Quantum Cryptography: Is your data safe even when somebody looks?

Tom Klitsner

July 3, 2001 – GSEC version 1.2e

Introduction

The peculiar nature of the theory of quantum mechanics has furrowed the brow of even the greatest physicists. According to quantum theory, objects exist as a superposition of their possible states and take on one of these physical states with a certain probability **only** once they are subjected to a measurement. Albert Einstein felt compelled by this aspect of quantum theory to object that "G-d does not play dice" (with nature) and during a heated philosophical discussion with a friend suddenly turned and asked if his friend really believed the moon was there only when somebody looks. While scientists and philosophers continue to ponder the very deep philosophical questions raised by quantum mechanics, clever strategies (if not practical systems) have been devised to use these quantum mechanical properties to potentially perform computational feats not possible with classical computing systems. While, for the most part, quantum computing devices are decades away (at least) from being practical, in the area of quantum cryptography – in particular the secure distribution of cryptographic keys – there exist strategies and systems that are feasible (perhaps even practical) today.

In order to understand how and why quantum cryptographic key exchange works, it is useful to understand a little bit of quantum mechanics. You can skip this section if you like and take my word for what the results are – but if you were a trusting person you wouldn't be reading a paper on cryptography would you? Besides, quantum cryptography can be thought of as a special case (probably the most simple case) of the broader topic of quantum computing. As such, understanding the properties of quantum mechanics that make quantum cryptography possible and useful will provide a basis for understanding more complex quantum phenomena (if this introduction should pique your interest in this area).

Basic Concepts in Quantum Mechanics

One of the most fascinating aspects of quantum mechanics is the assertion that all entities in nature have both particle and wave-like properties. While we think of light, for instance, as consisting of electromagnetic waves of various frequencies, we know that light also consists of particles called photons[1]. On the other hand we think of atoms or electrons as particles, but quantum mechanics tells us that these "particles" also have wave-like properties. The wave-like properties of matter are quantified in quantum mechanics by a mathematical function appropriately known as an object's *wavefunction*.

[1] Einstein did not officially win his Nobel Prize for the theory of relativity or discovering that $e=mc^2$, he was awarded it for demonstrating the particle nature of light with his theory of the photoelectric effect. Of course most of us know about photons because the starships on Star Trek were all armed with powerful Photon Torpedoes.

By performing mathematical operations (known as applying *operators*) on the wavefunction of an object it is possible to determine the physical properties of the object (e.g. – velocity, Kinetic energy, momentum). One of the fundamental consequences of this formulation is that, unlike classical objects that exist in one definite state, quantum objects exist in a superposition of their *possible* states. A quantum object continues to exist as a superposition of possible states until the point a measurement is made on the object (mathematically we would say than an operator acts on the wavefunction), whereupon the wavefunction is said to *collapse* into one of the possible states. A way to think about this difference between classical and quantum behavior would be to consider a traffic light. Classically the light is either red, yellow, or green (maybe a left or right turn arrow as well). A quantum traffic light would simultaneously exist in all 3 (or 4 or 5) potential final states[2] until perhaps a driver (of a quantum automobile) actually looked at (i.e. -performed a measurement on) the traffic light, whereupon it would turn one of its possible colors (imagine the turmoil this would cause at rush hour).

The double slit diffraction experiment is a classic example that illustrates the particle and wave-like nature of objects as well as the concept and consequences of a quantum particle existing as a superposition of its possible states. In this example a monochromatic (single frequency) beam of light is directed at two narrowly spaced slits resulting in a diffraction pattern very similar to the diffraction pattern that would be produced by the interference of two coherent classical wave fronts originating from the slits. (picture the pattern that would be formed if you dropped two pebbles near each other in an otherwise still pond). Not so surprising considering that we already knew that light had wave-like properties. If we perform the same experiment with a mono-energetic electron beam rather than a light beam, we get the same results. Perhaps a little more surprising because we think of electrons more as particles rather than waves, so this nicely illustrates the wave-like properties of electrons. Now, we perform the same experiment, but this time instead of a beam of electrons, we send one electron at a time towards the double slits. Now there are no other electron "waves" with which this single electron can interact to produce an interference pattern. Amazingly, we find that exactly the same interference pattern is produced as with the beam of electrons! If we now cover one of the two slits we find the double slit diffraction pattern goes away. We can even switch which slit we cover before each electron is sent and we still will not see the double slit diffraction pattern. When an electron encounters a double slit, it must in some sense pass through both slits simultaneously and then produce an interference pattern with itself. We can say that the wavefunction of the electron exists in a superposition of its two possible paths (passing through the left slit and passing through the right slit).

