Quantum Encryption

Table of Contents

Introduction

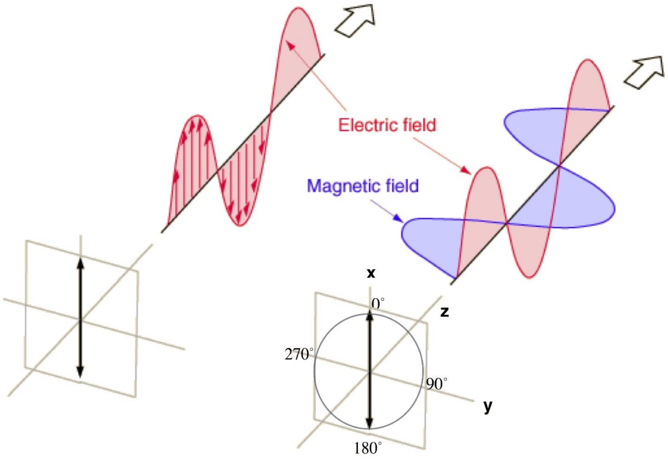
Currently, public key encryption, especially use of the RSA and elliptical curve algorithms, are the state of the art. Although there are many documented cases of successful attacks on these methods, they are uniformly the result of suboptimal implementation and not because a deficiency in the methods themselves. Indeed, if executed correctly, the key sizes in use today should, theoretically, not be susceptible to cyber attacks using current computer technology. However, there is concern that with technological advances, present day encryption techniques may become vulnerable. Therefore, the cyber security community is constantly attempting to develop new encryption schemes to prevent future cyber invasions. One of the most fascinating of these new schemes is quantum encryption. In this article, I will attempt to provide an introduction to the theory that underlies this budding technique.

Concepts in quantum mechanics

Before we delve into a discussion of quantum encryption, we'll need to consider some basic facts about quantum mechanics.

In quantum mechanics, one cannot predict the results of a single event with certainty, only with some probability. Consider a particle. One cannot determine with certainty where it will be in the next instance; only with some probability. For example, a particle may have a 75% chance of being in a lab in New York, a 10% chance of being at a restaurant in Los Angeles, 5% chance of being on Alpha Centauri and variable small fractions of a percent of being everywhere else in the universe. The chances of the particle being found at varying locations may or may not fluctuate from moment to moment but will be still be indeterminate; that is, until it's location is measured, at which time the particle's location will be known with 100% certainty. Such behavior is true of other properties of a particle besides position, properties like momentum and energy. The properties that are of central concern for our discussion here are photon polarization and electron spin. Let's consider photon polarization first.

Photon polarization



A photon is a particle of light. It's electromagnetic energy and consists of an electrical field and a magnetic field. The strength (or amplitude) of the electric field wavers back and forth regularly (that is, oscillates) in the x-z plane. The amplitude of the magnetic field oscillates in the y-z plane and the photon moves in the z direction. The electric and magnetic fields always oscillate in directions perpendicular to each other and the direction of motion of the photon is always perpendicular to the direction of oscillation of the electric and magnetic fields. According to the conventions shown in the diagram, if the electric field oscillates in the x-z plane, we say that the photon's plane of polarization is at 0 degrees. Or, another way of saying it is that the photon is polarized in the zero degree direction. Now suppose we rotate the plane of polarization clockwise such that the new plane of polarization makes a 45 degree angle with the x-z plane. The angle of polarization of the light is now said to be 45 degrees. Rotate the polarization plane 90 degrees and the angle of polarization is 90 degrees; Rotate it 123 degrees and the angle of polarization is 123 degrees, and so forth.

