

# Applications of Quantum Mechanics in Secure Communication

Mosayeb Naseri, Negin Fatahi, Ahmed Farouk, O. Tarawneh  
and M. Elhoseny

**Abstract** Over the last half century, the components of computers have become smaller by a factor of two every 18 months, a phenomenon known as Moore's law. In state-of-the-art computers, the smallest wires and transistors are approaching 100 nm feature size, which is approximately 1000x the diameter of an atom. Quantum mechanics is the theory of physics that describes the behavior of matter and energy in extreme conditions, such as short times and tiny distances. As transistors and wires become smaller and smaller, they inevitably begin to behave in intrinsically quantum mechanical ways. In this chapter it will be shown how it can be possible by using simple principles of quantum mechanics to reach a new field of communication science, named quantum communication. Also, the most recent development in quantum secure communication will be introduced and finally, the new method of secure dialogue between two agents (Alice, Bob), with the help of measurement concept in quantum mechanics will be presented.

**Keywords** Quantum effect · Entanglement · No cloning · Quantum cryptography · Quantum teleportation

---

M. Naseri (✉) · N. Fatahi  
Department of Physics, Islamic Azad University,  
Kermanshah Branch, Kermanshah, Iran  
e-mail: Sepehr1976@yahoo.com

A. Farouk · M. Elhoseny  
Faculty of Computer and Information Sciences, Mansoura University,  
Mansoura, Egypt

A. Farouk · O. Tarawneh  
Information Technology Department, Al-Zahra College for Women,  
3365, Muscat, Oman

## 1 Introduction

Quantum mechanics is probably the most successful physical theory of this century. It provides powerful tools which form one of the cornerstones of scientific progress, and which are indispensable for the understanding of omnipresent technical devices such as the transistor, semiconductor chips and the laser. The most important areas where these devices are used are modern communication and information- processing technologies. But quantum mechanics, until now, has only been used to construct these devices and quantum effects are absolutely avoided in the representation and manipulation of information. Rather than using single photons, we still use strong light pulses to send information along optical high-speed connections, and we rely on electrical currents in semiconductor logic chips instead of applying single electrons as signal carriers.

Quantum Communication is the art of transferring a message from one place to another by using the quantum state as a message carrier, traditionally, the sender is named Alice and the receiver Bob. Quantum communication methods utilize fundamental properties of quantum mechanics to enhance the power and potential of today's communication systems. Quantum information processing and communication theory is a broad field, including quantum teleportation, quantum cryptography, quantum dense coding. By way of 2017, the improvement and growth of a real quantum computer is still in early stages but many poetical and theoretical experimentations were implemented by many research groups [1–22].

In this chapter there is a brief introduction, in Sect. 2 we present the necessary quantum mechanical back-grounds for investigation of quantum communication in their simplest forms and some pure quantum mechanical phenomena are discussed. Section 3 describes the fundamentals of quantum communication including the concepts of quantum teleportation and quantum cryptography. In Sect. 4 a brief history of research on quantum secure communication is presented and finally, in the last section we give a brief summary [23–38].

## 2 Quantum Mechanics

Quantum mechanics arose from the need to understand the thermal properties of radiation and the discrete spectral features of atoms. From this, the present understanding of the non-classical behavior of the fundamental units of matter and radiation was developed. Quantum theory has turned out to be the most universally successful theory of physics. From its start in atomic spectroscopy, it has developed to predict structures of molecules, nuclei, and even the large-scale structures of the universe. Much of our electronics industry today utilizes quantum phenomena in an essential manner. Without the understanding offered by quantum theory, our ability to build integrated circuits and communication devices would not have emerged. In these areas the basic theoretical progress took place in the middle of the twentieth century; the

engineers who plan electronics devices need hardly worry about the problems still lingering on our interpretation of quantum theory.

## 2.1 States Space and Measurement

In quantum mechanics a physical state for example, a silver atom with a definite spin orientation is represented by state vector in a complex vector space. We call such a vector a ket and denote it by  $|\alpha\rangle$ , this state ket is postulated to contain complete information about system, everything we ask about the state is contained in the ket. Any ket  $|\alpha\rangle$  can be written as [39],

$$|\alpha\rangle = \sum_{a'} c_{a'} |a'\rangle. \quad (1)$$

With  $a', a'', \dots$  up to  $a^N$  and  $c_{a'}$  is a complex coefficient. In quantum mechanics each observable, such as momentum and spin components are represented by operators that act on kets.

When measurement is performed, the system is “thrown into” one of the eignestates, say  $|a'\rangle$  of observable A [39],

$$|\alpha\rangle \rightarrow |a'\rangle, \quad (2)$$

we do not know in advance into which of the various states the system will be thrown as the result of measurement. we do postulate, however, that the probability for jumping into some particular state is given by;

$$P_{a'} = |\langle a' | \alpha \rangle|^2. \quad (3)$$

So quantum physics establishes a set of negative rules stating things that cannot be done.

- (1) One cannot take a measurement without perturbing the system.
- (2) One cannot draw pictures of individual quantum processes.
- (3) One cannot duplicate an unknown quantum state.

