An Introduction to Quantum Cryptography

Christos Karageorgiou Kaneen

School of Electrical and Computer Engineering,
Technical University of Crete

ckarageorgkaneen@gmail.com

June, 2018

Abstract

This paper was written as part of a Quantum Technology course project with the attempt of providing a gentle introduction to the field of quantum cryptography, focusing on the fundamental quantum key distribution method underlying it. It is ideally aimed towards an undergraduate-level audience familiarized with basic quantum computation notation and operations.

Contents

1 Introduction

1.1 A brief overview

Quantum cryptography deals with the exploitation of quantum mechanical properties of elementary particles, such as photons, for accomplishing cryptographic communication tasks, such as the encryption and decryption of information at the ends of both the sender and the receiver, named Alice and Bob, respectively, by ensuring the confidentiality of the transmission. The advantage quantum mechanical methods over classical ones mainly has to do with the innate spontaneity of certain of the former's unique properties, whose realization render the latter extremely time-consuming, in comparison. For instance, the no-cloning theorem, combined with the inability of reading data encoded in a quantum state without changing it, make it possible to detect eavesdropping attempts, aka Eves. Despite there being many advances in methods and protocols over the years, such as quantum coin-flipping, quantum commitment, the bounded and noisy quantum-storage models, position-based quantum cryptography, device-independent quantum cryptography, post-quantum cryptography, etc., this paper focuses on the most important to-date and widely-applied secure communication scheme, called quantum key distribution (QKD). It involves two parties being able to produce a shared random secret key that can be used to encrypt ("lock") and decrypt ("unlock") the data bits to be communicated between two parties. In classical systems, cryptographical keys are generated using mathematical algorithms that are very hard (though not impossible) to break. Whereas, quantum cryptography uses a method of key distribution that relies on the laws of quantum physics in order to create a key. Although not completely hacker-proof, quantum cryptography offers huge advantages over traditional methods. It has also been hypothesized, though not at the time of writing fully proven, that currently used popular public-key encryption and signature methods, such as ellipticcurve cryptography (ECC) and RSA, can be broken by quantum adversaries.

1.2 Classical cryptography

Classical cryptography can be divided into several fields of study, two of which are of particular interest to us: symmetric-key and public-key cryptography. The former, and oldest of the two, involves both, Alice and Bob, sharing a common key, while, the latter involves using a pair of keys:

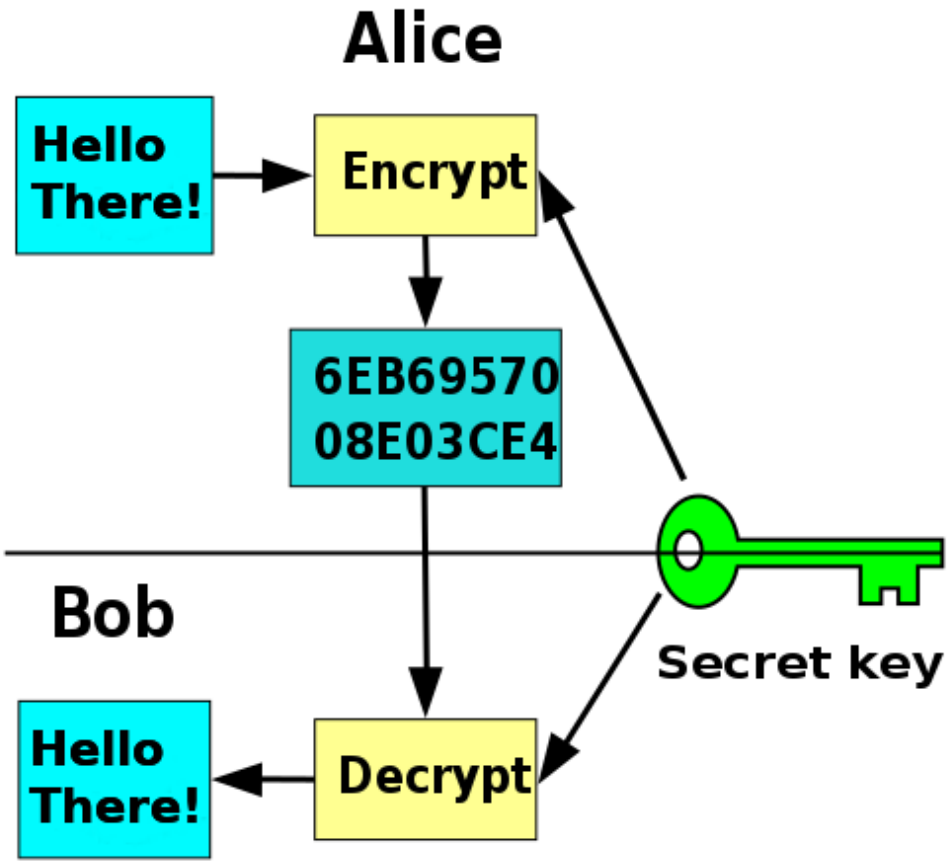

Figure 1: A popular symmetric-key encryption method: Advanced Encryption Standard (AES).