There are devices called polarization filters that function as follows: they will let a photon through 100% of the time if it is polarized at the angle at which the device is set; it will block the photon 100% of the time if it is set at an angle 90 degrees different from the angle at which the photon is polarized; and it will let the photon through some but not all of the time, if the angle of polarization differs from the filter's setting by some angle, theta, other than 90 degrees, the probability of it getting through being given by the square of the cosine of theta (for an explanation of why this is, click here). Individual photons will either get through or not get through but if you send in enough photons, then the percentage that get through will be the same as the probability of an individual photon getting through (or close to it). And one more thing: once a photon passes through a filter, it assumes the polarization angle at which the filter was set. That is, a photon that's polarized at 45° before it reaches a 90° filter will emerge from the filter polarized at 90°, if it passes through. In the vernacular of standard interpretation of quantum mechanics, the interaction with the filter (which essentially constitutes a measurement, if we care to look) causes collapse of the photon's wave function to 90°.

Prepare and measure quantum key distribution

How is this used for encryption? Here's the basic idea. Consider Alice, who wants to send a message to Bob. Alice has 4 single photon light-emitting diodes (spLED) that can generate single photons polarized at a given angle. Bob, on the receiving end, has two things: 1) polarizion filters and 3) a photon detector. More specifically, Bob has two types of filters. One—let's call it a + filter—can be set to either 0° or 90°. The other type of filter she has—call it an X filter—can be set to either 45° or 135°. The type of filter used, + or X, determines what's called the basis associated with that photon.

So Alice generates photons, one-by-one, polarized at one of four angles (0°, 90°, 45° or 135°) and sends them to Bob. The choice of polarization angle by Alice is randomly determined. After she sends the photon, she records 3 pieces of data about each photon she sends. First, she associates a number with each photon to identify it. Second, she assigns a digital code to each photon depending on its angle of polarization. She does the latter as follows: if the photon she sends is polarized at 0° or 45°, she assigns a value of 1 and if the photon is polarized at 90° or 135°, she assigns a value of 0. Third, for each photon, Alice records what's called a basis according to the following protocol: if the photon is polarized at 0° or 90° she designates the basis as "+"; if the photon is polarized at 45° or 135°, she designates the basis as "X". (The reason that she records the information the way she does, hopefully, will become apparent soon.)

Once Alice emits a photon, she sends the photon over an unsecured connection to Bob. Bob, on the other end, has no idea at what angle the photon was polarized, so he picks a filter (or basis) with which to measure the photon (either + or X) at random. If he chooses to measure the photon in the + basis, he sets his filter to either 0° or 90°. If he chooses to measure the photon in the X basis, he sets his filter to either 45° or 135°. He then checks to see whether or not the photon passes through the filter. If it does, it registers on a detector he has previously placed behind the filter. If the photon registers on the detector, Bob assigns that photon a digital value of 1. If it does not register, he records a 0.

Now if the incoming photon is polarized at 0°, and he chooses to use the + filter (set at 0°) it will register on the detector with 100% probability. If Bob's filter is set at 90° for the measurement, none of the photons will get through to the detector. That's easy enough. However, if he uses the X filter to measure, and the filter is set at 45°, then the photon has a 50% chance of registering. Why? According to the classic interpretation of quantum physics—which works well in describing the phenomena—the photon is in what's called a superimposition of states, 50% in the 45° polarization state and 50% in the 135° polarization state. It doesn't assume a definite state until a measurement is made. If, at the time of the measurement, it assumes the 45° state, the photon passes through the filter (which is set to 45°). If the photon assumes the 135° polarization state, it does not pass through the filter and does not register on the detector.

On the other hand, if Alice's photon is polarized at 45° and Bob uses his + filter set at 0°, 50% of the time, the photon will pass through the filter and register on the detector and 50% of the time, it won't. Again, this is because the photon initially polarized at 45° is in a superimposition of states—50% polarized at 0° and 50% at 90°. If, at the time of measurement, the photon assumes the 0° state, then it passes through the filter and registers on the detector; if it assumes the 135° state, it won't pass through or register.