This negative viewpoint of quantum physics, due to its contrast with classical physics, has recently been turned positive, and quantum information is one of the best illustrations of this psychological revolution. We present two novel and typical quantum computation phenomena. It is useful to encounter them early in the study of quantum computation.

## 2.2 Composite Quantum Systems and Entanglement, Hidden Variables and Bell Inequalities

Consider a two-electron system in a state;

$$|\psi^\pm\rangle_{12} = \frac{1}{\sqrt{2}}(|0\rangle_1|1\rangle_2 \pm |1\rangle_1|0\rangle_2) \quad (4)$$

Suppose we make a measurement on the spin component of one of the electrons, clearly, there is a 50–50% chance of getting either spin-up or spin-down, because the composite system may be in  $|0\rangle_1|1\rangle_2$  or  $|1\rangle_1|0\rangle_2$  with equal probabilities. But if one of the components is shown to be in the spin-up state, the other is necessarily in the spin-down state, and vice versa. In other words, when the spin component of electron 1 is shown to be up, the measurement apparatus has selected the first term  $|0\rangle_1|1\rangle_2$  of (4). It is remarkable that this kind of correlation can persist even if the two particles are well separated and have ceased to interact provided that they fly apart!. The above states together with;

$$|\psi^\pm\rangle_{12} = \frac{1}{\sqrt{2}}(|0\rangle_1|0\rangle_2 \pm |1\rangle_1|1\rangle_2) \quad (5)$$

are called Entangled states or EPR states [39–41].

Some have argued that the difficulties encountered here are inherent in the probabilistic interpretation of quantum mechanics and that the dynamic behavior at the microscopic level appears probabilistic only because some yet unknown parameters, so-called hidden variables, have not been specified.

In 1964, John Bell proposed a mechanism to test for the existence of these hidden variables, and he developed his inequality principle as the basis for such a test. He showed that if the inequality was ever not satisfied, then there were no such hidden variables [42].

## 2.3 No Cloning

It can be proved that it is impossible to copy an unknown quantum state perfectly. This feature is a direct consequence of the linearity of the Schrodinger equation. This pure quantum effect is known as “No Cloning” theorem [43].

### 3 Using Quantum Effects in Secure Communication

The goal of quantum communication is to transmit an unknown quantum state from one person to another one at a distant location. This can be obtained either by direct transmission of the state [44], or by disembodied transport, i.e., quantum teleportation [45]. Here we briefly introduce two pillars of quantum communication science, quantum teleportation and quantum cryptography.

#### 3.1 Quantum Teleportation

Quantum teleportation is a process that enables the transmission of an unknown quantum state via a previously shared EPR pair with the help of only two classical bits transmitted on a classical channel. The No-cloning theorem forbids a perfect copy of an arbitrary unknown quantum state.

Suppose Alice and a remote Bob share an EPR pair in the state;

$$|\Phi^+\rangle_{12} = \frac{1}{\sqrt{2}}(|0\rangle_1|0\rangle_2 \pm |1\rangle_1|1\rangle_2) \quad (6)$$

and she has a qubit that she want to send to Bob. Suppose that the state of the qubit is;

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (7)$$

So in the beginning of teleportation, Alice has the following state of the above diagram [43]:

$$\begin{aligned} |\psi\rangle|\Phi^+\rangle &= \alpha|0\rangle + \beta|1\rangle \frac{1}{\sqrt{2}}(|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2) \\ &= \frac{1}{\sqrt{2}}(\alpha|0\rangle_0|0\rangle + \alpha|0\rangle_0|1\rangle + \beta|1\rangle_1|1\rangle) \end{aligned} \quad (8)$$

Suppose that Alice applies a joint measurement on her two qubits, she first applies a CNOT quantum gate which transforms the state to:

$$\frac{1}{\sqrt{2}}(\alpha|0\rangle_0|0\rangle + \alpha|0\rangle_1|1\rangle + \beta|1\rangle_1|0\rangle + \beta|1\rangle_0|1\rangle) \quad (9)$$

where the first qubit is a control qubit and the second one is a target qubit. Next, the Hadamard transform is applied, which transforms the state to;

$$\begin{aligned}
& \frac{1}{2}(\alpha|0\rangle 0\rangle 0\rangle + \alpha|1\rangle 0\rangle 0\rangle + \alpha|0\rangle 1\rangle 1\rangle + \alpha|1\rangle 1\rangle 1\rangle) \\
& + \frac{1}{2}(\beta|0\rangle 1\rangle 0\rangle + \beta|1\rangle 0\rangle 0\rangle + \beta|1\rangle 1\rangle 0\rangle + \beta|1\rangle 1\rangle 1\rangle) \\
& = \frac{1}{2}|0\rangle |0\rangle (\alpha|0\rangle + \beta|1\rangle) + \frac{1}{2}|0\rangle |1\rangle (\alpha|1\rangle + \beta|0\rangle) \\
& + \frac{1}{2}|1\rangle |0\rangle (\alpha|0\rangle - \beta|1\rangle) + \frac{1}{2}|1\rangle |1\rangle (\alpha|1\rangle - \beta|0\rangle)
\end{aligned} \tag{10}$$

A measurement by Alice of her particles produces two classical bits. These bits specify one of four possible results (0, 0), (0, 1), (1, 0), (1, 1). So if Alice sends these two bits to Bob over a classical channel, this allows him to choose one of the following rotations to apply to his particle and transform it into the initial transformed state, so the minimal resources required for faithful teleportation are one EPR pair.