Quantum Computing Basics

In analogy to classical computing where the most basic component of information is the "bit", the most basic component of information in quantum computing is the "qubit" (which stands for "quantum bit" and is pronounced "cue-bit") [Bennett, 1995; Barenco *et*

[2] Although as we will see later on, this does not mean all the lights are on at once. In fact, we would say the light has no value until our quantum mechanical driver looked at it.

al., 1996; Deutsch *et al*., 1998, Mermin, 2000; Gershenfeld, 2000]. A classical bit has 2 distinct values "1" or "0". In a quantum computer these values are represented (using common quantum mechanics notation) as $|1\rangle$ and $|0\rangle$ which represent orthogonal states in a 2-state system. A qubit, instead of always having one or the other of these distinct values, can – as illustrated in the last section - exist as a superposition of these possible values

$$|\psi\rangle = \alpha\,|1\rangle + \beta\,|0\rangle$$

where $|\psi\rangle$ is the wavefunction of the qubit and α and β are the amplitudes of states $|1\rangle$ and $|0\rangle$ respectively. If a measurement is made on the qubit to determine its value, α^2 and β^2 are the probabilities that the qubit will take on the value $|1\rangle$ or $|0\rangle$ respectively.

Multiple qubits can also exist in a superposition in which the value of and individual qubit is correlated with that of the another qubit. For two qubits this would look like:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle + |1\rangle|1\rangle\right)$$

This type of state is called an *entangled state* in quantum mechanics to emphasize the tight correlation between the individual superimposed states from which it is composed. (This concept should become clearer later on when we discuss examples of entangled quantum states) [Henderson; Mermin 2000].

Much of quantum computing relies on the properties of superposition (described above) coupled with the fact that a transformation can be applied to an entire collection of qubits simultaneously resulting in potentially enormously parallel quantum computations. Beyond enhanced parallel computing capabilities, the properties of qubits can be used to solve problems for which there is no classical analog. Interestingly, almost all these discoveries have important significance to data encryption. Most important among these is the discovery of a strategy that allows large numbers to be factored in polynomial time versus exponential time (defeating some of the most popular encryption schemes, including RSA) [Shor, 1997]. Another important quantum computation results from the discovery of an algorithm for sorting/searching large (randomly ordered) lists of size *N* in $\sqrt{N}$ steps instead of on the order of *N* steps [3](which again could be used to defeat encryption algorithms such as DES by sorting through all possible keys quickly) [Grover, 1997; Grover, 1998]. Quantum teleportation – the ability to transport a quantum particle instantly across a potentially large distance – is another provocative area of basic research that uses quantum computing techniques [Bennett, 1993]. To be useful, these applications would require quantum computers consisting of hundreds or even thousands

[3] Think of trying to find a name in a regular phone book given only a person's phone number.

of qubits and many computational steps during which the qubits must remain in their delicate state [Deutsch, 1998]. For this reason, constructing a quantum computer capable of performing these calculations is probably decades away. In this paper, we will look at a far simpler application for quantum computing – secure cryptographic key exchange. This application requires only one or two qubits and one quantum measurement. Nonetheless, many of the principles behind this application are also important in the more sophisticated applications described above.