public and private, where anyone holding the public key can encrypt the data

bits, but which only the holder of the private key can decrypt. And thus,

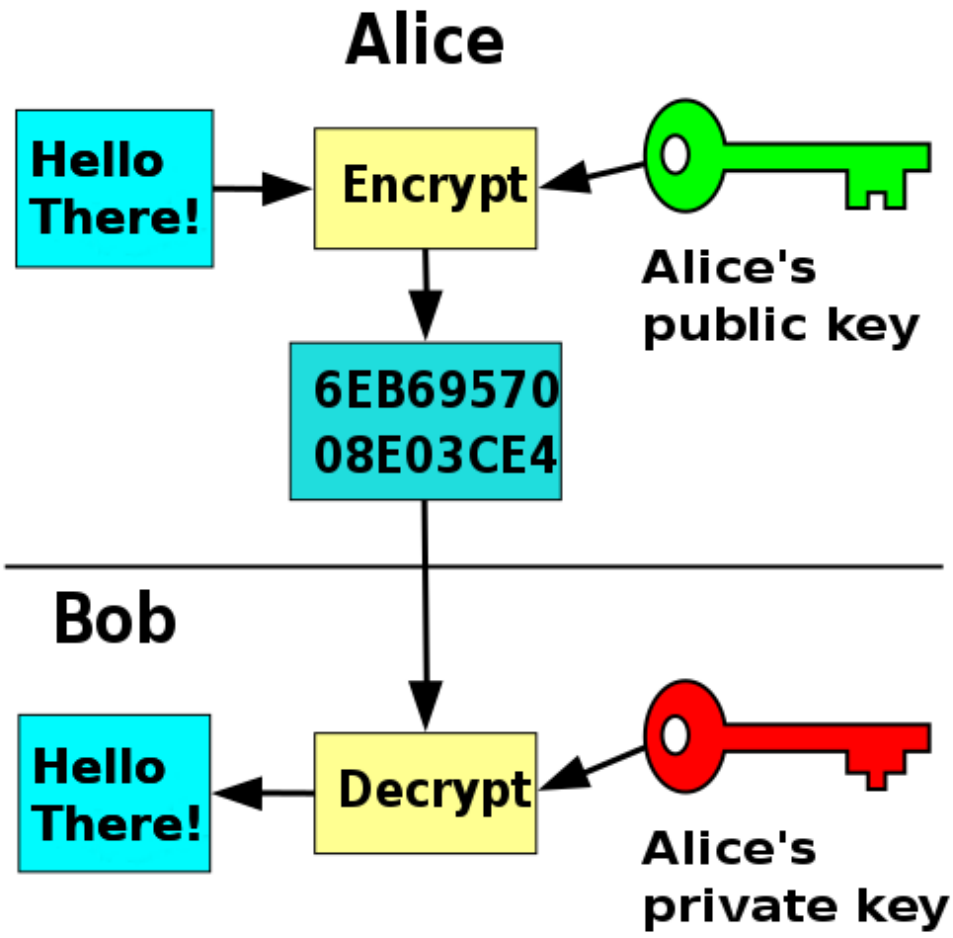

Figure 2: Popular examples of public-key encryption: RSA (Rivest-Shamir-Adleman) and Elliptic-curve cryptography (ECC).

the security wholly depends on the secrecy of the private key.

Before reviewing QKD, we will take a look at some examples of encrypting and decrypting data. We will assume two parties, Alice and Bob, who want to share a private message over an public channel. Using a trivial method we generate a random integer key k to which we can then add each message character in order to encrypt it. Let's represent the capital letters

of the alphabet using binary encoding:
$2^{\mathbf{4}} = 16 < (\#\ \textit{letters in alphabet}) = 26 < 2^5 = 32 \rightarrow (\#\ \textit{encoding bits}) = \mathbf{5}$:

$$\mathbf{A} \rightarrow 0000,\ \mathbf{B} \rightarrow 0001,\ \mathbf{C} \rightarrow 0010,\ \mathbf{D} \rightarrow 0011, \text{ etc.}$$

But, since the communication channel is public, Eve can easily tap into the line (e.g. optical fiber) and steal the data that is being transmitted without the parties realizing it.