Following the same logic, let's consider the other possibilities:

> If Alice's photon is polarized at 0° and Bob uses his X filter set at 135°, the photon will pass through the filter and register 50% of the time; 50% of the time, it won't.
>
> If Alice's photon is polarized at 90° and Bob uses his + filter set at 90°, then the photon will pass through the filter and register 100% of the time.
>
> If Alice's photon is polarized at 90° and Bob uses his + filter set at 0°, then the photon will not pass through the filter or register on the detector.
>
> If Alice's photon is polarized at 90° and Bob uses his X filter set at 45°, the photon will pass through the filter and register 50% of the time; 50% of the time, it won't.

If Alice’s photon is polarized at 90° and Bob uses his X filter set at 135°, the photon will pass through the filter and register 50% of the time; 50% of the time, it won’t.

If Alice’s photon is at 45° and Bob uses the X filter set at 45°, it will pass through and register 100% of the time.

If Alice’s photon is at 45° and Bob’s filter is X set at 135°, it get’s blocked 100%.

If Alices photon is at 45° and Bob uses the + filter, set at 90°, 50% will get through and 50% won’t.

If Alice’s photon is at 135° and Bob uses the X filter set at 135°, it will pass through and register 100% of the time.

If Alice’s photon is at 135° and Bob’s filter is X set at 45°, it get’s blocked 100%.

If Alices photon is at 135° and Bob uses the + filter set at 0°, 50% will get through and 50% won’t.

If Alices photon is at 135° and Bob uses the + filter set at 90°, 50% will get through and 50% won’t.

The following is a table that summarizes the information just described:

Polarization of Alice’s Photon	Basis of Bob’s Filter			
	+ (set at 0°)	X (set at 45°)	+ (set at 90°)	X (set at 135°)
0°	1 (100%)	0 (50%) 1 (50%)	0 (100%)	0 (50%) 1 (50%)
90°	0 (100%)	0 (50%) 1 (50%)	1 (100%)	0 (50%) 1 (50%)
45°	0 (50%) 1 (50%)	1 (100%)	0 (50%) 1 (50%)	0 (100%)
135°	0 (50%) 1 (50%)	0 (100%)	0 (50%) 1 (50%)	1 (100%)

As previously stated, the ‘1’s in the table mean the photon got through and registered on the detector; the ‘0’s mean it didn’t.

But the point of this whole exercise is to get a secret key, a string of numbers that is known to Alice and Bob and nobody else. In this case, as you might surmise, it turns out to be a string of zeros and ones.

How is this done? Well, once Bob has made his measurements, for each photon, he also records three pieces of information: photon number, the basis in which he measure (+ of X) and a digital code that indicates whether a photon registered or not (1 if it registered on the detector, 0 if it did not). Then Alice and Bob have a conversation, unsecured, open to the public.

In that conversation, they don’t directly tell each other what their secret key is. Instead, for each photon, Alice tells Bob what basis she used to generate the photon (although she doesn’t tell him at exactly what angle her photon is polarized; for example, she might tell Bob she used the + basis but doesn’t tell him if the photon she sent was polarized at 0° or 90°). Bob, for his part, tells Alice in which basis he measured. From the table, you can see that if the same basis was used to send and receive a photon, they know, with 100% certainty, at what angle Alice’s photon was polarized, and therefore, what digital code they should both use for their secret key.

To see this, consider the following two examples. For both of these examples, assume that, in their conversation, Alice and Bob discover that their basis agree and that, in each case, that basis is the + basis.

In the first case, suppose that Alice’s photon is polarized at 0°. Bob measures with his filter set at 0°. The photon gets through and registers on the detector. Bob reasons that, since he and Alice agree on their basis that Alice’s photon must have been polarized at 0° or 90°. But since the photon got through his 0° filter, Alice’s photon must have been polarized at 0°. Why? Because if it had been polarized at 90°, it would not have passed through his filter. Bob and Alice have agreed in advance that if Alice’s photon is polarized at 0° then that correlates with a secret code digit of 1 and if it is polarized at 90°, that correlates with a secret key digit of 0. Bob has deduced that Alice’s photon was polarized at 0°. Thus, he records a 1 for the secret key digit that stems from that photon.