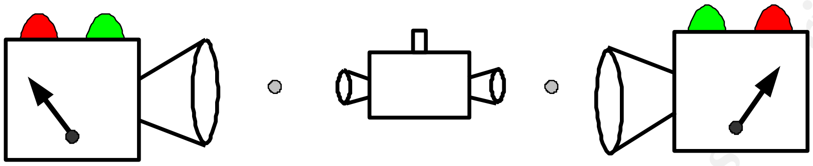
EPR, Bell's Theorem, and the Nature of the Universe[4]

One of the strangest properties that is implied in the theory of quantum mechanics is that the state of an object does not exist until it is measured. Everyone is familiar with the law that properties of any system are necessarily affected by the actions of the observer –quantum mechanics takes this a step further and asserts that these properties are actually *created* by the actions of the observer. This is the property of quantum mechanics that led Einstein to conclude that the theory of quantum mechanics must be incomplete. To illustrate this point Einstein along with Boris Podolsky and Nathan Rosen (the work is commonly referred to as EPR, [Einstein, 1935]) proposed the following *gedanken* (thought) experiment. Put two particles (say, electrons) in a correlated quantum state (an example of an EPR pair of particles is 2 electrons in the so-called singlet state where the electrons each have opposite spin – up and down – although it cannot be known which electron is up and which is down until they are measured). One then causes the particles to become separated by a large distance. EPR points out that if a measurement is made on one of these electrons and it is found that it is in the "up" state, we know with 100% certainty that the other electron will be in the "down" state when it is finally measured (this correlation between two quantum states is referred to as quantum entanglement – as we saw earlier). However, quantum mechanics tells us that this second electron does not take on the property of being in the "down" state until the moment it is actually measured. EPR assert that since the outcome of this second measurement is known, the second electron must have had the "down" property imbedded in it all along and – since we could just as easily have reversed the order of our measurements – that the first electron must have had the "up" property all along as well[5]. For many years this was thought to be merely a philosophical question with no real way to test either hypothesis (simply stated – does a property that one cannot know anything about exist all the same). Remarkably, in 1964 a physicist named John Bell discovered a variant of the EPR *gedanken* experiment in which the numerical predications of quantum theory preclude the existence of the hidden properties that EPR (and common intuition) assert must exist! This discovery, known as "Bell's Theorem" was illustrated in beautifully simple fashion by the work of another physicist, N. David Mermin [Mermin, 1985]. Mermin's

[4] Disclaimer: It is possible you will not understand the **entire** nature of the universe after reading this section.

[5] This is of course what our every day experience in the macroscopic world tells us – but Einstein's objections were for far deeper philosophical reasons than quantum mechanics asserting something non-intuitive – after all, the theory of relativity is also completely non-intuitive.

illustration needs no understanding of quantum mechanics until the very end and is described in the next few paragraphs.



Take a source that can emit two particles in opposite directions to each other as in the diagram above. After the particles leave the source they can no longer communicate with each other in any way. Some distance away place two detectors. The detectors each have two lights on them (red and green) and each have a switch with 3 positions (1, 2, 3). The switch on the detectors are set randomly and independently from each other after the source emits its two particles. When a particle enters a detector it causes the detector to flash red or green. The results are tabulated for a large number of runs and reveal two relevant features:

1. The pattern of red or green flashes is completely random – in particular this means the two detectors flash different colors half the time and the same colors half the time. This result is completely independent of the switch settings.

2. If one looks only at the data where both switches happen to be set to the **same** position (both set to 1, both to 2, or both to 3) the lights always flash the same colors (i.e. – both green or both red). Note that the particular color the light flashes is still independent of the switch position (e.g. – on one run both switches could be set to position 1 and both lights could flash green, while the next time both switches are set to position 1 both lights could flash red – all we know is that when the switches are set to the same position they both flash the same color).

As you will see below, this is actually a very strange pair of results. Since result 1 shows the pattern of flashing to be random, we can conclude that whatever properties the particles possess (that cause the lights to flash one color or the other) are assigned to these particles in a random fashion as well. How then can we arrange it so that this is true and yet each time the switch happens to be set the same for both detectors the lights flash the same color – result 2. Is this starting to seem strange yet?