### 3.2 *Quantum Cryptography*

It is clear that traditional cryptosystems are breakable given enough computing time, quantum cryptography offers the promise of unconditional security without face-to-face exchanges. Rather than relying on problems believed to be computationally “difficult,” quantum cryptography uses basic physical laws to provide provable unconditional security.

#### **BB84 Quantum Cryptography Protocol**

The first quantum cryptographic communication protocol, called BB84, was invented in 1984 by Bennett and Brassard [46]. This protocol has been experimentally demonstrated to work for a transmission over 30 km of fiber optic cable [47, 48]. In this section we describe the BB84 protocol. The basic tools are a quantum channel connecting Alice and Bob and a public classical channel, where Eve is allowed to listen passively, but not allowed to change the transmitted message. For the quantum channel, we use four signal states. For simplicity, let us for now regard the signals as realized by single photons in the polarization degree of freedom. Consider two sets of orthogonal signals, one formed by a horizontal and a vertical polarized photon, and the other formed by a 45° and a 135° polarized photon. These four polarized states are non-orthogonal. The overlap probability between signals from two different sets is one half. Bob has two measurement devices at his hand, one in the rectilinear (i.e., vertical/horizontal) basis and one in the diagonal (i.e., 45°/135°) basis. Notice that Bob’s two measurements do not commute. To assure the detection of Eve’s eavesdropping, Bennett and Brassard require Alice and Bob to communicate in two phases; at the first phase Alice and Bob are communicating over a one-way quantum channel as follows: (a) Alice

sends a sequence of signals, each randomly chosen from one of the above four polarizations. (b) For each signal, Bob randomly chooses one of the two measurements, rectilinear or diagonal basis devices to perform a measurement. (c) Bob confirms that he has received and measured all signals. In the first phase, Alice is required, each time she transmits a single bit, to use randomly with equal probability one of the two orthogonal alphabets; it follows from the Heisenberg uncertainty principle that no one, not even Bob or Eve, can receive Alice's transmission with an accuracy greater than 75% [49].

For each bit transmitted by Alice, we assume that Eve performs one of two actions, opaque eavesdropping with probability  $\lambda$ , or no eavesdropping with probability  $1 - \lambda$ . Thus, Eve is eavesdropping on each transmitted bit or Eve is not eavesdropping at all. Because Bob's and Eve's choice of measurement operators are stochastically independent of each other and of Alice's choice of alphabet, Eve's eavesdropping has an immediate and detectable impact on Bob's received bits. Eve's eavesdropping causes Bob's error rate to jump from 25% to;

$$\frac{1}{4} \cdot (1 - \lambda) + \frac{1}{2} \cdot \frac{1}{4} \cdot \lambda = \frac{1}{4} + \frac{\lambda}{8} \quad (11)$$

Thus, if Eve eavesdrops on every bit, i.e., if  $\lambda = 1$ , then Bob's error rate jumps from 25 to 37.5%, a 50% increase.

Phase 2 is dedicated to eliminating the bit locations (and hence the bits at these locations) at which error could have occurred without Eve's eavesdropping. Bob begins by publicly communicating to Alice which measurement operators he used for each of the received bits. Alice then in turn publicly communicates to Bob which of his measurement operator choices were correct. After this two way communication, Alice and Bob delete the bits corresponding to the incompatible measurement choices to produce shorter sequences of bits which we call respectively Alice's raw key and Bob's raw key. If there is no intrusion, then Alice's and Bob's raw keys will be in total agreement. However, if Eve has been at work, then corresponding bits of Alice's and Bob's raw keys will not agree with the probability;

$$0 \cdot (1 - \lambda) + \frac{1}{4} \cdot \lambda = \frac{\lambda}{4} \quad (12)$$

In the absence of noise, any discrepancy between Alice's and Bob's raw keys is proof of Eve's intrusion. So to detect Eve, Alice and Bob select a publicly agreed upon random subset of  $m$  bit locations in the raw key, and publicly compare corresponding bits, making sure to discard from the raw key, each bit as it is revealed. The other technique is to select a publicly agreed upon random subset of  $n$  bit locations in the canceled bits, making sure that these bits will violate a Bell inequality. The amount by which a Bell inequality is violated is thus an ideal measure of the security of the key.

## 4 Secure Quantum Communication

Since BB84 quantum key distribution has developed quickly. Quantum communication holds secret promise for transmission of secure message via quantum cryptography, distribution of quantum information, and distributing protocol and quantum teleportation. Many attempts have been made to apply these methods in design-ing communication protocols [50]. In 1999, Shimizo and Imoto proposed a DSQC protocol using entangled photon pairs [51]. In their scheme the ciphertext is encoded in the state of the entangled pairs, and they are transmitted from Alice to Bob. Bob performs a Bell-basis measurement to read out the partial information. Full information of the ciphertext is read out after Alice notifies him of the encoding basis through a classical communication. Beige et al. proposed a Deterministic Secure Quantum Communication (DSQC) scheme based on a single photon two-qubit state in 2002; in this scheme, the message can be read out only after transmission of additional classical information for each qubit [52]. In 2002, Bostrom and Felbinger presented a scheme for quasi-secure direct communication with EPR pairs [53], this scheme was based on quantum dense coding and the protocol called the ping-pong scheme [54]. Also in 2002, Long and Liu proposed a two-step highly efficient QKD protocol [55]. In 2003, the formal procedure to use protocol for quantum secure direct communication (QSDC) was given [56]. Today there are many people in the world studying the subject.

