PHYS 522 Essay
4/21/2014
Darryl Masson

Quantum Key Distribution

In modern cryptography, encryption and transmission of encrypted data are all quite well established. Encrypting a data stream ensures that no one tapping the line will be able to use the information unless this eavesdropper has the encryption key. The problem arises in the creation and distribution of this key. If a method of transmission is monitored, how is the key to be distributed among authorized parties? They key itself cannot be encrypted, as this leads to an infinite regress. The subtleties of quantum mechanics allow for a number of possible methods for the creation and distribution of encryption keys through the use of single photons or an entangled pair.

Cryptography involves encoding and decoding some message by an operation with a decryption key. Without this key the message is meaningless. Using only 5 bits, all Latin characters can be encoded via the location of the letter in the alphabet. A starts at 00001, B is 00010, C is 00011, and so on up to Z, with an extra five unused sequences. Increasing the number of bits to 6 (or a commonly seen 8 bits) increases the number of possible characters to 63 (or 255). Suppose the word SNOW is created with the 5-bit method. S is 10011, N is 01110, O is 01111, and W is 10111, making the full word 10011011100111110111. Now, let the encryption process involve addition modulo 2 of each letter with the key 11011. After piecewise encryption with this cypher, the encoded message would be 01000101011010001100. This combination is meaningless without being decoded - the first sequence of five, 01000, is 8, which is 'H', the second sequence, 10101, corresponds to 'U,' the third, 10100, to 'T,' and the final sequence, 01100, to 'L', so the net result is HUTL, which happens to nonsense. Only by reversing the encryption process, which would be subtraction modulo 2, can the original word be extracted. Thus, knowledge of the encryption key is critical. Without the key, the intercepted information is useless, and randomly generating a key and decrypting the data requires knowledge of how many bits the key contains (here we used 5 but we could easily have used 6 or 4 or any other number), and a lot of data processing to decrypt the recorded data and see if it makes any sense.

Modern cryptography involves keys generated by large prime numbers. To crack the encryption, the key must be factored into its component primes, which generally requires massive amounts of computation. However, if the key is cracked and the encoded information accessed, it would be of the utmost importance to have a way of knowing that the key has been compromised. This is the primary purpose of quantum cryptography - a method of creating and transmitting an encryption key in such a way as to ensure its interception en route can be detected. This can be accomplished via the use of single photons and the principle of wavefunction collapse.

In classical optical communication, someone sending a message ("Alice"), sends pulses of light down a fibre optic cable. The receiver ("Bob") has no way of knowing if the message has been intercepted, because a person of ill repute ("Eve") can copy the transmitted message via use of a beam

splitter, which duplicates the signal, and an amplifier, which boosts the measured signal to its original amplitude. Thus neither Alice nor Bob has any way of knowing that Eve has intercepted their communication.

This, however, can be mitigated through the use of single photons as bits. A linearly polarized photon can be represented as a combination of any two spanning states, for instance horizontal and vertical polarizations, or 45 degree and 135 degree polarizations. Using Dirac notation, we could say $|\psi\rangle = \cos\theta|\updownarrow\rangle + \sin\theta|\leftrightarrow\rangle = \cos\varphi|\nearrow\rangle + \sin\varphi|\nwarrow\rangle$. The two-dimensional Hilbert space represented by the photon polarization is spanned by an infinite number of pairs of basis vectors. Two convenient pairs are $|\updownarrow\rangle$ and $|\leftrightarrow\rangle$, and $|\nwarrow\rangle$ and $|\nearrow\rangle$. So if this arbitrary photon is measured with a beam splitter that measures horizontal and vertical polarizations, the photon wavefunction will collapse into one of the possible measurements of that basis - it'll either be vertically polarized or horizontally polarized, but not both. If the polarizing beam splitter measured in a different basis, the incident photon's polarization would collapse to one of that basis.. Any linearly polarized photon can be represented in this basis. The state $|\nearrow\rangle$ can be represented in terms of $|\updownarrow\rangle$ and $|\leftrightarrow\rangle$, as can $|\nwarrow\rangle$. So regardless of the polarization basis the photon was created in, it can be measured in $|\updownarrow\rangle$ and $|\leftrightarrow\rangle$.

