# CHAPTER 10

# Quantum Cryptography

Secure transmission of messages and data is of utmost importance in both commercial and defense applications. This involves transmission of digital bit streams or digitized analog signals through various means from one location to another over a secure channel. A major weakness of such systems is the physical channel used by a system for interconnecting users and the system. An unauthorized user must not have access to the data transmitted via the channel.

Cryptography is used to make a message unintelligible to any person who is not authorized to receive it; this is achieved by combining the message with some additional information known as the *key*. The process of disguising a message to hide its content is called *encryption*. Many secure transmission methods require a type of *encryption*. A message before it is encrypted is known as a *plain text;* an encrypted message is also known as a *ciphertext*. The reverse process of converting a ciphertext back to a plaintext is known as *decryption* The two main components required to encrypt information are an algorithm and a key. The algorithm is generally known but the key is kept secret; the message cannot be extracted from the encrypted data without using the key.

For example, a message can be encrypted by using the following rule:

*Replace every A in a message with a D, every B with an E, and so on through the alphabet.*

Thus, using this rule the

Plain text: RETREAT

can be converted into

Ciphertext: UHWUHDW

Only someone who has the *shift-back-by-3* key can decipher this message; this is done by deriving the *mod* 26 of the new position of a shifted letter. Thus,

Ciphertext: DWWDFN

can be decrypted to

Plaintext: ATTACK

The primary goal of cryptography has been to provide the following four services for enhancing information security:

*Confidentiality*: Protection from disclosure to an unauthorized person, that is, keep the information from any person whose identity has not been verified.

*Integrity*: Identifying any alteration to the data. A receiver should be able to verify that a message has not been modified during its transition from the sender to the receiver; in other words, an intruder cannot substitute the original message with a false one without being detected. Thus, data integrity allows a means for the detection of any unauthorized manipulation of data although it cannot prevent it.

*Authentication*: The process of confident identification of the originator of a message by a recipient. In other words, it confirms that the message received by one party has been sent by another party whose identity has already been verified.

*Non-repudiation*: An originator of a message cannot falsely deny later that he or she sent the message.

In summary, a secure system must satisfy the following requirements:

1. Allow legitimate users have access when they need it.
2. Keep out unauthorized users.

## 10.1 Principles of Information Security

Information security can be achieved by using *symmetric key cryptography* or by *public key cryptography*. Claude Shannon of Bell Laboratories published the fundamental theory behind symmetric key cryptography in 1949. In this type of cryptography a single key is used to encrypt and decrypt the message. The main advantage of sharing a key is that a large amount of information can be communicated in secret by sharing a small number of key bits.

A major requirement in symmetric system is that a secure key establishment mechanism is in place. If a key is compromised, impersonators can decrypt messages and the security of the system can no longer be assured. A separate pair of keys can be employed for each pair of users to enhance security; this however increases the number of keys rapidly. For example, in a group of $n$ people, the number of keys required will be $[n(n-1)]/2$. Secure key distribution remains the biggest challenge in using symmetric key cryptography.

Another class of security systems known as public key cryptographic system is very convenient to use and rely on a publicly known algorithms. The security of the Internet, for example, is partially based on such systems. A public key system uses separate keys for encryption and decryption. These keys are mathematically related; one key is used for encryption, the other one can decrypt the encrypted message and retrieve the original message back. For example, if one party A wants to communicate with another party B, then party A chooses a *private key* first. This key is not disclosed to anyone. A and B then exchange their public keys. To send a message to B, A first encrypts the message with the public key and then transmits it to B. B uses his/her private key to extract the corresponding plain text from the encrypted message.

The public-key system in a group of $n$ people requires $2n$ keys, that is, $n$ public and $n$ private keys. The most important advantage of public-key systems over their private counterpart is that the need for a sender and a receiver to share secret keys via some secure channel is eliminated; all communications involve only public keys, a private key is never transmitted or shared.

In a private key cryptography the secrecy of the key is dependent only on the secrecy of the key. The key must be composed of sufficiently long string of randomly chosen bits private key cryptography suffers from a major weakness—as indicated earlier it requires sharing of a secret key between two parties. An intruder can copy the secret key as it is being exchanged, thereby severely compromising the security of the system. Thus, a private key cryptographic system depends entirely on secrecy of the key.