## 5 Quantum Key Distribution in Satellite Communication

It is clear that traditional cryptosystems are breakable given enough computing time, quantum cryptography offers the promise of unconditional security without face-to-face exchanges. Rather than relying on problems believed to be computationally “difficult,” quantum cryptography uses basic quantum physics laws to provide provable unconditional security. The main principles which are used for quantum cryptography are the following:

- (a) It is not possible to determine simultaneously the position and the momentum of a particle with arbitrary high accuracy (Heisenbergs uncertainty principle).
- (b) It is not possible to measure the polarization of a photon in the vertical-horizontal basis and simultaneously in the diagonal basis.
- (c) Each measurement of the quantum state perturbs the quantum state.
- (d) It is not possible to copy quantum states (No-cloning-theorem).



## 5.1 BB84 Quantum Cryptography Protocol

The first quantum cryptographic communication protocol, called BB84, was invented in 1984 by Bennett and Brassard [46]. This protocol has been experimentally demonstrated to work for a transmission over 30 km of fiber optic cable [47, 48]. In this section we describe the BB84 protocol. The basic tools are a quantum channel connecting Alice and Bob and a public classical channel, where Eve is allowed to listen passively, but not allowed to change the transmitted message. For the quantum channel, we use four signal states. For simplicity, let us for now regard the signals as realized by single photons in the polarization degree of freedom. Consider two sets of orthogonal signals, one formed by a horizontal and a vertical polarized photon, and the other formed by a  $45^\circ$  and  $135^\circ$  polarized photon. These four polarized states are non-orthogonal. The overlap probability between signals from two different sets is one half. Bob has two measurement devices at his hand, one in the rectilinear (i.e., vertical/horizontal) basis and one in the diagonal (i.e.,  $45^\circ/135^\circ$ ) basis. Notice that Bob's two measurements do not commute. To assure the detection of Eve's eavesdropping, Bennett and Brassard require Alice and Bob to communicate in two phases; in the first phase Alice and Bob communicate over a one-way quantum channel as follows: (a) Alice sends a sequence of signals, each randomly chosen from one of the above four polarizations. (b) For each signal, Bob randomly chooses one of the two measurements, rectilinear or diagonal basis devices to perform a measurement. (c) Bob confirms that he has received and measured all signals. In the first phase, Alice is required, each time she transmits a single bit, to use randomly with equal probability one of the two orthogonal alphabets it follows from Heisenberg's uncertainty principle that no one, not even Bob or Eve, can receive Alice's transmission with an accuracy greater than 75% [49].

For each bit transmitted by Alice, we assume that Eve performs one of two actions, opaque eavesdropping with probability  $\lambda$ , or no eavesdropping with probability  $1 - \lambda$ . Thus, Eve is eavesdropping on each transmitted bit or Eve is not eavesdropping at all. Because Bob's and Eve's choice of measurement operators are stochastically independent of each other and of Alice's choice of alphabet, Eve's eavesdropping has an immediate and detectable impact on Bob's received bits. Eve's eavesdropping causes Bob's error rate to jump from 25% to;

$$\frac{1}{4} \cdot (1 - \lambda) + \frac{1}{2} \cdot \frac{1}{4} \cdot \lambda = \frac{1}{4} + \frac{\lambda}{8} \quad (13)$$

Thus, if Eve eavesdrops on every bit, i.e., if  $\lambda = 1$ , then Bob's error rate jumps from 25 to 37.5%, a 50% increase. So to intercept and gain information on the key, an eavesdropper must make measurements on some or all of the sent pulses. An eavesdropper can intercept, measure and resend every pulse but has to guess the random basis. This results in a 25% error rate in the key established between sender and receiver. The sender and receiver can monitor for eavesdropping by monitoring

the error rate of their system. Any increase of the error rate above a threshold value can be interpreted as an insecure line.

Phase 2 is dedicated to eliminating the bit locations (and hence the bits at these locations) at which error could have occurred without Eve's eavesdropping. Bob begins by publicly communicating to Alice which measurement operators he used for each of the received bits. Alice then in turn publicly communicates to Bob which of his measurement operator choices were correct. After this two way communication, Alice and Bob delete the bits corresponding to the incompatible measurement choices to produce shorter sequences of bits which we call respectively Alice's raw key and Bob's raw key. If there is no intrusion, then Alice's and Bob's raw keys will be in total agreement. However, if Eve has been at work, then corresponding bits of Alice's and Bob's raw keys will not agree with probability;

$$0 \cdot (1 - \lambda) + \frac{1}{4} \cdot \lambda = \frac{\lambda}{4} \quad (14)$$

In the absence of noise, any discrepancy between Alice's and Bob's raw keys is proof of Eve's intrusion. So to detect Eve, Alice and Bob select a publicly agreed upon random subset of  $m$  bit locations in the raw key, and publicly compare corresponding bits, making sure to discard from the raw key each bit as it is revealed. The other technique is to select a publicly agreed upon random subset of  $n$  bit locations in the cancelled bits, making sure that these bits will violate a Bell inequality. The amount by which a Bell inequality is violated is thus an ideal measure of the security of the key.