Let’s look at a second example. In this case, suppose Alice’s photon is polarized at 90°. Bob again measures in the + basis, with the 0° filter. The result is that the photon does not pass through the filter and does not register on the detector. He knows that Alice’s photon must have been polarized at 90°. How? Well, again, he knows that Alice’s basis is the same as his—the + basis. Therefore, her photon must have been polarized at either 0° or 90°. Since the photon did not get through his 0° detector, it must have been polarized at 90°. After all, if it had been polarized at 0°, it would have gotten through his filter and registered on his detector. Since Bob knows that Alice’s photon was polarized at 90°, as per their agreed-upon scheme (record 1 if Alice’s photon is at 0°; record 0 if Alice’s photon is at 90°), Bob records a 0 for the digit in the secret key that corresponds with that photon.

We could go on and see what happens in the other 6 scenarios that could possibly occur but I think you get the concept: if 1) Alice and Bob agree on their basis 2) Alice and Bob agree on a protocol regarding what secret digit to record for each of the angles at which Alice’s sent photon could be polarized and 3) Bob knows at what angle his polarization filter is set for measurement (which, of course, he does), then the secret key that Bob and Alice generate will be the same.

Accordingly, they save the data from photons on which they agree on basis and use that data for their key. On the other hand, if the basis used to generate and receive the photons differ, from the table, the digital codes generated for those photons will agree only 50% of the time, and randomly at that. Under those circumstances, they have no idea whether or not their digital codes agree. Therefore, they throw out this data and don’t use it to make their key.

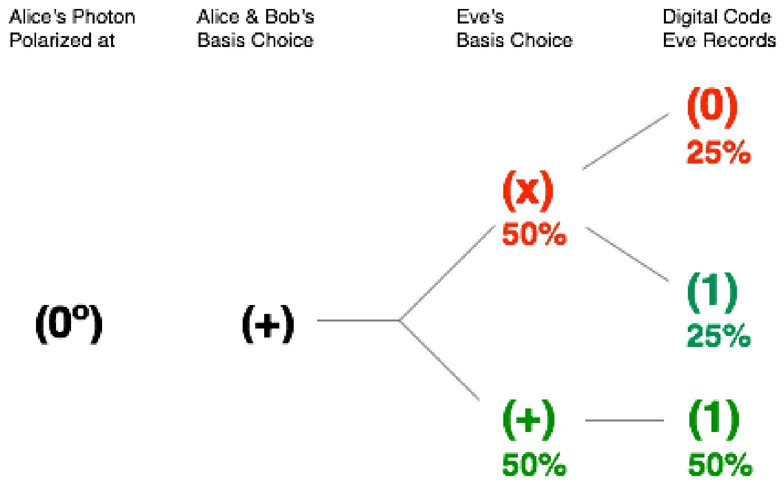
Checking for eavesdroppers

You may be wondering, *if this “conversation” that Alice and Bob have is public knowledge, couldn’t someone intercept Alice’s photons, measure them, wiretap the conversation and figure out the secret key?*

The answer is, *it’s possible, but if enough photons are sent, it’s extremely unlikely*.

Consider an eavesdropper. Call her Eve. Image that Eve is able to intercept Alice's photons, measure them, and send them on to Bob. Say Alice sends out a photon. Eve intercepts it. But this is before Alice and Bob have had their conversation in which they compare notes. So Eve is in the same boat as Bob. She must choose the basis to measure the photon at random. If she chooses the correct basis, then she will be able to correctly infer the digital code (0 or 1) for that photon every time. But since she's choosing her basis at random, and there are two possibilities for choice of basis, her chances of guessing correctly is 50%. However, even if she guesses the basis incorrectly, there is a 50% chance that she will determine the digital code correctly. These odds are true for every photon. Thus, of the cases in which Alice and Bob send and measure a photon with the same basis (i.e. the cases that they will use to compile their secret key), Alice will guess the digital code correctly 75% of the time.

