THE OPEN UNIVERSITY

SXP390 Tutor Marked Assignment 03 - Part 4

William Ockmore

August 18, 2016

1 THE BB84 AND B92 PREPARE AND MEASURE PROTOCOLS

1.1 BB84

The BB84 protocol was the first proposed QKD protocol, put forward as the name implies in 1984 by Bennet and Brassard in their paper

1.1.1 THE PROTOCOL

In BB84, Alice uses a single photon source to transmit a set of states to Bob, encoded in the polarization of the photons. Both Alice and Bob agree to align their polarizers in either the vertical/horizontal (×) basis, or the complementary basis of +45/-45 (+). Alice then transmits a set of photons down the quantum channel, randomly choosing one of the two bases for each photon, whilst Bob measures in his choice of basis for each photon received.

$$\begin{array}{rll} |H\rangle & \text{codes for} & 0_+ \\ |V\rangle & \text{codes for} & 1_+ \\ |{+45}\rangle & \text{codes for} & 0_\times \\ |{-45}\rangle & \text{codes for} & 1_\times \end{array}$$

Both Alice and Bob now have a list of sent of received bits, each with a basis. The second phase of the protocol is the classical sifting step: over the unsecured classical channel, they first start by comparing which bases were used for each bit, and discarding the bits for which they used different bases. For a list of size N this step will on average reduce its size by half, to $N/2$. Having matched the measurement basis, this list is referred to as the *raw key*.
Alice and Bob now reveal a random sample of their raw key to one another, to compare for errors. By comparing each bit publicly over the classical channel, they can estimate the error

rate for the quantum channel. If no errors are found, the raw key is already the secret key. If there are errors, Alice and Bob must either correct for them or discard their key INSERT REFERENCE. Both these actions can take place over the classical channel; hence this step is called the *classical post-processing*. At the end of this phase, depending on how much information Eve could possess, Alice and Bob either share a secret key or they must discard the potentially compromised key.

1.2 B92

The B92 protocol, involving just 2 non-orthogonal states, is the most minimalist QKD protocol in terms of encoding. Described by Bennet in 1992 whenever they get the bit sent without further discussion from Alice. Although sometimes easier to implement than the more popular BB84, it is more difficult to establish unconditional security in the case of B92, as it is much more sensitive to noise in the quantum channel.

1.2.1 The protocol

B92 can be carried out using the two bases used in BB84. Following on from the above description, Alice sends either $|H\rangle$ or $|+45\rangle$, and Bob chooses to measure the incoming bit in either the $(\times)$ or the $(+)$ basis. Both of these states code for 0 in BB84; if Bob measures the state that codes for 1 ($|-45\rangle$ or $|V\rangle$ respectively) he can be certain that Alice transmitted her bit in the opposite basis. Hence, B92 allows the participants to restrict their transmissions in the sifting phase to whether or not Bob made a conclusive measurement for each bit sent. After discarding all bits for which Bob cannot be certain, the raw key they are left with is on average $N/4$ bits long, for an initial transmission of N bits.
After a simple comparison of raw key length to the length of the initial string sent by Alice for the classical post processing step, the participants either possess a secret key, or have been alerted to the possibility of Eve's presence.

1.3 Methods of eavesdropping - limitations of BB84 and B92

In most literature on QKD, Eve is assumed for the completeness of security proofs to have no restrictions on her eavesdropping, other than the fundamental limitations of quantum mechanics itself; namely, the no-cloning theorem and the effects of measurement on a free particle. Briefly described here are the most commonly considered eavesdropping techniques that are considered for BB84 and B92.