## 5.2 *Entangled Photon Based Quantum Cryptography Protocol*

Einstein, Podolsky, and Rosen (EPR) in their famous 1935 paper [42] challenged the foundations of quantum mechanics by pointing out a "paradox." There exist spatially separated pairs of particles, henceforth called EPR pairs, whose states are correlated in such a way that the measurement of a chosen observable  $A$  of one, automatically determines the result of the measurement of  $A$  of the other. Since EPR pairs can be pairs of particles separated at great distances, this leads to what appears to be a paradoxical "action at a distance."

For example, it is possible to create a pair of photons (each of which we label below with the subscripts 1 and 2, respectively) with correlated linear polarizations. An example of such an entangled state is given by;

$$|\Omega_0\rangle = \frac{1}{\sqrt{2}} \left( |0\rangle_1 \left| \frac{\pi}{2} \right\rangle_2 + \left| \frac{\pi}{2} \right\rangle_1 |0\rangle_2 \right) \quad (15)$$

where state  $|0\rangle$  is a vertical linear polarization photon and state  $|1\rangle$  is a horizontal linear polarization photon [42].

Einstein et al. [42] then state that such quantum correlation phenomena could be a strong indication that quantum mechanics is incomplete, and that there exist “hidden variables,” inaccessible to experiments, which explain such “action at a distance”.

In 1964, Bell [45] gave a means for actually testing for locally hidden variable (LHV) theories. He proved that all such LHV theories must satisfy the Bell inequality. Quantum mechanics has been shown to violate the inequality.

In 1991, Ekert has devised a quantum protocol based on the properties of quantum-correlated particles [43].

The EPR quantum protocol is a 3-state protocol that uses Bell’s inequality to detect the presence or absence of Eve as a hidden variable. Consider three possible polarization states of EPR pair,

$$|\Omega_0\rangle = \frac{1}{\sqrt{2}} \left( |0\rangle_1 \left| \frac{3\pi}{6} \right\rangle_2 + \left| \frac{3\pi}{6} \right\rangle_1 |0\rangle_2 \right) \quad (16)$$

$$|\Omega_1\rangle = \frac{1}{\sqrt{2}} \left( \left| \frac{\pi}{6} \right\rangle_1 \left| \frac{4\pi}{6} \right\rangle_2 + \left| \frac{4\pi}{6} \right\rangle_1 \left| \frac{3\pi}{6} \right\rangle_2 \right) \quad (17)$$

$$|\Omega_2\rangle = \frac{1}{\sqrt{2}} \left( \left| \frac{2\pi}{6} \right\rangle_1 \left| \frac{5\pi}{6} \right\rangle_2 + \left| \frac{5\pi}{6} \right\rangle_1 \left| \frac{2\pi}{6} \right\rangle_2 \right) \quad (18)$$

For each of these states, we choose the following corresponding operators  $M_0$ ,  $M_1$ , and  $M_2$ , given as the following:

$$M_0 = |0\rangle\langle 0|, \quad M_1 = \left| \frac{\pi}{6} \right\rangle\langle \frac{\pi}{6}|, \quad M_2 = \left| \frac{2\pi}{6} \right\rangle\langle \frac{2\pi}{6}|.$$

there are two stages to the EPR protocol, the first stage over a quantum channel, the second over a public channel.

In the first stage for each time slot, a state  $|\Omega_j\rangle$  is randomly selected with equal probability from the set of states  $\{|\Omega_1\rangle, |\Omega_2\rangle, |\Omega_3\rangle\}$ .

One photon of this EPR pair is sent to Alice, the other to Bob. Alice and Bob at random with equal probability separately and independently select one of the three measurement operators  $M_0$ ,  $M_1$ , and  $M_2$ , and accordingly measure their respective photons. Alice records her measured bit. On the other hand, Bob records the complement of his measured bit. This procedure is repeated for as many time slots as needed.

In stage 2, Alice and Bob communicate over a public channel. At first Alice and Bob carry on a discussion over a public channel to determine those bit slots at which they used the same measurement operators. They each then separate their respective bit sequences into two subsequences. One subsequence, called the raw

key, consists of those bit slots at which they used the same measurement operators. The other subsequence, called the rejected key, consists of all the remaining bit slots. Now Alice and Bob now carry on a discussion over a public channel comparing their respective rejected keys to determine whether or not Bell's inequality is satisfied. If it is, Eve's presence is detected. If not, then Eve is absent.

Finally in the presence of noise, the remaining phase of the EPR protocol is the reconciliation phase [44].

## 6 Free-Space Quantum Cryptography

There are two applications which require free-space quantum cryptography rather than fibre based one. The first is short distance communication up to several kilometers, mainly in urban areas, where a fibre based connection is too expensive to deploy. The second is secure satellite communication, where a fibre link is not possible.

