Physics 200-04

No Cloning and Cryptography

There is an almost trivial theorem of quantum mechanics which turns out to be crucial for plugging the one last gap in the use of quantum mechanics for cryptography. There is the possibility that Eve, the attacker, simply makes an exact copy of each of the systems which fly by her. She then listens in to Bob telling Alice which bits he measured in whcih directions and measures her own copy that same direction. This would seem to get around the problem of her disturbing the state of the passing particle via her measurement.

Consider the process of copying. She must have some physical system, say it is also a two level system. This must start out in some state. So the combined system must start out in the state

$$|\psi\rangle|0\rangle \tag{1}$$

where the second particle is Eve's and the first is the particle that Aliceis sending to Bob. Now she carries out some operation on that incoming particle and her own, which leaves the system afterwards in the state $|\psi\rangle|\psi\rangle$. Ie, her own two level system is now in exactly the same state as the incoming particle.

In order to carry out the transformation, the physical process must act so as to effect a unitary transformation. But a Unitary transformation is always a linear transformation. Ie, if you carry out the transformation on the sum of two vectors, it must produce the sum of the two transformed vectors. So, let us assume that if the incoming particle comes in in the states either $|0\rangle$ or $|1\rangle$ the process makes a copy. Ie, the incoming state is

$$\begin{aligned} |0\rangle|0\rangle &\Rightarrow |0\rangle|0\rangle \\ |1\rangle|0\rangle &\Rightarrow |1\rangle|1\rangle \end{aligned} \tag{2}$$

Now, if Alice send the particle in the state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, by the linearity, the total state is

$$\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|0\rangle) \Rightarrow \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) \tag{3}$$

But this final state is **not** the same as $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) = \frac{1}{2}(|0\rangle|0\rangle+ |0\rangle|1\rangle + |0\rangle|1\rangle + |1\rangle|1\rangle)$ Ie, she has not managed to make a copy. Rather she

has created a so called entangled state. If Bob measures σ_3 and Eve then also measures σ_3 then Bob and Eve will agree on the outcome. However, since Alice did not send and eigenstate of σ_3 this will not help as that situation would be thrown out. If Bob now measures σ_2 instead, he will not get the value $+1$.

We can write the state

$$\begin{aligned}\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) &= \frac{1}{\sqrt{2}}\Big(\frac{1}{2}(|0\rangle|0\rangle + |0\rangle|1\rangle + |0\rangle|1\rangle + |1\rangle|1\rangle) \\ &\qquad \frac{1}{2}(|0\rangle|0\rangle - |0\rangle|1\rangle - |0\rangle|1\rangle + |1\rangle|1\rangle)\Big) \\ &= \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) \quad (4)\end{aligned}$$

Ie, it is a coherent sum of states with eigenvalue $+1$ for σ_1 of the first particle and eigenvalue $+1$ for σ_1 of the second particle, plus the state with eigenvalues of -1 for both. Ie, if Bob measures σ_1 he will only get the value which Alice sent half the time, and will get the other value the other half. Ie, Eve will have signaled her evesdropping by trying to copy the system passing by.

This "No Cloning" theorem is very powerful in understanding quantum information.