Arranging result 2 by itself is actually fairly easy. Before the particles leave their source they exchange information and set up a common instruction set that determines which color they will flash for each detector position. This can be done completely randomly so that for one run they could exchange an instruction set that causes the detectors to, say, flash red, green, red (RGR) for detector positions 1, 2, or 3 respectively, while for the next run they might pick green, red, green (GRG) for the 3 positions. That way if both detectors are set to the same position, the two detectors will always flash the same color. If the two detectors have different switch positions they may flash the same color or they may flash different colors[6].

But now lets look at what the creation of these pre-defined instruction sets implies for the results of our experiment. If we look at all 8 possible instruction sets, there are really two separate classes to consider. Class 1 has two instruction values the same and 1 that is different (i.e. – RRG, RGR, GRR, GGR, GRG, RGG). Class 2 has all 3 values the same (i.e. – RRR, GGG). These instruction sets are now applied against all the possible switch settings for the two detectors. Since we know the switches are set randomly we have nine equally probable pairs of switch settings (i.e. – if we designate the switch settings by pairs of numbers where the first number is the setting for switch 1 and the second for switch 2 then the complete set of switch settings are: 11, 12, 13, 21, 22, 23, 31, 32, 33). For all class 1 instruction sets, it is easy to see that the lights will flash the same color in 5 of these 9 pairs (e.g. – for RRG the lights flash the same for 12 and 21, as well as 11, 22, and 33). This means in all of our class 1 examples the lights flash the same color 5/9 of the time. For class 2, it is obvious that the lights will flash the same color all of the time. This means that no matter how the instruction sets are picked the lights should flash the same color at least 5/9 of the time (if in fact the instruction sets are picked randomly it will result in the lights flashing the same color 2/3 of the time – i.e. 48 of the 72 pair combinations). This is Bell's theorem for this *gedanken* experiment.

Now do you see the problem? The results for the experiment state that the two detectors should only flash the same color half the time (Result 1). Since we found that Bell's theorem for this situation states that for instruction sets to exist within each particle, the lights must flash the same at least 5/9 of the time, **we must conclude that no instruction sets exist within the particles described in this experiment.** Now you might claim that we (actually Mermin) have just picked a bad instruction set. Rest assured this is not so[7].

As you might now have guessed by the subject matter of this paper, the way to make a device with the properties described above is by using the quantum mechanical properties of particles. A system that produces results that match our experiment is in fact our correlated electron pair in the singlet state we discussed earlier when introducing the EPR

[6] Note that the most information that we can gain about the particles on any given run is the value that is set for two of the 3 positions (e.g. – if the detectors are set at positions 1 and 2, we will learn those two setting values but not the value for setting 3 – position 3 is now equivalent to the hidden values that EPR asserted must exist – we cannot know its value, but we "know" that value must exist nonetheless – say EPR).
[7] Since we've already established you are not the trusting sort – you should attempt to create other schemes that account for the stated results (remember there can be no communication between any parts of the experiment once the particles have left the source and the switches are set independently and randomly).