Public key cryptography does not have a key distribution problem. Its security relies on the fact that determining the factors of a number that is the product of two very large prime numbers is not computationally feasible. It has been shown that a quantum computer can derive the prime factors of very large numbers in polynomial time (see Shor's algorithm in Chap. 9). Public key cryptography will therefore become insecure if quantum computing becomes a reality. Quantum cryptography avoids all these issues by encrypting the shared key using a series of photons.

## 10.2 One-Time Pad

Vernam [1] proposed a scheme known as *one-time pad,* that encrypts data using a random key. The term "one-time pad" indicates that the key is used one time, and never used again. In topics of cryptographic communication the sender is identified as Alice, the receiver as Bob, and the intruder as Eve. The key must have the same number of bits as the data to be transmitted and must also consist of completely random bits that are kept secret from everyone except the sender and the receiver. The keys are used only once as indicated above; both the sender and the receiver must destroy their keys after use. The principle of operation of one-time pad is as follows:

Encryption by Alice:

$$c_i = d_i + k_i \quad i = 1, 2, 3 \ldots \ldots$$

where $d_i$ are data bits; $k_i$ are key bits; $c_i$ are encrypted data bits.

Decryption by Bob:

$$d_i = c_i + k_i \quad i = 1, 2, 3 \ldots$$

Thus Alice encrypts the data she sends to Bob by EX-ORing it with randomly generated key bits. Bob retrieves the encrypted data by EX-ORing the received data with the same key bits. Figure 10.1 illustrates the scheme assuming key bits are 100010000101100.

A major drawback of one-time pads is that the sender and the receiver must somehow exchange the secret key bits that they use. For instance, in the example above (Fig. 10.1) Alice and Bob share the key bits $k_1$ before the transmission of the encrypted information bits. A third party might intercept the communication between the sender and the receiver and access the key, thereby comprising the security of the data transmission. Thus the secure distribution of keys is the prerequisite for secure communication; this is known as the *key distribution problem.*

| Alice | | Bob | |
|---|---|---|---|
| $d_i$ | 000010010110000 | 100000010011100 | $c_i$ |
| | + | + | |
| $k_i$ | 100010000101100 | 100010000101100 | $k_i$ |
| $c_i$ | 100000010011100 | 000010010110000 | $d_i$ |

**Figure 10.1** An example of one-time pad.

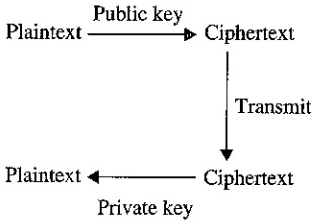


**FIGURE 10. 2** Public key cryptographic system.

## 10.3 Public Key Cryptography

As discussed earlier in this chapter, the communicating parties in public key cryptographic system uses two separate keys—a public key and a private key. The public key as the name suggests may be made accessible to anybody. The private key on the other hand is kept secret. Figure 10.2 shows the encryption and decryption process in a public key cryptographic system.

Public key cryptography uses a method of encoding and decoding that employs a special case of the one-way function known as a *trapdoor or one-way function* [2]. A function $f(x)$ is considered to be a one-way function if it is easy to compute the function $f(x) = y$ for any input $x$, but the opposite, that is, computing $x$ from $f(x)$, is significantly more complicated unless some piece of information (the trapdoor) is known. For example, it is relatively easy to multiply two prime numbers to generate a composite number, but is extremely difficult to factor a composite number (especially a very large integer) into a product of two prime numbers unless one of the numbers is known. It is intuitively clear that calculating $67 \times 83$ is much faster than finding the prime factors of 5761. However, the problem can be easily solved, if some additional information is given, for instance, knowing that 67 is one of the prime factors of 5761.

An important point to remember is that unlike in symmetric encryption, the two keys in public cryptography behave differently; the public key is the *only* key that can encrypt the data to be sent out. A public key is freely available to anyone who wants to use it. They can be distributed as email attachments or through a public key chain server that stores a large number of public keys. Although any one can have access to the public key, the encrypted data can only be decrypted by a party who knows the corresponding private key. The distribution of the private key is avoided, thus preventing any unauthorized party from accessing the key. Moreover even if the public key falls into hands of unauthorized persons, it is practically impossible to derive the decryption key from the encryption key because this is computationally infeasible.

