Physics 200-04

Quantum Cryptography

One of the uses to which quantum mechanics can be put is in the field of cryptography. Cryptography is the study of the secure transmission of messages from one person to another. This usually involves somehow hiding the message– scrambling the message in such a way that any evesdropper would not be able to make sense of the message, but anyone ”in the know” could retrieve the message.

A known technique, and the only technique which is known to be completely secure, is called the one time pad. Assume that Alice and Bob (A and B) wish to communicate with each other. Both have a “key”, a long string of completely random bits, and each key is the same. Bob now converts his message into a string of bits (for example using the usually ascii representation used in computers to encode letters are a string of 8 bits). He now goes down the message and for the nth bit in the message, he takes the nth bit of his random string of bits and adds that bit to the message bit, modulo 2. (Ie, 0+0=0, 0+1=1+0=1, 1+1=0) When Alice receives the message, she again adds the nth bit of the shared key to the nth bit of the message, and out pops the original bit. IF the key stream really is random, and if the attacker has no knowledge of what that key stream is, it is impossible to get out the original message.

However, how do Bob and Alice manage to exchange that key? This is always the greatest problem in cryptography.

Quantum cryptography solves this problem. What Alice does is send to Bob a series of two level systems. Using the operators $S_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and $S_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, Alice randomly sends either a $|S_1, 1\rangle$, $|S_1, -1\rangle$, $|S_3, 1\rangle$ or $|S_3, -1\rangle$.

Bob now randomly determines the value of either S_1 or S_3, not having any idea of what Alice chose. After he has determined the value, he gets in touch with Alice over a public channel, where they do not care if there is an evesdropper or not. Bob tells Alice which of the two attributes he determined, but not the value. Alice tells Bob which ones were right. Bob and Alice now keep only those values in which Alice sent an eigenstate of the same operator that Bob determined.

Now let us say that there is an evesdropper, called Eve. When Eve sees the two level system go by, she can decide to determine something about it. If she decides to determine S_1 she will be right 50% of the time, and will know that bit of the key. However the other 50% she will be wrong in that it was not the eigenstate of that operator which Alice sent. Since she has no idea what Alice sent, the best she can do is to send on the two level system after she has determined S_1. But the system will now be in an eigenstate of S_1. Assuming this is one of the cases where Bob and Alice agreed (Ie Alice sent an eigenstate of S_2 and Bob determined the value of S_2), then Bob will have a $50-50$ chance of getting the same value that Alice sent.

Thus, if Eve is trying to determine the key by trying to determine something about the two level system that Alice sent to Bob, she will cause Bob to get the wrong answer, ie, not the answer that Alice sent– 25% of the time.

Bob and Alice can now take a subset of the bits on which they agree on the attribute (Ie, Bob Determined the same attribute that Alice sent an eigenvector of), and see whether in any of those cases, Bob's value differs from what Alice sent. If it does, then there must be an evesdropper. If it does not for a large enough sample, then it is virtually certain $(1-(.75)^T$ where T is the number of test bits) that there was no evesdropping.

Copying?

Can Eve simply make a copy of each of the two level systems which Alice sends? She could then keep the copy, and when she hears Bob tell Alice which attribute he determined on each bit, she can then take the copy of that bit and determine the value of that attribute.

It turns out that this is impossible. She cannot copy the bit and leave that bit unchanged. But that will require more machinery to show.