paradox (one electron has spin up and the other spin down). An analogous system that is somewhat easier to understand mathematically, is a correlated (entangled) photon pair (this system has actually been produced and the results have been confirmed experimentally [Aspect, 1981; Jennewien 1999]). Instead of correlated spins the photons have left or right *polarizations*. An atomic emission process creates the entangled pair of photons with identical polarizations and traveling in opposite directions. The detectors in this case perform polarization measurements along 3 possible axes that are 120° apart from each other and perpendicular to the propagation direction of the photons (our 3 switches). When both detectors measure polarization along the same axis, the 2 identically polarized (and entangled) photons will of course be found to have the same polarization (lights both flash red or both flash green). This must be so, since in quantum mechanics jargon, we are applying the same *operator* (the polarization operator) against, by definition, identical states. When the photons have their polarizations measured at 120° angles to each other, something more peculiar happens. Classically, we know that by rotating a polarization filter in front of polarized light, the intensity of the light beam decreases by an amount proportional to the square of the cosine of the angle between the direction of polarization of the beam and the polarization direction of the filter[8]. In quantum mechanics there is no such thing as a quantum state having a lower "intensity". After a measurement (such as going through a polarization detector) the photon's wavefunction will collapse to one of its two possible states (as we discussed earlier). The quantum mechanical equivalent to the intensity attenuation is the probability with which the polarized photon will end up in its two possible final states (polarized along the detector axis or orthogonal to it). Therefore, quantum mechanics predicts that the polarization of the photons will be the same only ¼ of the time (¼ $=\cos^2(120^o)$). In terms of our wavefunction formalism, we can thing of this in the following way. Generate a wave function for one of the photons in terms of the other photon's polarization direction. This is equivalent to projecting a unitary vector (a vector of length = 1) along the directions of the final possible states (i.e. along the polarization axis of the detector or orthogonal to it). Basic trigonometry tells us that this would look like

$$|\psi\rangle = \cos(\theta)|1\rangle + \sin(\theta)|0\rangle$$

where $|1\rangle$ represents a final state with the same polarization as the other photon (lights flash the same colors) and $|0\rangle$ represents a final state with polarization orthogonal to the polarization of the other photon (lights flash different colors). Remember from our introduction that the square of the amplitude of a state equals the probability of a measurement yielding that state (i.e. – the probability of $|1\rangle$ = $\cos^2(120^o)$ = ¼ - just as our classical analog suggested).

Therefore for the 9 possible (random) combinations of orientations this means that 3 of them will always result in the same color light flashing (11, 22, 33) i.e. for $\frac{1}{3}$ of the

[8] If you take the lens of polarized sunglasses and rotate them with respect to each other you can see this effect – with the lens going dark when they are at 90° to each other.

settings the lights always flash the same color (they had better, since this was feature 2 of the experiment). - For the measurements along the 6 remaining orientations (12, 13, 21, 23, 31, 32) the lights will flash the same only ¼ of the time. This means that the lights will flash the same $\frac{1}{3}$ x 1 + $\frac{2}{3} \times \frac{1}{4} = \frac{1}{2}$ of the time. Just as feature 1 of our *gedanken* experiment required.

So what have we learned from this. First, the example above illustrates some of the properties of quantum mechanics that turn out to be useful in quantum computing and quantum cryptography. These include: 1) The properties of an *entangled* quantum state where one particle's state is tightly coupled to another's, even if the two particles are separated by potentially large distances, 2) The consequences of a particle's wavefunction being a superposition of possible states, leading to results that have no classical analog – i.e. – the photon had a probability associated with being in one of two polarization states, and. finally, 3) Quantum mechanics tells us, and our *gedanken* experiment confirms, that quantum particles do not carry instruction sets (hidden variables) and therefore these properties cannot exist until the point they are measured[9]. Any attempts to measure or copy the state of a quantum particle must by necessity destroy some of the information about the original state. None of these properties exist in classical systems and in the next section we will see how this can be exploited for cryptographic purposes.

Secure Cryptographic Key Exchange using Qubits

So how can we use the properties of quantum particles for encryption purposes? First, picture our entangled pair of quantum particles again. Suppose that Alice and Bob[10] sit at the two detectors described in the last section[11]. Alice pushes the button on the source and entangled quantum particles are generated and propagated toward the two detectors. Instead of flashing red and green, think of the detectors as displaying a "1" or a "0". Bob and Alice each independently set the switches on their detectors in a random fashion before each particle reaches their detectors (one could even use a random quantum process to choose the switch settings as well). Once all the particles have been sent, Bob and Alice compare their switch settings (but not the results of their measurements) for each particle (qubit) they receive. This comparison can take place over a public channel[12].