Now, the key to this whole business is a property of the wavefunction collapse postulate of quantum mechanics known as the no-cloning theorem. No cloning operator can successfully clone an arbitrary wavefunction. How does this work? If we define the operator U so $U|\psi\rangle = |\psi\rangle\otimes|\psi\rangle$, we see that this cloning operator U creates a direct product of a wavefunction with itself. Now, when U acts on a linear combination of arbitrary wavefunctions, it doesn't necessarily result in a perfect duplicate. We can show this by evaluating $U(|a\rangle + |b\rangle)$ in two ways. First, $U(|a\rangle + |b\rangle) = (|a\rangle + |b\rangle)\otimes(|a\rangle + |b\rangle) = |a\rangle\otimes|a\rangle + |b\rangle\otimes|b\rangle + |a\rangle\otimes|b\rangle + |b\rangle\otimes|a\rangle$. Or, $U(|a\rangle + |b\rangle) = U|a\rangle + U|b\rangle = |a\rangle\otimes|a\rangle + |b\rangle\otimes|b\rangle$. We see that the presence of the cross terms $|a\rangle\otimes|b\rangle$ and $|b\rangle\otimes|a\rangle$ form the discrepancy. Now, $|a\rangle$ and $|b\rangle$ can be constructed such that their direct products vanish, but this will only work for very specific wavefunctions; for arbitrary $|a\rangle$ and $|b\rangle$ this isn't always true. Thus, for Eve to be able to clone Alice and Bob's photons without detection, she would need to know their exact wavefunctions in order to construct the cloning apparatus so the cross terms always vanish, which in general is impossible.

The BB84 protocol is based on this no-cloning principle and is fairly widely used today to create and distribute encryption keys. Created by Gilles Brassard and Charles Bennett in 1984 (hence the name), it involves the transmission of photons created in one of two bases, either the $\oplus$ basis ($|\updownarrow\rangle$ and $|\leftrightarrow\rangle$) or the $\otimes$ basis ($|\nearrow\rangle$ and $|\nwarrow\rangle$). Numbers are encoded in these bases using $|\updownarrow\rangle$ and $|\nearrow\rangle$ as 1 and $|\leftrightarrow\rangle$ and $|\nwarrow\rangle$ as 0. Through the use of Pockels cells, Alice encodes data in either the $\oplus$ basis or the $\otimes$ basis, and Bob reads in either basis. Alice and Bob switch randomly between bases during encoding and decoding. If the same basis is used for both encoding and decoding a specific photon, then Bob will measure the same number (0 or 1) that Alice encoded with that photon. It the bases differ, the measurement is arbitrary. Once the message has been transmitted, Bob contacts Alice over an unsecured connection and tells her what bases he chose (not what he measured). Alice checks the bases Bob used against the bases she used, and tells Bob which bits have matching bases. Of this

subset of matching bases (called the "sifted set"), Bob sends a portion of his measurements to Alice. Alice checks Bob's measurements against her own, and if less than 25% are in error, the transmission was not intercepted, so the remaining bits in the subset of matching bases is used as the private encryption key.

The 25% comes from Bob having a 50% chance of measuring in the same basis as Alice and Eve also having a 50% chance of measuring in the same basis as Alice. If Eve intercepts the transmission, reads the photons, and retransmits them with a random basis, only 25% of the bits Bob measures will match what Alice sent. Thus, Alice can now detect if the NSA/Eve has intercepted their transmission. If the communication was intercepted, all bits are discarded and the process can be retried or a different communication method employed.

Let's see how this works. Here, + indicates the $\oplus$ basis and x indicates the $\otimes$ basis.

Alice	Send	1	0	1	1	0	0	0	1	0	1	0	1	1	1	0	1	0	1	1	0	0	0	1	0
	Basis	+	x	x	+	+	x	+	x	+	+	x	x	+	+	x	+	x	+	x	+	+	x	+	x
Bob	Basis	x	+	+	x	+	x	x	+	+	+	x	x	+	x	+	x	x	+	x	+	+	x	+	x
	Rec.	1	1	0	0	0	0	1	0	0	1	0	1	1	0	1	0	0	1	1	0	0	0	1	1
	Sifted	-	-	-	-	✓	✓	-	-	✓	✓	✓	✓	✓	-	-	-	✓	✓	✓	✓	✓	✓	✓	✓
	Check					✓				✓		✓		✓					✓		✓		✓		✓
	Key						0				1		1					0		1		0		1	

So here we see what happens under ideal conditions. Alice sends a message encoded in the two bases, and Bob receives a message. The sifted set is the set where both Alice and Bob use the same basis. Half of these are then used to directly check to see if Bob received what Alice sent, and the remainder forms the key. All 8 bits that are used in the check are correct, so the key would be 0110101. Now let's see what happens if Eve intercepts the photon stream and retransmits exactly what she measures.