1.3.1 Intecept-resend

Potentially the most straightforward eavesdropping technique generally considered is the intercept-resend strategy. Eve essentially takes the same actions as Bob; with her unrestricted capabilities, performs a quantum non-demolition measurement on the incoming photons from Alice, measuring in either the $\times$) or the $(+)$ basis. If she has measured in the basis used by Alice, the photon continues on to Bob, and Eve has obtained full information whilst introducing no errors to the signal. However, if she has measured in the wrong basis, her result will

be uncorrelated with Alice's; meanwhile, she will have sent along a modified state, so even if Bob measures in the same basis as sent by Alice, half the time he will get the wrong result

1.4 Blibby bloob

Operators on the right take precedence, and the result of the lowering operator $\hat{A}$ on the ground state of a quantum harmonic oscillator ψ_0 is always zero, by the definition of the energy eigenfunctions.

$$\psi_0(x) = \left(\frac{1}{\sqrt{\pi}a}\right)^{\frac{1}{2}} e^{\frac{-x^2}{2a^2}} \tag{1.1}$$

$$\hat{A}\psi_0(x) = 0 \tag{1.2}$$

As all operators following the furthest right operate on successive results of the previous operators, all such arrangements with the lowering operator on the furthest right, operating on the ground state, must return zero.

1.5 Part b

The expectation values of any quantum mechanical operator $\hat{A}$ are given by the sandwich integral

$$\langle A \rangle = \int_{-\infty}^{\infty} \Psi^*(x,t)\hat{A}\Psi(x,t)\,dx \tag{1.3}$$

In the present case this can be reduced to

$$\langle A \rangle = \int_{-\infty}^{\infty} \psi_n^*(x)\hat{A}\psi_n(x)\,dx \tag{1.4}$$

Where $\hat{A}$ is some combination of raising and lowering operators. With $\psi_n(x)$ representing the energy eigenfunction with quantum number n. If there are unequal numbers of raising and lowering operators in a term, then the resulting eigenfunction $\psi_m(x)$ will have $m \neq n$, and due to orthnormality the result must be equal to zero.

1.6 Part c

There are three separate operator components in the integral:

- $\hat{A}\hat{A}\hat{A}^\dagger\hat{A}^\dagger$ which has eigenvalue $\sqrt{n+1} \times \sqrt{n+2} \times \sqrt{n+2} \times \sqrt{n+1}$

- $\hat{A}\hat{A}^\dagger\hat{A}\hat{A}^\dagger$ which has eigenvalue $\sqrt{n+1}\times\sqrt{n+1}\times\sqrt{n+1}\times\sqrt{n+1}$
- $\hat{A}^\dagger\hat{A}\hat{A}\hat{A}^\dagger$ which has eigenvalue $\sqrt{n+1}\times\sqrt{n+1}\times\sqrt{n}\times\sqrt{n+1}$

Where n is the original quantum number of the energy eigenvalue in the integral.
From this it can be seen that the numerical factor produced by the operators is $\sqrt{4}\times\sqrt{1}\times 0$, which is equal to 3.
Taking the factor outside the integral we are left with

$$\langle p_x^4\rangle = \frac{3\hbar^4}{4a^4}\left[\int_{-\infty}^{\infty}\psi_n^*(x)\,\psi_n(x)\,\mathrm{d}x\right] = \frac{3\hbar^4}{4a^2} \tag{1.5}$$

1.7 Part d

The expression for kinetic energy is

$$E_{\text{kin}} = \frac{p_x^2}{2m} \tag{1.6}$$

And the operator is $\frac{\hat{p}_x^2}{2m}$. The corresponding relationship for the uncertainty is

$$\Delta E_{\text{kin}} = \sqrt{\langle E_{\text{kin}}^2\rangle - \langle E_{\text{kin}}\rangle^2} \tag{1.7}$$

The uncertainty in kinetic energy is therefore given by

$$\Delta E_{\text{kin}} = \frac{1}{2m}\sqrt{\langle p_x^4\rangle - \langle p_x^2\rangle^2} \tag{1.8}$$

The right hand side of the equation then becomes

$$\frac{1}{2m}\sqrt{\frac{3\hbar^4}{4a^4} - \frac{\hbar^4}{4a^4}} = \frac{\hbar^2}{2\sqrt{2}ma^2} \tag{1.9}$$