So, how can the parties secure the message? A very simple means of securing the message is to generate an integer key k to add to each character before transmission so that when Bob receives the message, he need only subtract k from each character to retrieve the original copy. That makes it inconvenient for Eve to steal any data without knowing k.

Example: Alice encrypts message **m** by adding key **k** to each of its characters **c**:

$$\mathbf{m} = \mathbf{c} + \mathbf{k}$$

Let's say Alice wants to share **HELLO** with Bob, and $k = 3$ (0011):

$$\begin{gathered}\mathbf{H} \rightarrow 00111 \rightarrow 01010 \rightarrow \mathbf{K} \\ \mathbf{E} \rightarrow 00100 \rightarrow 00111 \rightarrow \mathbf{H} \\ \mathbf{L} \rightarrow 01011 \rightarrow 01110 \rightarrow \mathbf{O} \\ \mathbf{L} \rightarrow 01011 \rightarrow 01110 \rightarrow \mathbf{O} \\ \mathbf{O} \rightarrow 01110 \rightarrow 10001 \rightarrow \mathbf{R}\end{gathered}$$

Alice encrypts **HELLO** $\rightarrow$ **KHOOR**, transmits it over the public channel where Eve might eavesdrop, but if she does not know the key she will not be able to understand the message. Bob then receives it and decrypts it back to the original message **KHOOR** $\rightarrow$ **HELLO** by subtracting the shared key k:

$$\mathbf{m} = \mathbf{c} - \mathbf{k}$$

Of course, the risk of eavesdropping can be minimized by employing a more sophisticated method. Let's take a look at a more realistic example: RSA, which involves four steps: key generation, key distribution, encryption, decryption.

Example:

1. ***Key generation***:
   - Choose two distinct prime numbers, such as: $p = 61$, $q = 53$
   - Compute $n = p \times q = 3233$
   - Compute the totient of the product $\lambda(n) = lcm(p-1, q-1)$: $\lambda(3233) = lcm(60, 52) = 780$
   - Choose any number $1 < e < \lambda(n)$ that is coprime to $\lambda(n)$: Let's choose $e = 17$
   - Compute d, where $d \times e \equiv 1 (mod\ \lambda(n))$: Lets choose $d = 413$
2. ***Key distribution***:
   Bob publicly transmits his public key (n, e) to Alice (so she can encrypt the message), whereas Bob's private key (n, d) (that decrypts the message) is never revealed.
3. ***Encryption***:
   The public key is $(n = 3233, e = 17)$, and so for a padded plain-text message m, the encryption function is:

   $$c(m) = (m^e)\ mod\ n = (m^{17})\ mod\ 3233$$
4. ***Decryption***:
   The private key is $(n = 3233, d = 413)$. For an encrypted cipher-text c, the decryption function is:

   $$m(c) = (c^d)\ mod\ n = (c^{413})\ mod\ 3233$$

   Thus, to encrypt, lets say, $m = 65$: $c(65) = 2790$
   And to decrypt $c = 2790$: $m(2790) = 65$

The problem: Although it is extremely difficult (very-very slow) for a classical computer to factor a sufficiently large enough n into its p and q, Shor's

algorithm demonstrates that a quantum computer can easily accomplish that task. Meaning, that for a quantum system there arises the need for a better-suited cryptographic scheme.

2 Quantum Key Distribution

Quantum key distribution (QKD) is a technique that allows two parties to share a common secret key that can be used for encryption, on Alices part, and decryption, on Bob's, so that, while being transmitted, the data remains incomprehensible to any observer who does not know the key. As mentioned earlier, the main idea of how key-confidentiality is ensured