The process of using public key cryptography is relatively straightforward. To send a message, the sender (Alice) obtains a copy of Bob's (recipient) public key, either by email or from a key chain

server that stores a large number of public keys. The resulting encrypted message is then sent to Bob who uses their shared private key to restore the original message.

The advantage of public key cryptography is that it does not require any initial secure exchange of secret keys for encrypting a message. However, it requires far longer keys to offer the same level of protection as symmetric encryption. A newer type of public key cryptography, known as *elliptic curve cryptography*, can be just as secure as symmetric encryption using similar key lengths [3].

## 10.4 RSA Coding Scheme

The widely used RSA (Rivest, Shamir, and Adelman) technique is a public key cryptographic system [4]. It facilitates the generation of public and private keys by choosing two large prime numbers $p$ and $q$, and making $N = p.q$. Next a random positive integer $e$ is chosen such that it is relatively prime to $(p - 1)\ (q - 1)$; $e$ is called the encryption constant. Then the decryption constant $d$ is derived such that $e.d = 1\ mod\ (p - 1)(q - 1)$. The public key is $(N, e)$, and the private key is $d$.

It should be mentioned that although $N$ is revealed to all, the factors $p$ and $q$ of $N$ are kept secret. Obviously if an intruding party can factor $N$ to find $p$ and $q$, then it can use $e$ of the public key to derive the private key $d$ from the expression $e.d = 1\ mod\ (p - 1)(q - 1)$. The steps of the RSA algorithm are as follows:

i. Generate two large prime numbers, $p$ and $q$, and let $n = p.q$.

ii. Let $\varphi = (p - 1)(q - 1)$.

iii. Choose another number $e$ which is relatively prime to $\varphi$; two numbers $a$ and $b$ that have no common factors other than 1 are said to be *co-prime* or *relatively prime.*

iv. Select e, $1 < e < \varphi$ such that $gcd(e, \varphi) = 1$; *gcd* (the greatest common divisor) of two integers $a$ and $b$ is the largest integer that divides both numbers.

v. Find $d$, such that $de \equiv 1 \bmod \varphi$. The notation "$a \equiv b\ (\text{mod}\ n)$" means $a$ is *congruent* to $b$, that is, $a$ and $b$ have the same remainder when divided by $n$.

vi. Encryption: compute $c = m^e \bmod n$, where $m$ is message block represented as a number $0 < m < n - 1$ and $c$ is the encrypted message.

vii. Decryption: compute: $m = c^d \bmod n$.

The security of RSA system is based on the fact that currently no algorithm is available for factoring a large number into a product of two

prime numbers in a reasonable amount of known for some time that Shor's quantum algorithm (discussed in Chap. 9) is capable of factoring very large numbers efficiently. Thus, the security of public key cryptographic system can be guaranteed only till quantum computers become technologically feasible.

Public key cryptography in general requires far longer keys to offer the same level of protection as symmetric encryption. Elliptic curve cryptography, on the other hand, can be just as secure as symmetric encryption using similar key lengths.

## 10.5 Quantum Cryptography

According to the quantum theory, light is an electromagnetic wave and is made up from a lot of particles known as photons, each photon has a specific energy $hf$ and a wavelength $c/f$. Recall that light has a pair of electric and magnetic fields that are perpendicular to each other as shown in Fig. 10.3. If the electric field component of a beam of light vibrates along a single direction (like the vertical direction Fig. 10.3) then the beam of light is said to be *polarized* in that direction [5].

Polarized photons can be created by passing a normal beam of light through a filter set for a specific angle of polarization. A photon incident on the filter will either pass through it or will be blocked; if the photon emerges it will be aligned to the angle of the filter regardless of its initial polarization angle of the filter regardless of its initial polarization.