The success of QKD over free-space optical paths depends on the transmission and de-tection of single photons against a high background through a turbulent medium. Although this problem is difficult, a combination of sub-nanosecond timing, narrow filters [45, 57], spatial filtering [46] and adaptive optics [47] can render the transmission and detection problems tractable. Furthermore, the essentially non-birefringent nature of the atmosphere at optical wavelengths allows the faithful transmission of the single-photon polarization states used in the free-space QKD protocol.

From 1991, when the free-space QKD was first introduced over an optical path of about 30 cm several demonstrations (indoor optical paths of 205 m and outdoor optical paths of 75 m) increased the utility of QKD by extending it to line-of-site laser communications systems. There are certain key distribution problems in this category for which free-space QKD would have definite practical advantages (as for example, it is impractical to send a courier to a satellite). In 1998 a research group at Los Alamos National Laboratory, New Mexico, USA developed a free-space QKD over outdoor optical paths of up to 950 m under night-time conditions [48]. Four years later, in 2002 the same laboratory have demonstrated that free-space QKD is possible in daylight or at night, protected against intercept/resend, beamsplitting and unambiguous state discrimination (USD) eavesdropping, and even photon number splitting (PNS) eavesdropping at night, over a 10 km, 1-airmass path, which is representative of poten-tial ground-to-ground applications and is several times longer than any previously reported results [49].

## 7 Free-Space Quantum Cryptography in Satellite Communication

With the exponential expansion of electronic commerce the need for global protection of data is paramount. Conventional key exchange methods generally utilize public key methods and rely on computational complexity as proof against tampering and eavesdropping. Satellite systems thus require future-proofing against the rapid improvements in computational power that may occur during their operational lifetime (many years). In this chapter we examine how can we use the free-space quantum channel in the future years of satellite telecommunication.

The quantum computing algorithms can be used to affirm our communication in the following four ways [58, 59]:

- (1) Open-air communication (horizontal telecommunication, below 100 km, instead of optical cable, using the twisted surface of Earth).
- (2) Satellite communications (between 300 and 800 km altitude, signal encoding and decoding). Quantum error correction allows quantum computation in a noisy environment. Quantum computation of any length can be created as accurately as desired, as long as the noise is below a certain threshold, e.g.  $P < 10^{-4}$ .
- (3) Satellite broadcast (our broadcast satellite orbit at 36,000 km, using 27 MHz signal) [50]. In quadrature phase shift keying (QPSK) every symbol contains two bits, this is why the bit speed is 55 Mbs. Half the bits is for error-coding, in the best case we only have 38 Mbs, but in common solutions there is only 27–28 Mbs, in which 5–6 TV-channels can be stored with a bandwidth of 2–5 Mbs each. The quantum algorithms can prove the effective bandwidth to better fill the band as in the traditional case.
- (4) Satellite-satellite communication (between broadcast or other satellites, using free-space, for signal coding and encoding, super density coding etc.).

So by placing a source of single photons and entangled photons on satellites we can propose a satellite based global key exchange system for key exchange between any two arbitrary points on the globe. This system would work by first exchanging keys between one ground station and the satellite. The satellite would then have to store the key securely until the second ground station came into view (up to several hours later). Exchanging the key with this second ground station would allow the first key to be sent down using an absolutely secure one-time-pad encoding scheme. The global reach of the system may be what drives the development but it will probably cost well in excess of ten million Euros (dollars) to build and fly [51].

## 8 Conclusions

In this chapter we survey some results in quantum communication. A brief introduction to some principles of quantum mechanics that are essential to understanding quantum communication is presented, and the main connections between quantum mechanics and secure information transfer have been discussed. It has been seen that the laws of quantum physics guarantee the security of sharing keys between two parties based on quantum cryptography, and provide a mechanism by which any attempt at eavesdropping can be detected immediately.

So, although quantum cryptography is not so practical right now, it is still worthy of study for several reasons. Unlike public-key cryptosystems, currently it works only over short distances. Also, with sufficient technical improvements, it might be possible in the future to implement quantum cryptography over long distances.

In this chapter, some results of the application of quantum cryptography in satellite communication has been presented. A brief introduction to quantum cryptography that is essential to understanding quantum satellite communication is presented. Although quantum cryptography is not so practical right now, it is still worthy of study for several reasons. Unlike public-key cryptosystems, currently it works only over short distances. Also, with sufficient technical improvements, it might be possible in the future to implement quantum cryptography over long distances. So, it will be possible by placing a source of single photons and entangled photons on satellites, to design global secure quantum communication networks.