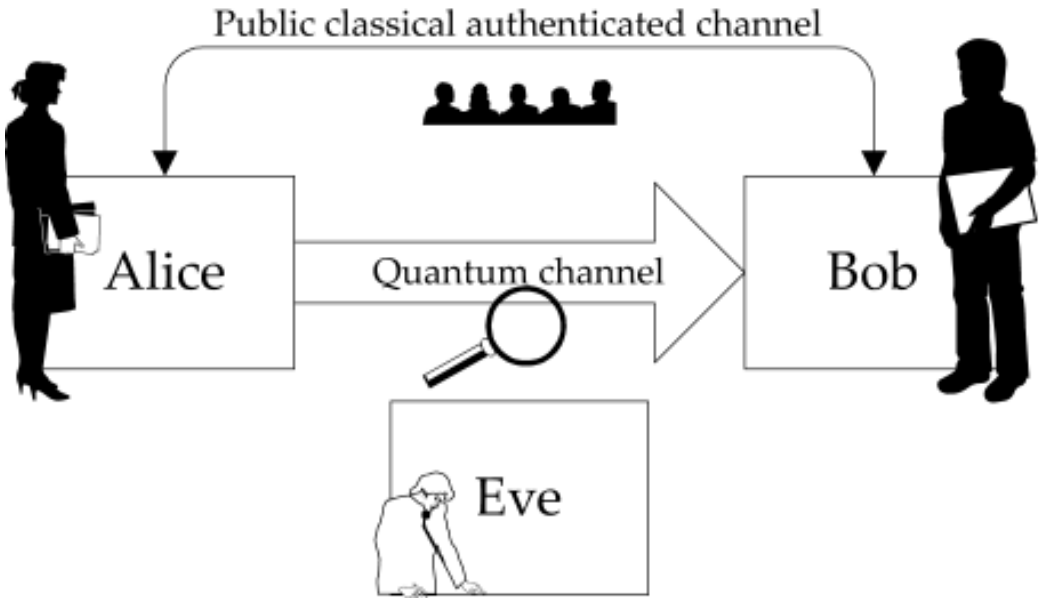

Figure 3: QKD overview

revolves around the quantum mechanical principles wherein if Eve tries to determine the key, it is sure that she will be detected by the parties (who will then go on to discard the key). If however, no tapping attempt is made, the secrecy of the distributed key is guaranteed.

QKD requires a non-classical transmission channel on which quantum particles can be transmitted between Alice and Bob. Although, theoretically, any quantum particle can be used, in practice, those carriers are usually photons, with the channel being either an optical fiber or the open air. In the photons, Alice will encode random bits of information that will make up the key, so that no Eve can predict any of the transmitted key-bits. For simplicity's sake, it will be presupposed that "truly random" bits (0s and 1s) are used. After the transmission, Alice and Bob will compare

bases and will only keep the identical-basis bits (a process called *sifting*), a fraction of which will then be checked for transmission errors (a process called *error correction*), including ones caused by eavesdropping. In such a case, no fundamental problem arises, as any Eve is guaranteeably detectable (through *error correction*), after which Alice and Bob, only in the worst case scenario, will need to recover a fresh secret key, out of the bits that are unknown to Eve or regenerate one anew, choices depending on pre-decided bit-error threshold parameters. To make things easier, it is assumed, that Alice and Bob do not have access to a private channel (as is the case in most realistic scenarios where applicability is to be sought after), with a public classical authenticated channel being used, instead. It has been proven that the confidentiality of data is absolutely guaranteed when the length of the encryption key is as long as the message to be transmitted and it is never reused for future messages; that is where the usefulness of QKD comes into effect.

To be more precise, the confidentiality of the transmitted data is ensured by two parts: the quantum-distributed key and the encryption protocol. QKD is only responsible for key distribution, meaning that its goal is guaranteeing the secrecy of a distributed key. Extra mechanisms involving the manipulation of the data (encryption/decryption - with the help of that secret key), will be discussed with the BB84 and E91 protocols, to be glimpsed upon further on.

3 QKD Protocols

3.1 BB84

3.1.1 Communicating the key

In order to generate the key that will be sent to Bob, Alice creates a random string of $2n$ qubits encoded in polarized photons and emits them. She chooses a specific polarization for each photon among four possibilities, two pairs of which are associated with two different linear polarization bases: $\{|0\rangle, |1\rangle\}$ (or '+') and $\{|+\rangle, |-\rangle\}$ (or '×'). Two can be described as being along the x, y axes, often denoted as $\uparrow$ (Vertical) and $\rightarrow$ (Horizontal), while the other two polarizations are at a $+45°$ orientation from the x and y axes and are usually denoted as $\nwarrow$ (Left) and $\nearrow$ (Right). Each pair corresponds to two orthogonal (90° difference) polarizations. Furthermore, the two pairs correspond to two separate polarizing beam splitter orientations, 45° from each other.