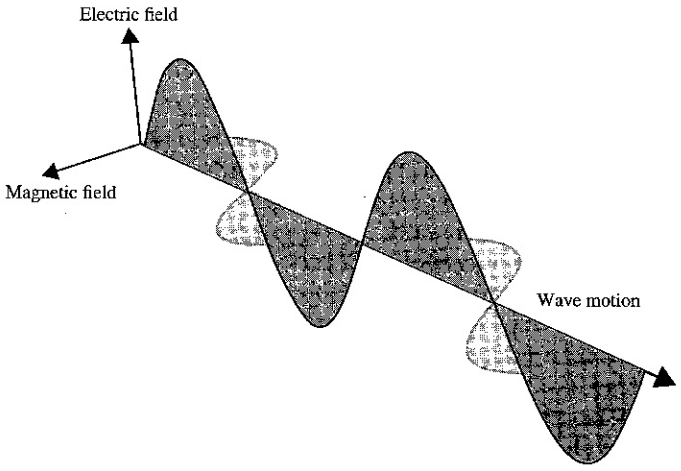


**Figure 10.3** Propagation of electromagnetic waves (Ref.5).


**Figure 10.4** Polarized modes of a photon.

Photons can be polarized in one of two bases: *rectilinear* (⊕) or *diagonal* (⊗), using an appropriate filter as shown in Fig. 10.4. A filter allows the transmission of a photon through it only if the polarization of the photon is aligned with the filter. In the rectilinear mode only photons with horizontal or vertical polarization pass through the polarizing filter. In the diagonal mode, on the other hand, only photons with polarization that are at an angle of +45° or –45°, to the horizontal axis can pass through the polarizing filter. Thus in the rectilinear mode, orientations | and — represent 0° and 90°, respectively, and in the diagonal mode orientations \ and / represent +45° and –45°, respectively.

Heisenberg's uncertainty principle shows that certain pairs of properties, known as *noncommutating* properties, are related in a way that it is impossible to measure these simultaneously; such pairs are called *conjugate pairs*. Rectilinear and diagonal polarizations constitute such a conjugate pair of noncommuting properties. Thus, a filter with 0° /90° orientation can correctly detect a rectilinearly polarized photon; a filter similarly with +45°/–45° orientation can detect a diagonally polarized photon. On the other hand, if a diagonally polarized filter is used to detect a rectilinearly polarized photon or vice versa, the outcome will be random with equal probabilities and the photon will lose all the information of its previous state.

## 10.6 Quantum Key Distribution

Key distribution as discussed earlier enables the sharing of cryptographic keys such as a private key between two or more parties so that they can securely share information such as a private key; the key can then be used to encrypt messages that are being communicated over an insecure channel. As indicated previously, the distribution of keys is a major weakness of private key cryptography.

Quantum cryptography overcomes this drawback by providing a secure way of sharing a random key between two separate parties. An additional advantage of quantum keys is that the sender and receiver can easily verify whether the key has been tampered with. It should be emphasized here that QKD is not a technique for encryption and decryption of data; it allows only secure distribution of private keys.

As the name implies, quantum cryptography is a particular form of cryptography that relies on the laws of quantum mechanics in

order to ensure unconditional security. It has its origin in a novel idea of Stephen Wiesner, a graduate student at Columbia University in 1969 [6]:

i. The polarization of photons cannot be simultaneously measured in incompatible bases (rectilinear/diagonal).

ii. Information of an individual property of a quantum particle, for example, the polarization of a single photon cannot be obtained.

iii. It is not possible for an intruder to access a message between Alice and Bob without changing its meaning.

iv. It is not possible to copy an unknown quantum state.

Once a key has been successfully transmitted, it can be used to encrypt a message in a classical symmetric cipher, for example, the one-time pad and can be transmitted by conventional means such as telephone or email. Thus, symmetric keys in conjunction with quantum key distribution can guarantee secure generation and transmission of private keys. More importantly, quantum key distribution is secure against new attacking strategies and against determined eavesdropping.