[9] Bell's Theorem and experiments such as the one described in this section, also raise deep – and controversial – questions regarding the nature of the universe, including concepts such as non-locality and as Einstein called them "spooky actions at a distance". These questions are well beyond the scope of this paper, but if they interest you, the references at the end contain and reference intriguing (yet disturbing) discussions of these issues.

[10] When giving examples in cryptography, instead of referring to person A sending data to person B we refer to "Alice" and "Bob" – preserving our A and B designators while remaining gender balanced if not gender-neutral. The individual who attempts to intercept Alice and Bob's messages is always the ever-tricky "Eve". I believe this is because the first example of malicious hacking was when Eve tricked Adam into eating the apple in the Garden of Eden – it's either that or because Eve stands for "Eavesdropper".

[11] There are other setups that can be used for quantum cryptographic key exchange, but since we have just spent so much time learning the properties of this one, we will stick with it. The principles that apply for this setup transfer to the other setups as well, although the statistics are slightly different.

Alice and Bob know that when their switches happen to be set to the same position, they will both read the same value of the qubit at their detector (a "1" or a "0"). So, by keeping the results of their measurements when their comparison shows they had set their switches the same, they have now exchanged a random string of bits. While a physicist might think that exchanging a random string of bits is of dubious value, a computer scientist (or a physicist thinking like a computer scientist) thinks … "cryptographic key".

Now suppose Eve wants to eavesdrop on this exchange. If she intercepts a qubit intended for Bob and then tries to retransmit an identical qubit she has the following problem. Eve has only a 1 in 3 chance of picking the same switch setting as Alice. If she picks one of the 2 other settings we have seen that she will get the same result as Alice only ¼ of those times. If Alice is randomly picking switch settings this means that Eve's data will match Alice's only ½ the time ($\frac{1}{3}\times 1 + \frac{2}{3}\times\frac{1}{4} = \frac{1}{2}$, just as in our example above). So now, if Eve attempts to re-transmit a qubit to Bob, she will transmit it with the wrong state on average ½ the time. Clearly at this point, poor Bob's crypto-key will not match Alice's and any message that is sent from one will not be decodable by the other[13].

So how do we make this exchange of keys secure? One way to detect a problem is to note that the results at the detectors are governed by the fact that our qubits are correlated with one another (because they are put into an *entangled state* to start) [Ekert, 1991]. If Eve intercepts and then retransmits one of the qubits, she destroys that entangled state. While Alice and Bob do not want to share the results of their measurements when they have chosen identical switch settings (as that would reveal their secret key) they reveal nothing of value (in terms of encryption) if they compare their values for the data where they have different switch settings. Remember that for these settings their results ("1" or "0") should match only ¼ of the time. If however Eve has intercepted, measured, and then retransmitted the qubit intended for Bob, Bob and Alice will find that their results match more often than ¼ of the time (in fact if Eve intercepts every particle and then retransmits her results to Bob, Bob and Alice will find that their results match 3/8 of the time instead of ¼ - a 50% increase in the number of matches).

Another more efficient and straightforward (but less elegant) way to check for eavesdropping is to use some of the data obtained when Alice and Bob have set their switches to the same position [Bennett, 1995; Jennewien 1999; Benjamin, 2000; Mermin 2000]. Remember that when Eve tries to retransmit particles to Bob, she makes an error on average ½ the time. If, before Alice and Bob exchange information using their common key, they also compare some of the results of their measurements, they will quickly detect Eve's tampering. As an example, if Alice and Bob exchange 300 qubits they will find that – on average – they will have set the switches on their detectors the

[12] Note – while we don't care if Eve overhears the public exchange of information after the qubits are sent, we do care that Alice is really communicating with Bob. If Eve is able to completely impersonate Bob in some way then this scheme (along with every other cryptographic system) obviously fails.