$\|\rightarrow\rangle = \|0\rangle$	$\|\uparrow\rangle = \|1\rangle$
$\|\nwarrow\rangle = \frac{(\|\rightarrow\rangle + \|\uparrow\rangle)}{\sqrt{2}} = \|+\rangle$	$\|\nearrow\rangle = \frac{(\|\rightarrow\rangle - \|\uparrow\rangle)}{\sqrt{2}} = \|-\rangle$

When Bob receives a photon, he realizes its polarization with a polarization beam splitter placed at a random orientation: either the vertical $\{\uparrow, \rightarrow\}$ or the 45^o $\{\nwarrow, \nearrow\}$. If his choice corresponds to the polarization used by Alice during transmission, he obtains the result corresponding to the value chosen and sent by Alice. E.g. If Alice sends a photon with a $\{\uparrow, \rightarrow\}$ polarization and Bob places his beam splitter at the 45° $\{\nwarrow, \nearrow\}$ orientation, then he will obtain a random result, uncorrelated to Alice's initial choice. So, retrieving the corrent data bits that were sent by Alice depends on his choosing as a measuring basis one that corresponds to the polarization basis chosen by Alice. But, how will Bob know which qubits he received are the correct ones? The answer is twofold. The first process is called *reconciliation* or *sifting*: In order for Alice and Bob to agree upon the congruent data bits, they must first compare their bases and keep only the bits corresponding to their specific matching bases. It suffices for Bob to announce his chosen bases on the public channel and for Alice to reply with the ones that were correct (same as her polarization bases), prompting Bob to discard bits corresponding to the rest (non-corresponding bases). Ideally, if there was no eavesdropping, both are left with an identical key (see Fig. 4). Realistically, Bob is left with

a key composed of bits measured using identical bases. That key will then have to pass through the second process, *error correction*. In both cases, the resulting key, produced by discarding the bits where Alice and Bobs bases differ, is called the *sifted key*.

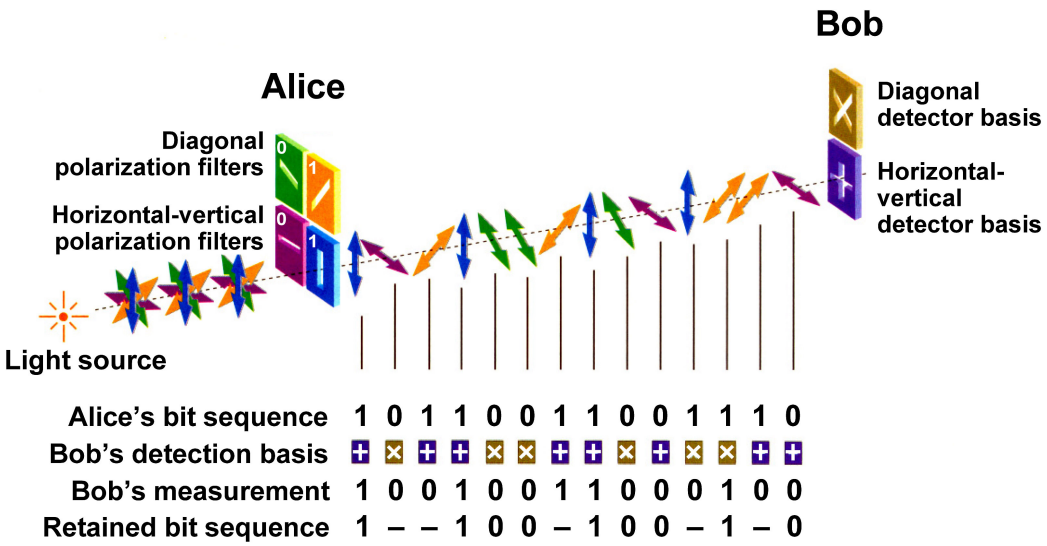

Figure 4: An ideal QKD, with no Eve

It shall be seen that if specific communicated and compared qubits of Bob's *sifted key* differ despite their bases being identical, it will mean that someone has been eavesdropping.