## References

1. Metwaly, A., Rashad, M.Z., Omara, F.A., Megahed, A.A.: Architecture of point to multipoint QKD communication systems (QKDP2MP). In: 8th International Conference on Informatics and Systems (INFOS), Cairo, pp. NW 25–31. IEEE (2012)
2. Farouk, A., Omara, F., Zakria, M., Megahed, A.: Secured IPsec multicast architecture based on quantum key distribution. In: The International Conference on Electrical and Bio-medical Engineering, Clean Energy and Green Computing, pp. 38–47. The Society of Digital Information and Wireless Communication (2015)
3. Farouk, A., Zakaria, M., Megahed, A., Omara, F.A.: A generalized architecture of quantum secure direct communication for N disjointed users with authentication. *Sci. Rep.* **5**, 16080–16080 (2014)
4. Wang, M.M., Wang, W., Chen, J.G., Farouk, A.: Secret sharing of a known arbitrary quantum state with noisy environment. *Quantum Inf. Process.* **14**(11), 4211–4224 (2015)
5. Naseri, M., Heidari, S., Batle, J., Baghfalaki, M., Gheibi, R., Farouk, A., Habibi, A.: A new secure quantum watermarking scheme. *Optik-Int. J. Light Electron Opt.* **139**, 77–86 (2017)
6. Batle, J., Ciftja, O., Naseri, M., Ghoranneviss, M., Farouk, A., Elhoseny, M.: Equilibrium and uniform charge distribution of a classical two-dimensional system of point charges with hard-wall confinement. *Phys. Scr.* **92**(5), 055801 (2017)

7. Geurdes, H., Nagata, K., Nakamura, T., Farouk, A.: A note on the possibility of incomplete theory (2017). [arXiv:1704.00005](https://arxiv.org/abs/1704.00005)
8. Batle, J., Farouk, A., Alkhambashi, M., Abdalla, S.: Multipartite correlation degradation in amplitude-damping quantum channels. *J. Korean Phys. Soc.* **70**(7), 666–672 (2017)
9. Batle, J., Naseri, M., Ghoranneviss, M., Farouk, A., Alkhambashi, M., Elhoseny, M.: Shareability of correlations in multiqubit states: Optimization of nonlocal monogamy inequalities. *Phys. Rev. A* **95**(3), 032123 (2017)
10. Batle, J., Farouk, A., Alkhambashi, M., Abdalla, S.: Entanglement in the linear-chain Heisenberg antiferromagnet Cu (C 4 H 4 N 2) (NO 3) 2. *Eur. Phys. J. B* **90**, 1–5 (2017)
11. Batle, J., Alkhambashi, M., Farouk, A., Naseri, M., Ghoranneviss, M.: Multipartite non-locality and entanglement signatures of a field-induced quantum phase transition. *Eur. Phys. J. B* **90**(2), 31 (2017)
12. Nagata, K., Nakamura, T., Batle, J., Abdalla, S., Farouk, A.: Boolean approach to dichotomic quantum measurement theories. *J. Korean Phys. Soc.* **70**(3), 229–235 (2017)
13. Abdolmaleky, M., Naseri, M., Batle, J., Farouk, A., Gong, L.H.: Red-Green-Blue multi-channel quantum representation of digital images. *Optik-Int. J. Light Electron Opt.* **128**, 121–132 (2017)
14. Farouk, A., Elhoseny, M., Batle, J., Naseri, M., Hassanien, A.E.: A proposed architecture for key management schema in centralized quantum network. In: *Handbook of Research on Machine Learning Innovations and Trends*, pp. 997–1021. IGI Global (2017)
15. Zhou, N.R., Li, J.F., Yu, Z.B., Gong, L.H., Farouk, A.: New quantum dialogue protocol based on continuous-variable two-mode squeezed vacuum states. *Quantum Inf. Process.* **16**(1), 4 (2017)
16. Batle, J., Abutalib, M., Abdalla, S., Farouk, A.: Persistence of quantum correlations in a XY spin-chain environment. *Eur. Phys. J. B* **89**(11), 247 (2016)
17. Batle, J., Abutalib, M., Abdalla, S., Farouk, A.: Revival of Bell nonlocality across a quantum spin chain. *Int. J. Quantum Inf.* **14**(07), 1650037 (2016)
18. Batle, J., Ooi, C.R., Farouk, A., Abutalib, M., Abdalla, S.: Do multipartite correlations speed up adiabatic quantum computation or quantum annealing? *Quantum Inf. Process.* **15**(8), 3081–3099 (2016)
19. Batle, J., Bagdasarayan, A., Farouk, A., Abutalib, M., Abdalla, S.: Quantum correlations in two coupled superconducting charge qubits. *Int. J. Mod. Phys. B* **30**(19), 1650123 (2016)
20. Batle, J., Ooi, C.R., Abutalib, M., Farouk, A., Abdalla, S.: Quantum information approach to the azurite mineral frustrated quantum magnet. *Quantum Inf. Process.* **15**(7), 2839–2850 (2016)
21. Batle, J., Ooi, C.R., Farouk, A., Abdalla, S.: Nonlocality in pure and mixed n-qubit X states. *Quantum Inf. Process.* **15**(4), 1553–1567 (2016)
22. Metwaly, A.F., Rashad, M.Z., Omara, F.A., Megahed, A.A.: Architecture of Multicast Network Based on Quantum Secret Sharing and Measurement (2015)
23. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: *Proceedings of the International Conference on Computer Systems and Signal Processing*, vol. 175, Bangalore, 1984
24. Ekert, A.: *Phys. Rev. Lett.* **67**, 661 (1991)
25. Shor, P.W., Preskill, J.: *Phys. Rev. Lett.* **85**, 441 (2000)
26. Lutkenhaus, N.: *Phys. Rev. A* **61**, 052304 (2000)
27. Einstein, A., Podolsky, B., Rosen, N.: Can quantum, mechanical description of physical reality be considered complete? *Phys. Rev.* **47**, 777 (1935)
28. Bohm, D.: *Quantum Theory*. Prentice-Hall, Englewood Cliffs (1951)
29. Ekert, A.K.: Quantum cryptography based on Bell’s theorem. *Phys. Rev. Lett.* **67**(6), 661–663 (1991)
30. Walker, J.G., Seward, S.F., Rarity, J.G., Tapster, P.R.: *Quantum Opt.* **1**, 75–82 (1989)
31. Seward, S.F., Tapster, P.R., Walker, J.G., Rarity, J.G.: *Quantum Opt.* **3**, 201–207 (1991)
32. Buttler, W.T., et al.: *Phys. Rev. A* **57**, 2379–2382 (1998)
33. Primmerman, C.A., et al.: *Nature* **353**, 141–143 (1991)