## 10.7 BB84

Bennet and Basard, inspired by Wiesner's scheme, proposed a quantum key distribution (QKD) protocol [7]. This protocol, known as BB84, allows a sender (Alice) to send photons to a receiver (Bob). Alice and Bob communicate via a one-way quantum channel and a two-way public channel. Alice has a source of single photons and two polarizing filters—one rectilinear and one diagonal. Figure 10.5 illustrates a quantum key distribution system:

The quantum channel, however, is vulnerable to any possible manipulation from an eavesdropper. Alice and Bob must ensure that

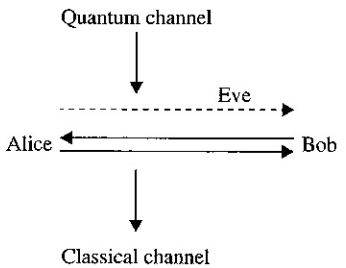


**Figure 10.5** A quantum key distribution system.

the eavesdropper, usually called Eve, cannot tap on the quantum channel and listen to the exchanges over the classical channel.

A photon has three types of spins: *horizontal, vertical,* and *diagonal.* An unpolarized photon has all three spin states at the same time. By passing it through a polarization filter, a photon can be polarized to let through only a particular spin. All the unwanted types are eliminated. Furthermore, single photons cannot be copied; this is because the linearity of quantum mechanics does not allow cloning of unknown quantum states as explained (see Chap. 7).

The BB84 protocol can be implemented using polarized single photons. Alice can transmit single photons randomly in either a rectilinear (⊕) or diagonal (⊗) basis. In each basis, one orientation of the photon is used to represent the logic value 0 and the other one to represent 1; this is agreed upon by Alice and Bob before the key formation begins.

Note that in practical quantum cryptography, a qubit is represented by the polarization state of a photon. The polarization state of a randomly polarized photon is a superposition of any pair of orthogonal states such as:

- Horizontal (H) and vertical (V) polarization
- +45° and –45° diagonal polarization

The polarization of a photon can thus be modeled by a qubit; the state of the qubit is represented as

$$|\psi> = a|\mathrm{H}> + b|\mathrm{V}> = c|+45°> + d|-45°>$$

where $a$, $b$, $c$, and $d$ are complex numbers and $|a|^2 + |b|^2 = |c|^2 + |d|^2$.

For a chosen orthogonal state pair, one polarized state is assumed to be $|0>$ and the other one as $|1>$. For example, for a rectilinear state pair:

$$|\mathrm{V}> = 1 \quad \text{and} \quad |\mathrm{H}> = 0$$

for a diagonal state pair

$$|+45°> = 1 \quad \text{and} \quad |-45°> = 0$$

Thus, a photon can be assumed to be a qubit with one bit of quantum information.

Figure 10.6 shows the basis, angle, polarization, and logic value of single photons. For example in the rectilinear mode, orientations | and — represent 1 and 0, respectively. In the diagonal (⊗) mode, orientations \ and / represent 1 and 0, respectively.

| Basis | Angle | Polarization | Logic value |
|---|---|---|---|
| ⊕ | 0° | — | 0 |
| ⊕ | 90° | \| | 1 |
| ⊗ | 45° | / | 0 |
| ⊗ | −45° | \ | 1 |

**Figure 10.6** Characteristics of single photons.

To perform BB84, Alice and Bob have to first agree on how bits will be encoded in the polarization directions for each filter. This means they should form a bit table like the one shown above in Fig. 10.6.

The following steps describe the BB84 protocol:

i. Alice generates a random sequence of 0s and 1s. She then replaces each bit in the binary sequence with a randomly chosen polarization shown in Fig. 10.6. Theoretically any quantum particle can be used to replace the bits. The photon is preferred, however, because they can be transmitted over longer distances without decoherence.

ii. Alice sends the photons corresponding to each bit replacement in the binary sequence to Bob via the quantum channel, while keeping record of the polarization basis and the logic value of the transmitted photons.

iii. As Bob is not aware of which basis Alice has chosen for a photon, he randomly chooses one of the two bases. If he chooses the same basis as Alice, the polarization is recorded correctly. Alternatively, if he chooses a different basis, the initial polarization of the received photon is lost and the result is a random polarization. It is also possible that sometimes Bob does not register anything because of errors in the detection or in the transmission.

iv. Once Bob receives all the photons sent by Alice, he confirms that he has received and measured all of them. The bit string corresponding to the photons received by Bob is called a *raw key*.

v. Next, Bob announces via the public channel his choice of basis for each photon. This does not lead to any security compromise since Bob reveals only which bases he used, not which result he obtained. Thus, an eavesdropper cannot get any information related to the key formation.

vi. Alice and Bob then compare the bases they selected and discard all non-matching bases. In other words, Alice and Bob keep only the bits corresponding to the same bases. Since both Alice and Bob have randomly chosen the bases, there is an equal probability of getting matched and unmatched results. As a consequence, almost 50% of the qubits are available for forming the secret key. Note that the key is truly random because neither Alice nor Bob can decide which key will result at the end of the procedure.