Following from the relation $\frac{\hbar^2}{2m} = \frac{1}{2}\hbar\omega_0 a^2$, it can now be shown that

$$\Delta E_{\text{kin}} = \frac{1}{2\sqrt{2}}\hbar\omega_0 = \frac{E_0}{\sqrt{2}} \tag{1.10}$$

2 Question Two

2.1 Part a

The wave function in the question is a linear combination of products of functions of position and time, or stationary states. The time dependent phase factors are of the form $T(t) = e^{-iEt/\hbar}$, and the full time-dependent wave function can be written as

$$\Psi(x,t) = \frac{1}{\sqrt{2}}\left(\psi_1(x)e^{-iE_1 t/\hbar} - \psi_3(x)e^{-iE_3 t/\hbar}\right) \tag{2.1}$$

When looking at a harmonic oscillator the energy levels can be expressed as $E_n = (n+\frac{1}{2})\hbar\omega_0$, and so the wave function becomes

$$\Psi(x,t) = \frac{1}{\sqrt{2}}\left(\psi_1(x)e^{-3i\omega_0 t/2} - \psi_3(x)e^{-7i\omega_0 t/2}\right) \tag{2.2}$$

2.2 Part B

As the energy eigenfunctions are real, $\psi_n^*(x) = \psi_n(x)$ for both. Hence the expression for $\Psi^*(x,t)$ is

$$\Psi^*(x,t) = \frac{1}{\sqrt{2}}\left(\psi_1(x)e^{+3i\omega_0 t/2} - \psi_3(x)e^{+7i\omega_0 t/2}\right) \tag{2.3}$$

Born's rule gives probability density as

$$|\Psi(x,t)|^2 = \Psi^*(x,t)\Psi(x,t) \tag{2.4}$$

Which for the wave function in question comes out as

$$|\Psi(x,t)|^2 = \frac{1}{2}\left[\psi_1^*(x)\psi_1(x) + \psi_3^*(x)\psi_3(x) + \psi_1^*(x)\psi_3(x)e^{-2i\omega_0 t} + \psi_3^*(x)\psi_1(x)e^{+2i\omega_0 t}\right] \tag{2.5}$$

2.3 Part C

As both the eigenfunctions are odd functions, then both $\Psi(x,t)$ and $\Psi^*(x,t)$ must also be odd. The expectation value $\langle x\rangle$ is given by the sandwich integral of its operator $\hat{x}$, which is just x.

$$\langle x\rangle = \int_{-\infty}^{\infty} \Psi^*(x,t)\, x \Psi(x,t)\, \mathrm{d}x \tag{2.6}$$

As the integral is the product of three odd functions, it mus be equal to zero as it is symmetric about the origin, and this is true at all times.
There is a different approach that can be taken; as the situation in question is a harmonic oscillator, $\hat{x}$ can be alternatively expressed as

$$\hat{x} = \frac{a}{\sqrt{2}}\left(\hat{\mathrm{A}} + \hat{\mathrm{A}}^\dagger\right) \tag{2.7}$$

Which, when acting on a linear combination of $\psi_1(x)$ and $\psi_3(x)$, will produce a linear combination of $\psi_0(x)$, $\psi_2(x)$ and $\psi_4(x)$, which is orthogonal to the original function; again leaving the result as $\langle x\rangle = 0$.

2.4 Part d

The period of the breathing oscillations is $T = \frac{2\pi}{\omega_0}$.

