Advanced Quantum Mechanics
problem set number 19
7.3.2012 at 10:15 (antresola).

Quantum cryptography

1. Initial state of spin 1/2 particles a i b is given as ($\sigma_n = \pm 1$ is a shorthand notation for a projection of spin on axis n being $\pm 1/2$):

$$|\Sigma\rangle = \frac{1}{\sqrt{2}} \left\{ |\sigma_z = +1\rangle_a |\sigma_z = +1\rangle_b + |\sigma_z = -1\rangle_a |\sigma_z = -1\rangle_b \right\}. \tag{1}$$

   Show that the same state can be written as:

$$|\Sigma\rangle = \frac{1}{\sqrt{2}} \left\{ |\sigma_x = +1\rangle_a |\sigma_x = +1\rangle_b + |\sigma_x = -1\rangle_a |\sigma_x = -1\rangle_b \right\}. \tag{2}$$

   Particles in state (1) (or (2)) are sent out in opposite directions. Alice measures projection of $a-$particle spin along axis $\vec{n}_{\theta_a}$. What are possible results of this measurement and what are corresponding probabilities. Consider two cases: $\theta_a = 0$ (z axis) or $\theta_a = \pi/2$ (x axis). What is a total state $a \otimes b$ after measurements done by Alice depending on the result she obtained.

2. After the measurement performed by Alice, Bob measures projection of $b-$particle spin along axis $\vec{n}_{\theta_b}$. Take again two cases: $\theta_a = 0$ (z axis) or $\theta_a = \pi/2$ (x axis). List possible results and corresponding probabilities depending on results obtained by Alice. When Bob and Alice will get the same result with probability 1?

3. Consider the case when $\theta_a = 0$. Suppose that there is a spy S between the source and Bob. The spy measures spin projection of $b-$particle along axis $\vec{n}_{\theta_s}$. What results the spy will get depending on results obtained by Alice? Then Bob measures the projection of $b-$particle spin for $\theta_b = 0$. What results can Bob get depending on the results of the spy, and with what probability?

   What is the probability that Alice and Bob get the same results after the measurement performed by the spy? What is the expectation value $P(\theta_s)$ of obtaining the same result for the following two strategies of the spy: 1) the spy chooses angle θ_s randomly from $[0, 2\pi]$ with uniform probability; 2) the spy chooses only $\theta_s = 0$ or $\theta_s = \pi/2$ with probability 1/2.

4. In order to transmit confidential message (a message is a sequence of n bits: $++--+\ldots$) Alice and Bob apply the following procedure:

   (a) first they synchronize their axes, i.e. Bob's and Alice's z and x axes are the same;

(b) Alice who controls the source, prepares a sequence of $N \gg n$ spins of particles a and b in state (1). Alice sends particles b to Bob and measures spin of particles a;

(c) for every particle Alice and Bob measure the spin along z or x axes. For every measurement Alice and Bob chose the measurement axis randomly with probability 1/2. There is no correlation between their choices. They keep their results for further processing;

(d) Bob chooses a fraction F from N measurements and communicates to Alice by phone the number of the measurement, its axis and the result. In practice $F \sim 1/2$;

(e) Alice compares her results with the ones of Bob. She can (with some probability) decide whether there was a spy or not. If she concludes that the spy was not there she proceeds further, otherwise she calls the police;

(f) If Alice tells Bob that there was no spy, Bob tells her openly the choices of the axis in the remaining measurements, however, he does not disclose the results.

Construct the last step of this procedure, so that the n bit transmission is successful. The best way is to discuss some simple example, say 2 bit message with $N = 12$ measurements. Discuss effectiveness of this procedure. How Alice can tell that there was a spy? What is the probability of discovering a spy (say for $FN = 200$). Finally, can the spy hide himself if he knows the directions of the axes chosen by Alice and Bob?