To illustrate, assume that Alice decides to send the following bits to Bob:

| Bits | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|

and chooses the following bases to convert the bits:

| Basis | + | × | + | × | × | × | + | + |
|---|---|---|---|---|---|---|---|---|

The polarization of the resulting single photons are:

| Polarization | \| | / | — | \ | \ | / | \| | — |
|---|---|---|---|---|---|---|---|---|

Bob detects the state of each photon he receives by randomly picking one of the bases of photons. If he makes the correct guess in picking the base Alice used for sending a particular photon, he obviously detects the correct orientation of the photon and the correct logic value the photon represents. For example, if Alice sends a 1 using the rectilinear mode (as in the first bit in the above bit sequence) and Bob chooses the same polarization mode, he is guaranteed to receive a 1. On the other hand, if Bob picks the diagonal base, the probability of his receiving a 1 is reduced to 50% and there is a 50% probability of his receiving a 0 instead. The modes Bob selected and the polarizations of the resulting photons are:

| Mode | + | + | × | × | + | × | + | × |
|---|---|---|---|---|---|---|---|---|
| Polarization | \| | — | / | \ | \| | / | \| | / |

After all the bits have been sent, Alice informs Bob of the bases she used to send each photon but not its orientation via the public channel. Bob also communicates to Alice via the public channel the bases he used. If Bob used a base that is different from Alice's photon, he ignores the corresponding bit. Alice and Bob keep only those bits for which their bases match perfectly; the remaining bits are discarded. Statistically, only 50% of the transmitted bits agree. These bits

are used as the key. This shorter key is called a *sifted key.* The following example illustrates the BB84 key generation protocol:

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Alice random Bits | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 |
| Alice base | ⊗ | ⊗ | ⊕ | ⊗ | ⊕ | ⊗ | ⊕ | ⊗ | ⊕ | ⊕ | ⊕ | ⊗ |
| Alice polarization | \ | \ | \| | \ | — | \ | — | \ | — | \| | \| | / |
| Bob base | ⊗ | ⊕ | ⊗ | ⊗ | ⊗ | ⊕ | ⊕ | ⊗ | ⊗ | ⊗ | ⊕ | ⊕ |
| Bob's polarization | \ | \| | \ | \ | / | \| | — | \ | / | \ | \| | — |
| | ↑ | | | ↑ | | | ↑ | ↑ | | | ↑ | |
| Secret key | 1 | | | 1 | | | 0 | 1 | | | 1 | |

Note that in this case, the sifted key has less than 50% of the original key bits. Thus, BB84 is inherently inefficient in its use because many key bits, as high as 50%, are discarded during the key formation process as shown in the above example.

A simplified version of the BB84 protocol was proposed in Ref. [8]. This version uses two states, rectilinear and diagonal, for representing 0 and 1 respectively instead of four states in BB84. Pasquinucci et al. [9] proposed a protocol that uses three orthogonal bases and six states to encode the key bits. Thus an intruder has to correctly choose the base used by the sender and receiver out of three possible bases. This increases the probability of the intruder making more errors in selecting the correct base, thus allowing easier intrusion detection.

Scarani et al. [10] proposed another variation of the BB84 protocol known as SARG04 in 2004. The first phase of the protocol is the same as the first phase of BB84. In the second phase when Alice and Bob determine for which bits their bases matched, Alice announces a pair of non-orthogonal bases. Instead of the exact bases that she used to encode her bit, one of the bases in this pair is the base she used to encode the key data bit. At the receiving end, Bob will correctly measure the polarization state if he chooses the same basis as Alice. Otherwise, the data will have an unpredictable value. If there are no errors, then the length of the key remaining after the sifting stage is ¼ of the raw key.