[13] One could think of this as a Denial of Service attack – but if Eve can intercept the qubits being transmitted, she already has the ability to just block them rather than wasting time re-transmitting them.

same 1/3 of the time or for about 100 qubits. If Eve has tampered with any of the qubits, there is a 50/50 chance that the measurements Alice and Bob make will disagree. If Alice and Bob compare the results for one of these 100 particles their odds of agreeing will be 1 in 2. If that was all they did, before transmitting their message then Eve would be able to decode Alice's message to Bob about ½ the time (of course, poor Bob would not). If they now compare 2 particles out of the hundred, the odds of both agreeing are ½ x ½ = ¼ and if you continue this you see that the odds of a set of test bits agreeing go down exponentially with the number of test bits used, i.e. – the probability of tampering going undetected = $(½)^n$ where n is the number of test particles used. By using just 10% of the data – in this case 10 particles – the odds of Eve not being detected are $(½)^{10}$ or 1 in a 1024 (in a real system there would be some natural noise in the data that was not necessarily due to tampering – but this procedure would allow you to quantify that noise and determine an upper bound to the amount of potential tampering). If you were to use 100 bits out of a 1000 bit key for testing purposes the odds of tampering going undetected go up to 1 in 10^{30}.

The One-Time Code-Pad

Why is this powerful? By having the ability to exchange a key (random string of bits of arbitrary length) with absolute security before each message is sent, you have created a secure one-time code-pad system [Garfinkel, 1996; Stallings, 1999; Mermin 2000]. While there are a variety of cryptographic procedures that could be applied using such a key a straightforward example of this is the XOR (exclusive OR, $\oplus$) binary operation. A bitwise XOR operation between two binary numbers results in a "1" if either bit is a "1", but not both. Otherwise the result is "0". There are two important features to understand about the XOR binary operation.

1) If you apply an XOR between a coherent message (bit string) and a random Key (random bit string) then the result will be a random bit string.
2) If you apply an XOR between two bit strings, the first being a message and the other being the key, and subsequently XOR this result with the key again, your original message's bit string will be recovered. (note the reverse is also true. If you XOR the encoded bit stream with the original coherent message then the original encoding Key will be recovered).

It is easy to convince yourself that the second property above is true. Here is an example:

Message == M = 10101010
Key = K = 11000101

Encrypted Code == E = M $\oplus$ K == 01101111

Decoded Code == $E \oplus K$ == 01101111 $\oplus$ 11000101 = 10101010 == Message

The first property can also be understood by thinking about what happens if you start with a random string and XOR it with anything else. Even if you XOR a random string with a string of all 0's or all 1's you end up with the original random string or its inverse (which of course is also random).

We can now see that XORing a coherent message with a securely exchanged random one-time key yields an unbreakably encoded message. A brute force attack, where every possible key is applied against the encoded message, is not only impractical (a small 100 bit message would have 2^{100} or 10^{30} possible keys) but since the bit string is truly random applying these keys would yield all possible results for a message of that length, with no way of knowing which was the correct message.

However, to be perfectly secure the key must be at least as long as the message and the key may only be used once (hence the "one-time" part of "one-time code-pad). This can be seen as follows:

If we have two coherent message strings M1 and M2 and one random key, K then applying K to each string yields two encoded messages E1 and E2:

$E1 = M1 \oplus K$
$E2 = M2 \oplus K$

If we then take the XOR of the two encoded messages we get:

$E1 \oplus E2 = (M1 \oplus K) \oplus (M2 \oplus K)$

Since binary operations such as XOR are commutative we can rearrange this:

$= (M1 \oplus M2) \oplus K \oplus K$

But since we know that XORing twice with K just yields the original string we have:

$E2 \oplus E2 = M1 \oplus M2$

Since M1 and M2 are both coherent messages, this bit string is no longer random and standard code-breaking techniques [Stallings, 1999- p.76] (based on things such as linear and differential crypto-analysis] can be used to separate and decode both messages.

