Notes - lecture 5
2/3/14
Darryl Masson

Introduction to Quantum Information:
Communication and Cryptography

When information and computation theory was first being developed, information was viewed as a macroscopic phenomenon, such as that contained within books. Examples of microscopic information, such as that found within DNA or the ever-shrinking transistor, were as yet unknown. Some scientists involved with the development of quantum mechanics recognized the potential of phenomena such as entanglement, but in general quantum mechanical effects were viewed as a hassle and a cause of unreliability for miniature devices. Applying the principles of quantum mechanics to information theory is a recent trend. Its applications now include cryptography, computation, and many other areas.

Cryptography involves decoding some message by an operation with a decryption key. Without this key the message is meaningless. For instance, letters can be encoded with 5 bits - the location of the letter in the alphabet. A is thus 00001, B is 00010, C is 00011, and so on up to Z. Suppose the word FOX is created with this method - it would be 001100111111000. Now, let the encryption process involve addition modulo 2 with the key 110100110101101. With this cypher, the encoded message would be 111000001010101. This combination is meaningless without being decoded - the first sequence, 11100, is 28, which isn't any Latin character. The second sequence, 00010, corresponds to 'B' and the final sequence, 10101, to 'U', so the net result is worthless. 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.

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 it cannot be intercepted en route. 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 $|\theta\rangle = \cos\theta|\updownarrow\rangle + \sin\theta|\leftrightarrow\rangle$. 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 - it'll either be vertically polarized or horizontally polarized, but not both. 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, a property of the wavefunction collapse postulate of quantum mechanics is 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 for arbitrary $|a\rangle$ and $|b\rangle$ this isn't always true.

The BB84 protocol is based on this no-cloning principle. Created by Gilles Brassard and Charles Bennett in 1984, 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, 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 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.

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 would change 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 output multiple photon pulses even when tuned properly. 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.

One option is to use entanglement as a method of key distribution. Any measurement of the state of either of a pair of entangled particles will destroy the entanglement, 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 $|\updownarrow\rangle$ would be a 1, and $|\leftrightarrow\rangle$ a 0.