The SARG04 protocol provides almost the same security as BB84. However, SARG04 provides better protection against the PNS (photon number splitting) vulnerability of the BB84 protocol. It arises because Eve can take away a photon and can obtain all the information from it after the public key sifting stage [11].

## 10.8 Ekart 91

It is a three-state protocol that uses the Einstein-Podolsky-Rosen (EPR) paradox discussed in section 6.4. This protocol can be described in terms of the three polarization states of an EPR photon pair [12]. For example, three possible states are:

$$|\varphi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1 |90\rangle_2 - |90\rangle_1 |0\rangle_2)$$

$$|\varphi_1\rangle = \frac{1}{\sqrt{2}}(|30\rangle_1 |120\rangle_2 - |120\rangle_1 |30\rangle_2)$$

$$|\varphi_2\rangle = \frac{1}{\sqrt{2}}(|60\rangle_1 |150\rangle_2 - |150\rangle_1 |60\rangle_2)$$

The symbols for bits 0 and 1 in these states are

$$|\varphi_0\rangle \; |0\rangle = \text{Bit } 0$$

$$|90\rangle = \text{Bit } 1$$

$$|\varphi_1\rangle \; |30\rangle = \text{Bit } 0$$

$$|120\rangle = \text{Bit } 1$$

$$|\varphi_2\rangle \; |60\rangle = \text{Bit } 0$$

$$|150\rangle = \text{Bit } 1$$

As in BB84, there are two stages of communication between Alice and Bob; one over a quantum channel and the other over a public channel.

An EPR pair of photons is first created in randomly selected states from the set $\{|\varphi_0\rangle, |\varphi_1\rangle, |\varphi_3\rangle\}$. One photon of the EPR pair is sent to Alice and the other to Bob using the quantum channel. For each photon they receive, Alice and Bob select randomly and independently an operator from the set of three that were chosen for measuring the photons. They measure their respective photons with the selected operator. Alice records her measured bit while Bob records the complement of his measured bit. This process is repeated for all the needed photons.

In the first part of the second stage, they release via the public channel which basis they used for each bit slot measurement. They separate the measurement results into two groups:

1. The first group consists of bit slots for which the same measurement operators are used.

2. The second group consists of bit slots for which different operators are used.

Any photons which are not measured in the first or the second group are discarded. The first group is used to establish a *raw key*, while the second group that includes all the remaining bit slots is called a *rejected key*.

The EPR protocol, unlike BB84, does not discard the rejected key bits. Instead, they are used to test the presence of an intruder. During the second phase of the second stage, Alice and Bob publicly announce the results obtained for those cases in which they used *different* operators. Assuming Alice and Bob picked the measurement operators randomly and independently, the correlation between their results is found to be the same as *CHSH* (Clauser, Horn, Shimony, and Holt) inequality and is equal to $-2\sqrt{2}$ [13]. A major variation of this value would indicate the presence of an eavesdropper. On the other hand, if the CHSH inequality is not violated, Alice and Bob can trust that the perfectly anti-correlated results that they obtained can then be converted into a secret key.

For each measurement where Alice and Bob used the *same* basis, they should expect opposite results due to the principle of quantum entanglement. This means that if Alice and Bob both interpret their measurements as bits (as before), they each have a bit string which is the binary complement of the other. Either party could invert their key and share a secret key. They can then use this set of common private keys to encrypt and decrypt their messages and communicate secretly. However, each key can only be used once and cannot be repeated in order to keep the keys completely random.

The eavesdropper Eve cannot get any information from the photons while they are in transit because the information is *formed* in a photon only after it is measured and the result is communicated to legitimate users.

If Eve tries to detect photons coming from the source, she has to randomly choose her own measurement base since she does not know what base Bob will use. Therefore, about half the time she will choose a different basis than Bob. Suppose Alice sends one type of polarized photons, some of which are received by Eve and Bob. If Eve decides to use a different basis for measurement and Bob decides to use the same basis as Alice, Alice and Bob keep the resulting data since they both used the same basis. But since Eve used the wrong basis, she does not know what their result was.

Suppose instead that Eve decided to measure the polarized photons according to same basis Alice used, but Bob decides to measure these using a different basis. Here Eve would know the polarization that Alice sent, but since Bob did not choose the correct basis, Alice and Bob would throw the results out.