3.1.2 Detecting an eavesdropper

As already mentioned, due to fundamental quantum principles exploited by this protocol, it can be assured once a raw copy of the key bits has been obtained, that no data has been tapped. An unavoidable problem with classical communication is the man-in-the-middle attack, commonly known up to now as eavesdropping. It is an attack on a communication channel where a third party, Eve, makes independent connections with other parties and relays messages between them, giving the impression that they are communicating directly to each other. Let Alice and Bob (as usual) be two parties who wish to communicate over a channel and let the eavesdropper Eve (as usual, again) be the third party who wishes to intercept the conversation. Initially, Alice requests Bob's public key. Bob sends the key, but Eve is able to intercept it. Eve then passes her own public key onto Alice, claiming to be Bob. Alice encrypts the message with Eve's key and passes the encrypted message onto Eve (unknowingly). Eve then decrypts the message and encrypts it with Bob's public key. When Bob receives the message, he believes it is coming directly from Alice.

For the sake of understanding how Alice and Bob are safe from Eve, let us play devil's advocate by assuming her position. By pretending to be Eve, we will try to obtain the information intended for Bob, but secretly (without being detected). Thus, according to what has been mentioned so far, if we intercept a polarized photon (being sent from Alice to Bob) and make a polarization measurement upon it, Bob will simply receive a useless piece of data (post-measurement qubits are said to be destroyed). With that in mind, a smarter post-measurement move would be to resend a photon to Bob (so its superposition does not collapse) with the polarization basis just used to measure the previous one, so that if it "survives" *sifting* and makes it to the final, accepted key (communicated on the public channel), we will know that the qubit we spied on was part of the key. What Bob can do, faced with such a problem, is to sacrifice a randomly chosen subset of qubits of the "sifted key" (the one they agreed on, after the first sifting) and send the remaining subset to Alice through the public channel. Once Alice receives the remaining subset, she will be able to determine whether or not the initial key was eavesdropped, by the second process; "error correction". How does it work? "Error" correction simply utilizes the fact that there are cases when Eve happens to choose a different polarization orientation (resend basis) than the one chosen by Alice (encoding basis). Such cases are

"Datum" 2, 4 and 5 of Fig. 5. Remember, that prior to *error correction*, the qubits that Alice and Bob hold are a randomly selected subset of the *sifted key*. In the Fig. 5 example and in general, the fact that the result measured by Eve is random is combined with the fact that in half of the cases, Alice finds a wrong polarization in Bob's qubits despite their corresponding bases being identical! The accepted qubits form the final key. See, for instance, the cases of "Datum" 2 and 4. If the number of errors surpass a predefined error-rate threshold, Alice warns Bob about Eve and that key is discarded.

To summarize, we must keep in mind the specific property that is at the core of the BB84 protocol, namely the impossibility of finding (by using a measurement basis), the polarization of a single photon if the basis that was used to polarize it (polarization basis), to begin with, is not know, which, combined with the no-cloning theorem, render this protocol provably secure.

Datum	1	2	3	4	5	6	7
Alice's Encoding Basis	+	×	+	+	+	×	×
Alice's Send Polarization	→ (H)	↗ (R)	↑ (V)	→ (H)	↑ (V)	↖ (L)	↗ (R)
Eve's Detection & Resend Basis	+	+	+	×	×	×	×
Eve's Detected Polarization	→ (H)	↑ (V)	↑ (V)	↗ (R)	↖ (L)	↖ (L)	↗ (R)
Bob's Detection Basis	+	×	+	+	+	+	×
RECONCILIATION/SIFTING							
Match?→ Keep	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	**No**	*Yes*
SIFTED KEY	0 (→)	1 (↑)	1 (↑)	1 (↗)	0 (↖)	-	1 (↗)
ERROR CORRECTION							
Bob's Detected Polarization	→ (H)	↖ (L)	↑ (V)	↑ (V)	↑ (V)	-	↗ (R)
Match?→ Keep	*Yes*	**No**	*Yes*	**No**	*Yes*	-	*Yes*
FINAL KEY	0 (→)	-	1 (↑)	-	1 (↑)	-	1 (↗)

Figure 5: An example of realistic QKD (note: for error correction the whole sifted key is used - instead of some subset of it)

3.2 E91

3.2.1 Prerequisites

The EPR paradox, although, initially designed to demonstrate quantum mechanics' incompleteness as a physical theory, subsequently came to show how it defies classical intuition. Einstein, Podolsky & Rosen mainly relied on two classical principles: locality and realism, stating that distant objects cannot have direct influence on one another and that there exists a reality that is independent of an observer or measurer. Quantum cryptography violates both by adhering to the following principles:

1. The polarization of a photon cannot be measured in non-compatible bases at the same time (e.g. bases '+' and '×').

2. Individual quantum processes cannot be distinctly described.

3. Measuring a quantum system always disturbs it.

4. It is impossible to duplicate unknown quantum states.

The third principle plays an essential role in ensuring that the most valued property of quantum cryptography, its security, is preserved. It implies, as has already been examined, that Eve cannot eavesdrop on a message sent between Bob and Alice, without altering it, and therefore being exposed. And she cannot conceal herself due to the fourth principle. The E91 protocol further exploits quantum entanglement in which although no definite conclusions can be made about the state of each of the particle before measurement, the state of both particles is well defined, post-measurement. Quantum entanglement refers to the inability to define the quantum state of one object without reference to the quantum state of another object, entangled to the first. Up until now we have seen the BB84 protocol of which the E91 protocol is a modification. The former used four quantum states, with each pair making up a different base. Alice sent particles to Bob in one of the four states, and Bob randomly selected bases in which to measure the particles. As shall be discussed, E91 uses six and also EPR states are taken into consideration.

3.2.2 Description

Instead of relying upon a source owned by Alice, which could be tapped by Eve, a source emits pairs of spin-1/2 particles ($|\uparrow\rangle$ or $|\downarrow\rangle$) in singlet states

$$\phi = \frac{(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle)}{\sqrt{2}}$$

that Alice and Bob share. In state $|\uparrow\downarrow\rangle$, particle A has an $\uparrow$ spin and B a $\downarrow$ spin, whereas in state $|\downarrow\uparrow\rangle$ particle A has a $\downarrow$ spin and B an $\uparrow$ spin. The well-defined combined state of both particles and the unknown spin of either particle is called the superposition of states. In other words, it is known that one particle is spinning up and the other is spinning down, but it is impossible to tell which particle is which. Both Alice and Bob randomly pick one of the three axes-bases in which to measure the incoming particles, that can be mathematically represented as vectors a_i and b_j, respectively $(i, j = 1, 2, 3)$. Assuming the particles are traveling along the z axis, the vectors a_i and b_j are located in the $x - y$ plane, perpendicular to the trajectory of the particles. By using the vertical x axis from which to measure the angles, the vectors a_i and b_j can be described by $\phi_1^a = 0°$, $\phi_2^a = 45°$ and $\phi_3^a = 90°$ and $\phi_1^b = 45°$, $\phi_2^b = 90°$ and $\phi_3^b = 135°$: the orientation of Alice and Bob's analyzers, respectively. Each measurement can yield two results, $+1$ (spin $\uparrow$) and -1 (spin $\downarrow$), potentially revealing one bit of information. Thus,

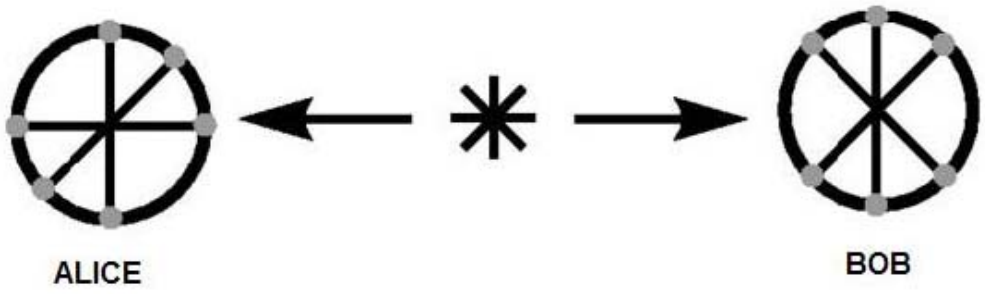

Figure 6: Possible basis-axis orientations for Alice and Bob

there is a 1/3 probability that Alice and Bobs bases will be compatible. For example, if Alice and Bob chose a compatible basis, and Alice measured a