Is this practical? The answer, I suppose depends on how badly you wish to protect a piece of data from an eavesdropper. It is now possible to produce qubits (actually polarized photons) and transmit them over tens of kilometers through fiber optic cables without damaging their quantum state. Equipment to measure the quantum states (polarization of the photons) of these particles is also available and cryptographic systems have been constructed. No doubt, there are organizations within the Federal government and perhaps even in the commercial world that have applications where this type of security could be considered appropriate and worth the expense. As with the entire field of cryptography – whereas applications may originally start out as capabilities used only on the most sensitive of projects, as our economy and general lifestyles depend more and more on secure and private digital communications, these capabilities will inevitably find their way into more mainstream applications.

References:

[Aspect, 1981] Aspect, A., Grangier, P., Roger, G., Physical Review Letters, **47**, (1981): 460.

[Barenco *et al.*,1996] Barenco A., Ekert, A.,Sanpera, A., and Machiavello, C., "A short introduction to quantum computation" CQC Introductions: Quantum Computing. http://www.qubit.org/intros/comp/comp.html

[Benjamin, 2000] Benjamin, Simon. "Quantum Cryptography: Single Photons "on Demand" Science, **290** (2000): 2273-2274. Available online at: http://www.sciencemag.org/search.dtl

[Bennett *et al.*, 1993] Bennett, C.H, Brassard, G., Crepeau, C., Jozsa, R., Peres, A., and Wootters, W., "Teleporting an Unknown Quantum State via Dual Classical and EPR Channels", Physical Review Letters **70**, (1993): 1895.

[Bennett, 1995] Bennett, Charles H. "Quantum Information and Computation.", Physics Today, October 1995: 24 – 30.

[Deutsch *et al.*, 1998] Deutsch, David and Ekert, Artur. "Quantum Computation", http://www.qubit.org/intros/PhysicsWord/PhysicsWorld.html , from Physics World, March 1998

[Einstein *et al.*, 1935] Einstein, A., Podolsky, B., and Rosen, N., Physical Review, 47 (1935): 777.

[Ekert, 1991] Ekert, Artur K., "Quantum Cryptography Based on Bell's Theorem", Physical Review Letters, **6**, (1991): 661 – 663.

[Ekert, 1995] Ekert, Artur. "What is Quantum Cryptography" CQC Introductions: Quantum Cryptography. http://www.qubit.org/intros/crypt.html (20 March, 1995).

[Garfinkel *et al.*, 1996] Garfinkel, Simson and Spafford, Gene. Practical UNIX & Internet Security. Sebastopol: O'Reilly & Associates, Inc., 1996.

[Gershenfeld, 2000] Gershenfeld, Neil. The Physics of Information Technology. Cambridge: Cambridge University Press, 2000. 252 – 285

[Grover, 1997] Grover, L.K. "Quantum Mechanics Helps in Searching for a Needle in a Haystack", Physical Review Letters, **79**, 1997: 325 – 328.

[Grover, 1998] Grover, L.K. "Quantum Computers Can Search Rapidly by Using Almost Any Transformation". Physical Review Letters, **80**, 1998: 4329 – 4332.

[Jennewien, 1999] Jennewien, Thomas et al., "Quantum Cryptography with Entangled Photons", preprint – submitted to Physical Review Letters, arXiv:quant-ph/9912117, 28 Dec 1999. http://arXiv.org/abs/quant-ph/?9912117

[Henderson] Henderson, Leah and Vedral Vlatko, "CQC Introductions: Quantum Entanglement", http://www.qubit.org/intros/entang/

[Mermin, 1985] Mermin, N. David. "Is the moon there when nobody looks? Reality and the quantum theory.", Physics Today, April 1985: 38 – 47.

[Mermin, 2000] Mermin, N. David. "Lecture Notes on Quantum Computation and Quantum Information Theory", CS483 - Lecture Notes and Homework Assignments. http://www.lassp.cornell.edu/~cew2/CS483/CS483_home.html (October, 2000).

[Shor, 1997] Shor, P.W. "Polynomial-time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum computer". SIAM Journal on Computing, **26**, 1997: 1484 – 1509.

[Stallings, 1999] Stallings, William. Cryptography and Network Security, Principles and Practice, Second Edition. Upper Saddle River: Prentice Hall, Inc, 1999.