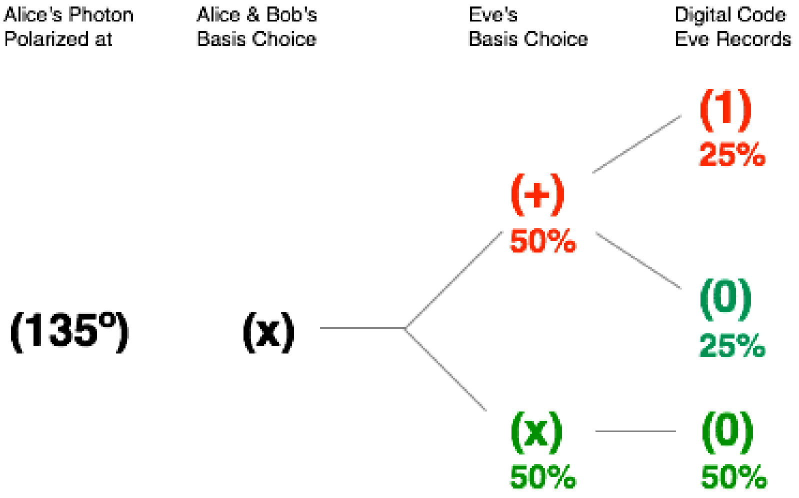
Here is a diagram that may help you see why this is true:



Suppose Alice polarizes her photon at 0° and Bob correctly measures in the + basis. One hundred percent of the time, the photon will pass through his filter and he will record a digital code of 1. Eve, on the other hand, will correctly measure in the + basis only 50% of the time, but when she does, she will correctly guess digital code of 1 every time. However, on the occasions when she chooses the basis incorrectly, by chance, the photon will pass through her filter and she will record the correct digital code (1) one half of the time. One half of 50% is another

25%. Thus, Alice will guess the digital code (1) 75% of the time—50% of the time when she chooses the basis correctly and 25% when she doesn't.

Let's look at another example:



Say Alice polarizes her photon at 135° and Bob correctly measures in the X basis (set at 45°). One hundred percent of the time, the photon will fail to pass through his filter and he will record a digital code of 0. Eve, on the other hand, will correctly measure in the X basis only 50% of the time, but when she does, she will correctly guess the digital code of 0 every time. However, on the occasions when she chooses the basis incorrectly, by chance, the photon will not pass through her filter and she will record the correct digital code, 0, one half of the time. One half of 50% is another 25%. Thus, again, Alice will guess the correct digital code (0) 75% of the time.

We could repeat the argument for photons polarized at 45° and 90°, but I hope it's clear from the above examples that the result will be the same: Eve will guess correctly 75% of the time.

So what are the chances that Eve will correctly guess the entire secret key? Well, it depends on how long the key is. If the key is one digit long then the chance of Eve guessing it is 75%. Two digits long and it's $(0.75) \times (0.75) = (0.75)^2 = 0.56$ = 56%. Three digits and it's lower: $(0.75) \times (0.75) \times (0.75) = (0.75)^3 = 0.42$ or 42%."

From this, we can see a pattern emerging. The formula to determine the likelihood that Eve will resolve the entire secret key (P_E) is:

$$P_E = (0.75)^n$$

where n is the number of photons evaluated in which Alice and Bob use the same basis.

If, for instance, Alice and Bob, use 48 photons for their key, then the chance that Eve will guess it is:

$$P_E = (0.75)^{48} = 0.000001$$

That's about a 1 in a million.