3 Question 3

3.1 Part a

The wavenumbers k_1 and k_2 correspond to the region where the potential is zero ($x < 0$ and $x > L$) and the region where the potential is V_0 ($0 \leq x \leq L$) respectively.
We know that $E_0 = 2V_0$, so:

$$k_1 = \frac{2\sqrt{mV_0}}{\hbar} \qquad k_2 = \frac{\sqrt{2mV_0}}{\hbar} \tag{3.1}$$

3.2 Part b

As the potential energy function is finite everywhere, $\psi(x)$ and $\frac{\mathrm{d}\psi}{\mathrm{d}x}$ must be continuous everywhere. Continuity at $x = 0$ implies

$$A + B = C + D \tag{3.2}$$

$$ik_1A - ik_1B = ik_2C - ik_2D \quad \Rightarrow \quad k_1(A-B) = k_2(C-D) \tag{3.3}$$

And continuity at $x = L$ implies

$$Ce^{ik_2L} + De^{-ik_2L} = Fe^{ik_1L} \tag{3.4}$$

$$ik_2Ce^{ik_2L} - ik_2De^{-ik_2L} = ik_1Fe^{ik_1L} \quad \Rightarrow \quad k_2\left(Ce^{ik_2L} - De^{-ik_2L}\right) = k_1Fe^{ik_1L} \tag{3.5}$$

3.3 Part c

Dividing equation 3.2 by 3.3 we find

$$\frac{A+B}{A-B} = \frac{k_1}{k_2}\frac{C+D}{C-D} \tag{3.6}$$

Making use of the special case where $k_2L = \pi/2$, equation 3.4 becomes

$$i(C-D) = Fe^{ik_1L} \tag{3.7}$$

Similarly for equation 3.5,

$$-k_2(C+D) = ik_1Fe^{ik_1L} \quad \Rightarrow \quad -\frac{k_2}{ik_1}(C+D) = Fe^{ik_1L} \tag{3.8}$$

Dividing 3.7 by 3.8, we gain the following result:

$$\frac{k_1}{k_2}\frac{C-D}{C+D} = 1 \quad \Rightarrow \quad \frac{k_1}{k_2} = \frac{C+D}{C-D} \tag{3.9}$$

Using this, the substitution can be made into 3.6.

$$\frac{A+B}{A-B} = \frac{k_1}{k_2}\frac{C+D}{C-D} = \frac{k_1^2}{k_2^2} \tag{3.10}$$

In part a., it was clear that $k_1 = \sqrt{2}k_2$, which can also be expressed as $k_1/k_2 = \sqrt{2}$. This leads simply on to

$$\frac{A+B}{A-B} = 2 \quad \Rightarrow \quad A = 3B \tag{3.11}$$

The constants A and B are related to the reflection coefficient of the beam R as

$$R = \left|\frac{B}{A}\right|^2 = \frac{1}{9} \tag{3.12}$$

It is defined that

$$R + T = 1 \tag{3.13}$$

Therefore the transmission coefficient T must be equal to $8/9$.

4 Question Four

4.1 Part a

In Dirac notation an expectation value for a Hermitian operator $\hat{\mathrm{B}}$ is expressed as

$$\langle \mathrm{B} \rangle = \left\langle \Psi \middle| \hat{\mathrm{B}}\Psi \right\rangle \tag{4.1}$$

Also, for any Hermitian operator,

$$\begin{aligned} \left\langle \Psi \middle| \hat{\mathrm{B}}\Psi \right\rangle &= \langle \Psi | \hat{\mathrm{B}} | \Psi \rangle \\ &= \left\langle \hat{\mathrm{B}}\Psi \middle| \Psi \right\rangle \end{aligned} \tag{4.2}$$

The expectation value of B^2 is given by

$$\left\langle \mathrm{B}^2 \right\rangle = \left\langle \Psi \middle| \hat{\mathrm{B}}^2\Psi \right\rangle \tag{4.3}$$

$\hat{B}^2 = \hat{B}\hat{B}$, so 4.3 can be rewritten as

$$\begin{aligned}\langle B^2 \rangle &= \langle \Psi \,|\, \hat{B}\hat{B}\Psi \rangle \\ &= \langle \Psi | \hat{B} \,|\, \hat{B}\Psi \rangle \\ &= \langle \hat{B}\Psi \,|\, \hat{B}\Psi \rangle\end{aligned} \tag{4.4}$$

