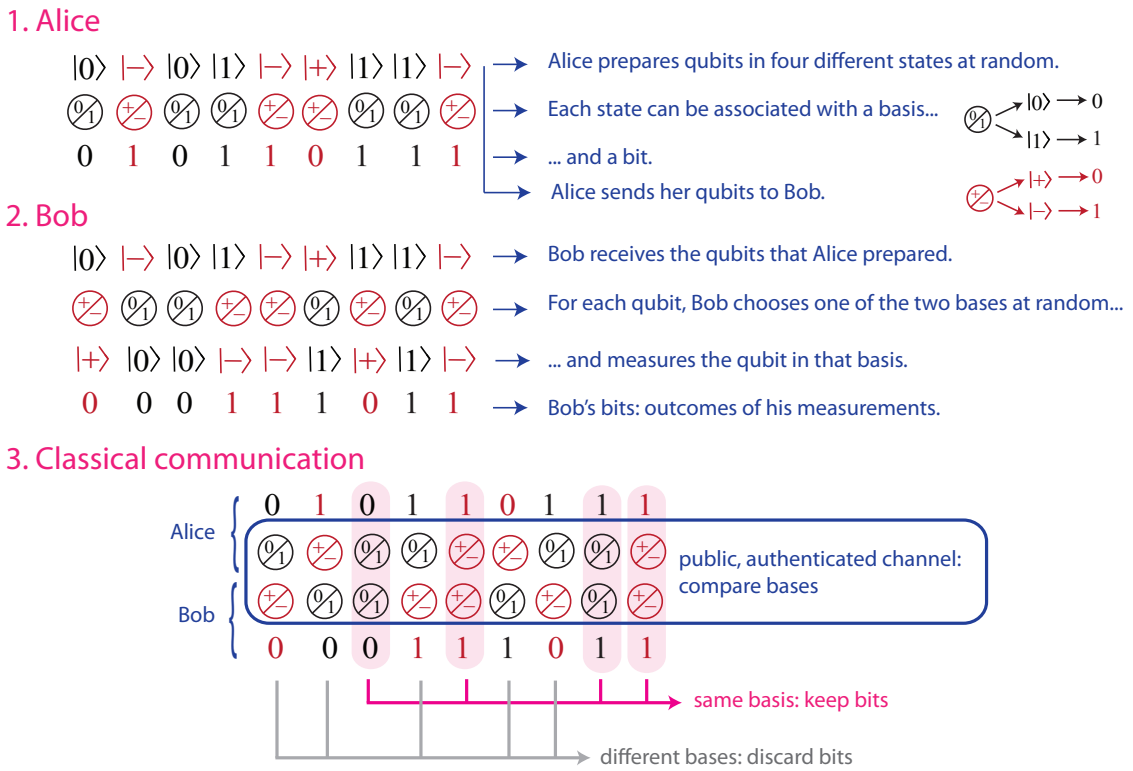

Figure 1: The BB84 prepare and measure protocol

d) Describe three problems that could arise when implementing a quantum key distribution scheme experimentally.

Exercise 12.2 Devetak-Winter Example

a) Compute $-H(A|B)$ for the noisy ebit:

$$(1-\epsilon)|\psi^+\rangle\langle\psi^+| + \epsilon\frac{\mathbb{1}}{4} \tag{1}$$

b) For which values of ϵ are you absolutely sure that you cannot obtain any secret key using quantum key distribution?