Alice and Bob can also use such an analysis to tell whether someone is eavesdropping. What they would do is take a sample of data from the photons where they agreed on a basis. Theoretically, they should record the same digital code 100% of the time. Therefore, if they find any discrepancies at all, they know that someone is listening in. This is because discrepancies can only occur if Eve guesses wrong. An example of how this could happen is as follows:

Alice sends out a 0° photon. Eve guesses wrong and uses an X filter. The photon hits the X filter in a fifty-fifty superimposition of the 45° and 135° states. Eve sets her filter at 45°. Then 50% of the time, the photon gets through, polarized at 45°, and gets to Bob. But Bob is using the + filter, so 50% of 50% (or 25%) of the time, he measures a 0 instead of a 1. If Eve weren't there, Bob would measure 1 correctly 100% of the time. However, with Eve around, there's a 75% chance that Bob will record the correct answer and 25% chance that he won't. If enough photons are sent, Bob gets 75% right and 25% wrong—same as Eve.

Now, [the total number of photons Alice and Bob evaluate] = [the number of photons where Alice and Bob agree (A)] + [the number of photons where Alice and Bob disagree (D)]. To express this as probabilities, divide both sides by [the total number of photons evaluated]. Mathematically:

$T = D + A$

where,

$A =$ Number of photons on which Alice and Bob agree

$D =$ Number of photons on which Alice and Bob disagree

$T =$ Total number of photons

and

$\frac{T}{T} = \frac{D}{T} + \frac{A}{T}$ so

$1 - \frac{A}{T} = \frac{D}{T}$ where

$\frac{A}{T} =$ probability of agreement

$\frac{D}{T} =$ probability of discrepancy

It follows then that the probability of finding a discrepancy, and thus detecting the presence of Eve (P_D), equals one minus the probability of agreement. But we already said, the probability of agreement between Alice and Bob when Eve is listening equals the probability that Eve guesses right. And I already told you that that probability equals $(0.75)^n$. Therefore:

$$P_D = 1 - (0.75)^n$$

So for example, if Alice and Bob wanted to make the probability of detecting Eve (P_D) = 0.999999, they'd use n = 48 (i.e., sample data on 48 of the photons in which they employed the same basis; recall that $(0.75)^{48}$ = 0.000001; 1 – 0.000001 = 0.999999). If they found discrepancies, then they'd know Eve was eavesdropping. If not, then they could be 99.9999% certain that Eve was not listening. If this degree of certainty were acceptable to them, then they'd use their data for a secret key (although they would throw out the 48 data points that they used to check for an eavesdropper since that analysis would have been done publicly).

Once satisfied that their private key is secure, Alice can send Bob pick out 256 or so photons on which they agree on basis and generate a 256 digit string of 0's and 1's; a so-called 256 bit symmetric key. This key can then be used to encrypt an actual message.

Use of quantum keys for encryption

How? Well, each character of the message is coded as a number. There's actually a standard that most everyone uses called the ASCII standard (ASCII = American Standard Code for Information Interchange)[1].

How is the symmetric key encrypt the message using the ASCII code? Easy. Multiply the ASCII code for the text of the message by the symmetric key to get a new number (= the encrypted message).

Security of quantum key distribution

How secure is such symmetric key encryption? To give you an idea, if an attacker attempts a brute force attack on a 256 bit key (that is, tried every possible combination for each digit), it would take about 10^{57} years. How did we arrive at that number? As follows:

To guess every digit of a 256 bit symmetric key, an intruder's computer would have to try up to 2^{256} number combinations.

First, approximate 2^{256} in decimal form. To do this, find the exponent that we have to raise 10 to to get approximately 2^{256}. Mathematically, this can be written as

$10^x = 2^{256}$;

We need to find x in the above equation. x is the exponent to which we need to raise 10 to get 2^{256}. But the exponent to which we need to raise 10 to get 2^{256}, by definition, is the logarithm to the base 10 of 2^{256}.