Alice	Send	1	0	1	1	0	0	0	1	0	1	0	1	1	1	0	1	0	1	1	0	0	0	1	0
	Basis	+	x	x	+	+	x	+	x	+	+	x	x	+	+	x	+	x	+	x	+	+	x	+	x
Eve	Basis	x	+	+	x	x	+	x	+	x	x	+	+	x	+	x	x	+	x	x	+	+	x	x	+
	Rec.	0	1	1	0	1	0	1	1	0	0	0	1	0	1	0	0	1	0	1	0	0	0	1	1
Bob	Basis	+	x	x	+	+	+	x	x	x	+	x	+	+	x	x	+	x	x	+	+	x	x	+	x

	Rec.	1	0	0	1	1	0	1	0	0	1	1	1	0	1	0	1	0	0	1	0	0	0	1	0
	Sifted	-	✓	✓	✓	✓	-	-	✓	-	✓	✓	-	✓	-	✓	✓	✓	-	-	✓	-	✓	✓	✓
	Check		✓		✓				x			x				✓		✓					✓		✓
	Key			0		1					1			0			1				0			1	

Now, two of the bits Alice and Bob use to check don't match (and a few that remain don't, either, but they won't know this), so they can infer that they have been eavesdropped upon and can either try again, use a different photon channel, or use a different method of key distribution.

One other way Eve can intercept the transmission is via a Trojan horse method. If Eve sends a powerful pulse down the channel back towards Alice (in between Alice's transmitted photons), by analyzing the light that reflects off Alice's apparatus, Eve can determine which polarization state the most recently transmitted photon is in. This is fairly easy to counter if its use is suspected, but it is very effective against an unsuspecting Alice, as the polarization states are the key to the entire operation.

As nice as this is in theory, in practice there are a few complications. Photons may be absorbed or scattered during propagation between Alice and Bob. The transmission line may have some birefringence, which could act as a half-wave plate and rotate the polarization of the photon during transmission. The detectors used may register false detections. All these serve to reduce the number of bits available for the creation of the all-important encryption key. Also, a reliable single-photon source is still a bit of a black box. Attenuated single-frequency lasers output photons on a Poisson distribution, which will still occasionally output multiple photons in one pulse even when tuned properly. When this happens, Even can capture the extraneous photon(s) without disrupting the communication. The odd photon here and there isn't going to make much difference, but all the ways a photon can go missing tend to add up. Also, the medium through which the photons propagate can have an effect. If the photons travel through free space, the signal may be disturbed by stray solar radiation and changes in the intervening atmosphere. Fibre cables subject the photon to the aforementioned absorption and birefringence. Also, the use of Pockels cells generates a certain amount of acoustic noise, which Eve could use to figure out which base a photon is encoded in.

There are also other requirements. One is that Alice and Bob are connected by a single continuous dedicated fibre cable. Any repeater arrays will destroy the carefully prepared polarization state and thus the procedure. Also, Alice and Bob must be able to detect the case where Eve attempts to impersonate one or the other to disrupt the process and capture the key. The apparati that Alice and Bob work with must not have been tampered with in any way (including any alteration of the random number generator that determines which base to encode the photon or modifications made to the single photon detectors).

Another option is to use entanglement of photons as a method of key distribution. Any measurement of the state of either of a pair of entangled particles will force the measured state onto the other particle, which will destroy the entanglement and ensuring that any attempts by Eve to intercept the

transmission will result in her detection. Assuming Eve does not do this, the measurements of state of entangled particles could be used as the encryption key - a particle measured in |↕> could be a 1, and |↔> a 0. When Alice and Bob make measurements of a pair of entangled photons, they will both measure the same polarization. The same base-switching technique used in the BB84 protocol would foil any attempts at interruption. If Alice and Bob compare some measurements when their bases match, any discrepancies indicate Eve's presence.

Quantum key distribution uses superposition of states, wavefunction collapse, and the no-cloning principle to allow for the secure generation and transmission of an encryption key. A variety of protocols exist and while they are in use today, widespread adoption and total security still depend on the refinement of the technologies used, such as single photon sources and single photon detectors. Barring these, the vagaries quantum mechanics can render ineffectual any attempts to hijack the creation and distribution of an encryption key, allowing for the safe and secure transmission of encrypted data.