spin ↑ particle, the quantum state of the system would collapse into state $|\uparrow\downarrow\rangle$, and the probability of Bob measuring a spin ↓ particle would be 100%. In that respect, if Alice observes a spin ↓ particle, Bob will detect a spin ↑ particle with a 100% probability. However, if Alice and Bob measured the spins in incompatible bases, we cannot be that certain about the outcome. If Alice measures the particles in one basis, Bob's measurement outcome in a non-compatible basis will be random. For example, if Alice detects a spin ↑ particle in the a_2 basis and Bob measures in the incompatible b_2 basis, there exists an equal 50% probability of detecting either a spin ↑ or a spin ↓ particle. Due to entanglement, it is implied that Bob's particle somehow "knows" how Alice's particle was measured and orients itself accordingly. There seems to exist some form of action or connection at a distance, informing Bob's particle about the basis Alice used, so that his particle can "decide" whether or not it should complement Alice's measurement in the same basis, or pick a random orientation, if incompatible bases are chosen. So, if Alice and Bob choose compatible bases, their measurement results will be anti-correlated (Bob's particle will have spin ↑, and Alice's will have spin ↓). And if they choose incompatible bases, the *sifting* takes place, where they must publicly announce which bases the particles were measured in order to discard the corresponding bits (of differing bases) without needing to reveal them (that is: the outcomes of their measurements). The remaining "sifted key" shrinks down to 30% of its original size (on average). Within the "sifted key", the spin ↑ and spin ↓ states of the particles usually correspond to bit values 0 and 1. But, how are we secure against Eve gaining any information about the key? Until a measurement is made, the states of the particles are not yet collapsed. So, trying to gain information about the system without making a measurement is impossible because no information yet "exists". For example, let's say both Alice and Bob choose to measure a particle in the 45° basis (a_2 and b_1, respectively), and Alice detects a spin ↑ particle, then Bob must definitely detect a spin ↓ particle. If Bob does not, it might mean that Eve has tapped on the connection. If Eve is indeed trying to intercept, she must choose a basis in which to measure her particle. If she detects the particle in her basis, it means that she has measured it, therefore destroying it. If Eve's basis is different from Alice and Bob's, she will get a random measurement result. She will then have to recreate her detected particle (usually in the basis of her measurement) and send it to Bob. After such an intervention, the orientation upon measurement (Bob's received particle) will be random. If he measures an orientation that does not correlate to Alice's result (as Eve

did), he will get an error. Contrary to BB84's four states, the reason E91 utilizes six is so that an eavesdropper can be detected without having to leak out information about his key, as happens in the former protocol.
The quantity

$$E(a_i, b_j) = P_{++}(a_i, b_j) + P_{--}(a_i, b_j) - P_{+-}(a_i, b_j) - P_{-+}(a_i, b_j)$$

is the correlation coefficient of Alice and Bob's a_i and b_j measurements. Where $P_{\pm\pm}(a_i, b_j)$ denotes the probability of obtaining ± 1 along a_i and ± 1 along b_j (with ± 1 meaning spin $\uparrow$ or spin $\downarrow$). As mentioned earlier, and as predicted by quantum entanglement, the two pairs of analyzers of the same orientation (a_2, b_1 and a_3, b_2) give a value of $E(a_2, b_1) = E(a_3, b_2) = -1$, which hints anti-correlation of the results obtained by Alice and Bob. Now, one can define a quantity S, which is the sum of all correlation coefficients for which Alice and Bob used analyzers of different orientations (incompatible bases):

$$S = E(a_1, b_1) - E(a_1, b_3) + E(a_3, b_1) + E(a_3, b_3)$$

Bell, using local realism, proved that $S \leq 2$. However, quantum mechanics gives that $S = 2\sqrt{2}$. This simply means that if the states are truly entangled, the rules of local realism are defied and Bell's theorem is violated. Therefore, by publicly announcing the values Alice and Bob measured in an incompatible basis, they can figure out a value for S. Therefore, after the transmission has taken place, Alice and Bob can publicly announce the orientations of the analyzers they have chosen for each particular measurement. Specifically, they divide the measurements into two groups:

1. A group for which they used different orientation of analyzers
2. A group for which they used the same orientation of their analyzers.

Subsequently, Alice and Bob publicly reveal the results obtained within the first group of measurements only, which allows them to establish the value of S. If the particles were not disturbed by Eve, or anything else, their expected value is $2\sqrt{2}$ and they can rest assured that the values they measured in a compatible basis are anti-correlated and that their *sifted key* is secure. It should generally not be forgotten that even if the possibility of an eavesdropper is eliminated, the sifted key may contain other, system-related errors. So, anything different to anti-correlation indicates an error occurrence in the system.

A portion of detected errors is referred to as the Quantum Bit Error Rate (QBER). The QBER is calculated by dividing the number of errors by sample size and multiplying by 100% and it is an indication of the efficiency of the system. In general, an error rate that exceeds approximately 15% serves as a good indication that some malicious Eve is present. Assuming that the possibility of Eve was eliminated, Alice and Bob proceed onto refining their keys through error correction and privacy amplification (which are both classical algorithms, used for further securing the final key). Finally, after error-correction has been applied to the sifted key, Alice and Bob may use the resulting key to safely communicate.