$x = log_{10} 2^{256}$; use the logarithm change of base rule[2]

$log_{10} 2^{256} = \frac{log_2 2^{256}}{log_2 10}$; use logarithm power rule[2]

$log_{10} 2^{256} = \frac{256 log_2 2}{log_2 10} = \frac{256 \cdot 1}{log_2 10}$; use a calculator to simplify the expression on the right

$$\frac{256}{log_2 10} \approx \frac{256}{0.301} \approx 77$$

So $x \approx 77$. That means that we would need to try as many as approximately 10^{77} combinations to guess a 256 bit symmetric key.

Now back to our original question: how long would that take? Well, in a previous article[3], we determined that a decent computer can perform around 10^{12} operations per second. We have approximately 10^{77} operations to perform, so:

$$\frac{10^{77}\ steps}{10^{12} \frac{steps}{second}} = \frac{10^{77}}{10^{12}} \cdot \frac{steps}{\frac{steps}{second}} = 10^{65} seconds$$

Next, we need to figure out how many years 10^{65} seconds represents:

$$60 \frac{seconds}{minute} \cdot 60 \frac{minutes}{hour} \cdot 24 \frac{hours}{day} \cdot 365 \frac{days}{year} = 31,536,000 \frac{seconds}{year} = 3.1536 \times 10^7 \frac{seconds}{year}$$

Finally, we divide our number of seconds by the number of seconds per year to find up to how many years it might take to crack the code:

$$\frac{10^{65} seconds}{3.1536 \times 10^7 \frac{seconds}{year}} \approx 0.317 \times 10^{58}\ years = 3.17 \times 10^{57}\ years$$

There are other strategies that can be used to try to decrypt a 256 bit symmetric key. A brief overview of these strategies can be found elsewhere, one of which is at this site from Clemson University[4]. However, when symmetric key encryption is implemented properly, deciphering a message encoded with it is nearly impossible using current technology.

Quantum entanglement protocol

Note that there is another way to implement quantum encryption; that is, to make use of quantum entanglement[5]. Entanglement can be seen in a number of particle systems and particle characteristics but the one most applicable to quantum encryption is photon polarization.

Basics of quantum entanglement

If you shoot a strong laser beam at a beta-barium borate crystal, most of the photons will pass straight through. However, as small portion of the photons undergo what is called spontaneous parametric down-conversion (SPDC)[6]. That is, they are split into two photons - sent off in different directions, at specific (spatial) angles - each having half the energy of the original photon but each polarized opposite to the other. For example, if one photon (called the signal photon) is polarized at an angle of 0°, then the other (called the idler photon) is polarized at 90°. If the signal photon is polarized at 45° then the idler is polarized at 135°, and so on. This is called type II SPDC.

On the other hand, if the laser beam is directed at a potassium dihydrogen phosphate crystal, then some of these photons also become entangled. But this time, they polarized at the same angle. This is called type I SPDC.

However, the signal and idler photons so produced don’t just become polarized at a given specific angle. They assume a superimposition of states (i.e., they each assume all possible polarization angles - at the same time!). Furthermore, they maintain this superimposition of states until they’re measured, at which time they assume either opposite (anticorrelated) polarization angles if they’ve undergone type II SPDC or the same polarization angle (correlated) if they've undergone type I SPDC. And that happens simultaneously. It doesn't matter how far apart the photons are when they're measured. One could be on earth and the other on Alpha Centauri 4.367 light-years from earth (meaning that it would take photons of light - which travel at the speed of light, 3×10^8 meters/second, the fastest that anything in the universe can travel - 4.367 years to travel from one entangled photon to the other). When one photon, say the one on earth, is measured, the other photon, on Alpha Centauri, assumes either the anticorrelated state of polarization (with type II SPDC) or the correlated state of polarization (with type I SPDC). Immediately. Before any signal can be sent between them to tell the entangled partner how to behave. Albert Einstein called it "spooky action at a distance."