34. Bennett, C.H., DiVincenzo, D.P., Smolin, J.A.: Capacities of quantum erasure channels. [arXiv:quant-ph/9701015](#)
35. Buttler, W.T., Hughes, R.J., Kwiat, P.G., Lamoreaux, S.K., Luther, G.G., Morgan, G.L., Nordholt, J.E., Peterson, C.G., Simmons, C.M.: Practical free-space quantum key distribution over 1 km. [arXiv:quant-ph/9805071](#)
36. Bacsardi, L.: Using quantum computing algorithms in future satellite communication. *Acta Astronautica* **57**(28), 224229 (2005)
37. Bacsardi, L.: Satellite communication over quantum channel. *Acta Astronautica* **61**, 151–159 (2007). Gschwindt, A.: Satellite broadcast, in Hungarian, Muszaki Konyvkiado, Budapest (1997)
38. Rarity, J.G., Tapster, P.R., Gorman, P.M., Knight, P.: Ground to satellite secure key exchange using quantum cryptography. *New J. Phys.* **4**, 82 (2002)
39. Sakurai, J.J.: *Modern Quantum Mechanics*. Addison-Wesley Publication Company (1985)
40. Nielson Michael, A., Chuang Hsaac, L.: *Quantum Information and Computation*. Cambridge University Press (2000)
41. Deng, F.G., Li, X.H., Li, C.Y., Zhou, P., Zhou, H.Y.: *Phys. Rev. A* **72**, 044301 (2005)
42. Bell, J.S.: *Physics* **1**, 195–200 (1964)
43. Johns, W.: *Quantum Teleportation; Deutsch's Algorithm*. Lecture Notes. University of Calgary (2006)
44. Cirac, J.I. et al.: *Phys. Rev. Lett.* **78**, 3221 (1997); Van Enk, S.J., Cirac, J.I., Zoller, P.: *Science* **279**, 205 (1998)
45. Bennett, C.H., et al.: *Phys. Rev. Lett.* **70**, 1895 (1993)
46. Bennett, Charles H., Gilles, B.: Quantum cryptography: public key distribution and coin tossing. In: *International Conference on Computers, Systems and Signal Processing*, Bangalore, India, pp. 175–179, December 10–12, 1984
47. Phoenix, S.J., Townsend, P.D.: Quantum cryptography: how to beat the code breakers using quantum mechanics. *Contemp. Phys.* **36**(3), 165–195 (1995)
48. Townsend, P.D.: Secure key distribution system based on quantum cryptography. *Electron Lett.* **30**(10), 809–811 (1994)
49. Lomonaco, Jr. S.J.: A Quick Glance at Quantum Cryptography. [arXiv:quant-ph/9811056](#)
50. Gui-In, L., et al.: *Front. Phys. China* **2**(3): 252–273 (2007)
51. Shimizu, K., Imoto, N.: *Phys. Rev. A* **60**, 157 (1999)
52. Beige, A., Englert, B.G., Kurtsiefer, C.: *Acta Phys. Pol.* **101**(3), 357 (2002)
53. Bostrom, K., Felbinger, T.: *Phys. Rev. Lett.* **89**, 187902 (2002)
54. Wojcik, A.: *Phys. Rev. Lett.* **90**, 157901 (2003)
55. Long, G.L., Liv, X.S.: *Phys. Rev. A* **65**, 032302 (2002)
56. Deng, F.G., Long, G.L., Liv, X.S.: *Phys. Rev. A* **68**, 042317 (2003)
57. Shannon, C.E., Weaver, W.: A more complete analysis of the communication problem can be found. In: *The Mathematical Theory of Communication*. University of Illinois Press, Chicago (1963)
58. Fu-Guo, D., Xi-Han, L., Chun-Yan, L., Ping, Z., Hong-Yu, Z.: *Phys. Scr.* **76**, 25–30 (2007)
59. Deng, F.G., Long, G.L., Liu, X.S.: *Phys. Rev. A* **68**, 042317 (2003)



Quantum Computing: An Environment for Intelligent  
Large Scale Real Application

Hassanien, A.E.; Elhoseny, M.; Kacprzyk, J. (Eds.)

2018, IX, 505 p. 203 illus., Hardcover

ISBN: 978-3-319-63638-2