The operator corresponding to kinetic energy is $\frac{\hat{p}_x^2}{2m}$. Using the fact that any scalar factor can be taken outside of Dirac brackets, the expectation value for kinetic energy is given by

$$\langle E_{\text{kin}} \rangle = \frac{1}{2m} \langle \Psi \,|\, \hat{p}_x^2 \Psi \rangle \tag{4.5}$$

Using identical logic to the above set of steps, the relation becomes

$$\langle E_{\text{kin}} \rangle = \frac{1}{2m} \langle \hat{p}_x \Psi \,|\, \hat{p}_x \Psi \rangle \tag{4.6}$$

4.2 Part B

Rewriting the Dirac bracket in its integral form gives

$$\begin{aligned}\langle \hat{p}_x \Psi \,|\, \hat{p}_x \Psi \rangle &= \int_{-\infty}^{\infty} \left(-i\hbar \frac{\partial \Psi}{\partial x} \right)^* \left(-i\hbar \frac{\partial \Psi}{\partial x} \right) \mathrm{d}x \\ &= \hbar^2 \int_{-\infty}^{\infty} \left(\frac{\partial \Psi}{\partial x} \right)^* \left(\frac{\partial \Psi}{\partial x} \right) \mathrm{d}x \\ &= \hbar^2 \int_{-\infty}^{\infty} \left| \frac{\partial \Psi}{\partial x} \right|^2 \mathrm{d}x\end{aligned} \tag{4.7}$$

So $\langle E_{\text{kin}} \rangle$ can be written as

$$\langle E_{\text{kin}} \rangle = \frac{\hbar^2}{2m} \int_{-\infty}^{\infty} \left| \frac{\partial \Psi}{\partial x} \right|^2 \mathrm{d}x \tag{4.8}$$

Due to the modulus, this integral, and therefore the expectation value, cannot be negative; it must be positive and real-valued everywhere.

4.3 Part C

If the ket vector is defined as

$$\left| \hat{p}_x \Psi \right\rangle = \sum_n c_n \left| \phi_n \right\rangle \tag{4.9}$$

Then the corresponding bra vector must be equal to

$$\left\langle \hat{\mathrm{p}}_x \Psi \right| = \sum_n c_n^* \left\langle \phi_n \right| \tag{4.10}$$

Equation 4.6 can be rewritten as

$$\begin{aligned} \langle E_{\mathrm{kin}} \rangle &= \frac{1}{2m} \sum_n \sum_k c_n^* \left\langle \phi_n \right| c_k \left| \phi_k \right\rangle \\ &= \frac{1}{2m} \sum_{n,k} c_n^* c_k \left\langle \phi_n \middle| \phi_k \right\rangle \end{aligned} \tag{4.11}$$

As the functions ϕ_n form a complete orthonormal set, $\left\langle \phi_n \middle| \phi_k \right\rangle = 0$ if $n \neq k$, and 1 if $n = k$; the Dirac bracket in the sum can therefore be replaced by the Kronecker delta δ_{nk}.

$$\langle E_{\mathrm{kin}} \rangle = \frac{1}{2m} \sum_{n,k} c_n^* c_k \delta_{nk} \tag{4.12}$$

It then becomes a sum over only one of the indicies, and the required result is obtained:

$$\langle E_{\mathrm{kin}} \rangle = \frac{1}{2m} \sum_n c_n^* c_n = \frac{1}{2m} \sum_n |c_n|^2 \tag{4.13}$$

4.4 Part d

The coefficients for the functions ϕ_1 and ϕ_2 are $3\hbar/L$ and $-2i\hbar/L$ respectively.

$$\begin{aligned} \langle E_{\mathrm{kin}} \rangle &= \frac{1}{2m} \sum_n |c_n|^2 \\ &= \frac{1}{2m} \left(|c_1|^2 + |c_2|^2 \right) \\ &= \frac{1}{2m} \left[\frac{9\hbar^2}{L^2} + \frac{4\hbar^2}{L^2} \right] \\ &= \frac{13\hbar^2}{2mL^2} \end{aligned} \tag{4.14}$$