Use of quantum entanglement for key distribution

Perhaps you can anticipate how this might be used for quantum key distribution. Consider a source of entangled photons, located between Alice and Bob. For convenience, we'll assume that they're created by type I SPDC so that their polarizations are positively correlated. One photon of the entangled pair is sent to Alice and the other is sent to Bob. Like in our previous example, both Alice and Bob have two types of polarization filters that they can use for measurement: a + filter that can be set at either 0° of 90°, and an X filter that can be set to 45° or 135°. If a photon gets through the 0° or 45° filters, they record a digital code of 1. If a photon gets through the 90° or 135° filters, they record a digital code of 0. After collecting data on a large number of photons, Alice and Bob have a public conversation in which they compare the basis in which they measured each photon. As in our previous example, they keep data from photons in which they measured in the same basis and discard data in which their measurement basis differ. Because, for their saved data, the photon that Alice and Bob receive are of the same polarization, and because they measure in the same basis, they can come up with a digital code that is identical.

For example, suppose that for a specific photon, Alice and Bob, after their public conversation, agree that they measured in the same basis. Suppose that this photon got through Alice’s 0° filter. When it did, Alice recorded a 1 for her digital code. Because Bob also measured in the + basis, he would have had to have measured using either a 0° filter or a 90° filter. Because the photon that reached Bob was entangled with the photon that reached Alice, as soon as Alice measured her photon, the photon that reached Bob would have become polarized at exactly the same angle as Alice’s. Thus, in this case, the photon that reached Bob would have been polarized at 0°. If Bob used his 0° filter to measure, with 100% certainty, the photon will have gotten through. If he used his 90° filter, with 100% certainty, the photon will have not gotten through. Either way, Bob knows that the photon that reached him was polarized at 0°. Therefore, he also records a 1.

In contrast, suppose a given photon got through Alice’s 135° filter and she recorded a digital code of 0. Since, after their public conversation, Alice and Bob agree that they measured in the same basis, Bob will had to have measured using either his 45° or 135° filter. Although Bob doesn’t know it, *we* know that because Alice’s and Bob’s photons were entangle, the photon of the entangled pair that reached Bob would also have been polarized at 135°. If Bob measured at 45°, then, with 100% certainty, the photon that reached him will not have passed through his filter. But if he measured at 135°, then the photon will have gotten through. Either way, again, Bob knows that the photon that reached him was polarized at 135°. Therefore, he records a digital code of 0, same as Alice.

We could go through every combination, but hopefully you can see that, if we did, the results would be the same as the above examples: Bob and Alice will record the same digital code for each photon on which they agree on basis.

Before they decide to use their code, Bob and Alice go through a security analysis, as outlined previously. If they conclude with a sufficient degree of certainty that their are no intruders, then they use their symmetric key to encrypt their message.

Conclusion

In this article, I have described the basics of quantum encryption. In theory, if implemented correctly, this encryption technique should be impossible to break. You may find it surprising, then, that quantum key distribution and encryption are rarely used today. The reason is that the technology needed to make this method of encryption functional is immature. The main problem, currently, is the distance over which a quantum encryption system will work - it’s too short. This is because, as photons travel from their source to their intended target in such a system, they tend to interact with other particles. In so doing, their polarization can be changed. Despite this shortcoming, because of the technique’s potential, considerable effort is being expended to solve this and other problems that currently plague this method. At any rate, even if the technique is currently of little practical utility, I think you will agree that the concepts that underlie quantum key distribution and encryption are fascinating and fun to ponder.

References

1. ASCII
   https://en.wikipedia.org/wiki/ASCII

2. Logarithms
   https://samartigliere.com/computer-science/rsa-encryption-1/

3. Computer operations per second
   https://samartigliere.com/computer-science/rsa-encryption-2/

4. Methods to attack symmetric key encryption
   https://www.cs.clemson.edu/course/cpsc424/material/Cryptography/Attacks%20on%20Symmetric%20Key.pdf

5. Quantum entanglement
   https://en.wikipedia.org/wiki/Quantum_entanglement

6. Spontaneous parametric down-conversion
   https://en.wikipedia.org/wiki/Spontaneous_parametric_down-conversion