# Quantum Communication versus Classical Communication

Ola Hegazy
Imam Abdulrahman Bin Faisal University, KSA
Faculty of Community Service, Imam Abdulrahman Bin Faisal University, KSA

***Abstract:*** This paper introduces the quantum communication as the new era of data communication and compares it with the classical ordinary way of data communication. In this comparison we introduce the main basics and concepts of the quantum communications that mainly rely on the quantum mechanics, which is mainly based on Super-position principle, No-Cloning theorem, Entanglement phenomena, and Super-dense coding technique. In this paper we will present some basic definitions of Super-position principle, No-Cloning theorem, Entanglement in quantum mechanics, present how to use the maximally entangled states known as Bell States, and Super-dense Coding technique to achieve secure direct message communication.

***Keywords:*** *Super-position, Entanglement, Quantum Secure Direct Communication (QSDC), and Super dense Coding.*

## I. INTRODUCTION AND BACKGROUND

In recent years, a new communication era of quantum communication or in other words ***Quantum Teleportation*** has been raised, and a lot of researches has been addressing the differences between the quantum communication and the classical communication in the terms of cryptographic techniques [1,2,3]. This mainly because of the ultimate security of the quantum media nature which guarantees the ***confidentiality*** of the message, and this kind of security is based on the quantum mechanics laws rather than the mathematical complexity as in the classical cryptography techniques. Rather than the security and confidentiality of transmission, there are other aspects to be considered. In a good transmission the grantee of transmission for all data and information of a message is also an important issue along with the sharpness and correctness of the delivery of this data; which means an error/noise free transmission without any interpretation for the message, these two aspects grantees the ***integrity*** and ***availability*** of the message. The last two issues are primitively granted by the characteristics of the quantum phenomena that are governed by the quantum mechanics.

On the other hand; the old way of classical communication depends mainly on the power of mathematical computations which is increased greatly nowadays with the development of technology every day [4]. They use this hardness and infeasibility of the mathematical computation in evaluating the formula that used to encrypt the private message using a pre-shared key and again to decrypt it on the other side depending somehow on the same formula or its reverse.

In all researches that has been addressed the comparison between these two techniques, there are only some demonstrations of the historical development of the quantum cryptography as started in 1984 when Bennett [5] proposed his new approach of quantum key distribution (QKD) that uses the quantum ideologies for distribution of quantum private secret key, where as this was the first application of the quantum cryptography alike the classical cryptograph, and some other demonstrations of the historical development of the classical techniques used to create complicated formula to encrypt the plain text with more and more lengthy keys.

In my work here, I'll focus on some important differences between the quantum teleportation and the classical communication that make the quantum one to be a way advanced than the classical one.

## II. WHY QUANTUM NOT CLASSICAL BIT?

### 2.1 The high security and large capacity of information

Hegazy, 2009 [4] paper clearly indicates that as the security of any message transmission is always the main target of any communication (sometimes more important than the communication itself), the quantum communication using the *quantum cryptography* arises particularly for this reason and gained wide acceptance and popularity. Also, we can say that quantum communication can excel in this field, and this is mainly because of the properties of the quantum transmission media which are the light photons. At the time that the classical transmission uses the electric field which constitutes of electrons to represent one unit of information "bit", by using two different voltage levels to express the "1" and "0" bits, so every bit can only represent one of these two states; the quantum bit "qubit" is represented by the light photon which is expressing the bit representation in its polarization and this polarization could be in two basic states; vertical polarization and horizontal polarization, but the most interesting phenomena of this qubit is it could have a ***superposition*** of both polarizations, a property which is fundamental to quantum mechanics [6]. These two polarization statuses in which a *qubit* can be measured are defined as "basis states" or "basis vectors", they are represented by ***bra-ket*** —or **Dirac** notation labelled $\left|0\right\rangle$ and $\left|1\right\rangle$. The pure status of any *qubit* is defined as a rectilinear ***Superposition*** of the basis states, that means that the *qubit* could be described as the linear addition of the qubits $\left|0\right\rangle$ and $\left|1\right\rangle$ and it is defined by the function "$\left|\psi\right\rangle = \left(a\left|0\right\rangle + b\left|1\right\rangle\right)$" with the coefficient ***a*** and coefficient ***b*** are complex numbers.

So, by using this *Superposition* states and the infinite values of the complex numbers ***a*** and ***b***, we can represent a **huge amount** of information by these two *qubits*, while the two classical bits can only represent 4 values of information.

When this *qubit* is measured in the typical basis, the probability to get the result $\left|0\right\rangle$ equals $\boldsymbol{a^2}$ and the probability to get the result of $\left|1\right\rangle$ is $\boldsymbol{b^2}$. Whereas the absolute squares of the values should equal to the sum of the probabilities, then this leads to ***a*** & ***b*** should be govern by the formula $\left|a\right|^2 + \left|b\right|^2 = 1$, natively because this assures that you must measure either one state or the other.

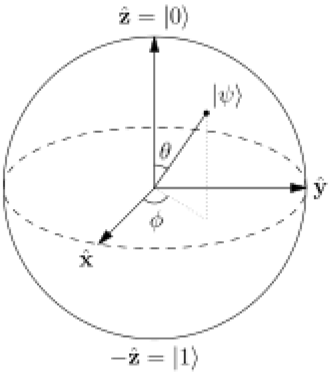

Fig. 1 Qubit bases vectors

The properties of the photons are governed by the quantum mechanics, which in turn are way different of the properties of the electrons that used in the classical communication. One of the most interesting properties of the light particles "photons" is that; their quantum status cannot be measured without alerting it and fluctuating the state of the photons themselves [4]. So as the measuring operation itself is consider a manipulation of their state. So, the use of this phenomenon of the photon's characteristics will support the disabling of one of the well known and dangerous eavesdropping attacks; which is reading or downloading the information of the message during transmission without being noticed by the two legitimated parities. That's because any trial of measuring the state of any qubit will definitely alert it, so only the allowed parity at the receiving end can only measure it without saving cause after measuring it will be changed and respectively missed.

### 2.2 The nature of the qubit and its representation

The most important and interesting characteristics of the quantum mechanics rather than its physical nature are:

1. The ***No-Cloning*** theorem.
2. The ***Entanglement*** phenomenon and its example ***Super-dense coding technique***.

### The *No-Cloning* theorem

An exciting feature of the quantum state is that; it can't be copied, and it is known as "***No-Cloning theorem***" [6] or in other words -in physics- "***no-go theorem***" of quantum media which prevents the generation of identical states of a random quantum status. As will be explained in the following phenomenon; that we can generate a correlated state of two pair of photons to have a certain correlation factor(s) between them but not exact factors for both states.

Accordingly, even in case of any intruder or eavesdropper could drop the message or read it through the transmission (with the knowledge of both legitimated transmission parities), he/she couldn't reuse it by saving it or resend it.

### The *Entanglement* phenomenon

*Quantum Entanglement* is another exciting and surprising phenomenon of the light photons that could be defined as the occurrence of a certain correlation that born between a pair or groups of photons that are generated or interacted together in a way that such a quantum state of each photon can't be expressed separately but alternatively, a quantum state may be defined to the whole system. States that having such correlations are named ***entangled*** states. Amongst these states, ones that possess the highest correlation are known as "maximally entangled states or EPR states" as historically, it had been pointed out by Einstein as the concept of a non-local influence due to entanglement, Podolsky, and Rosen (Hayashi, 2006) [7]. This phenomenon can be used to cause *non-local phenomenon* that is the pure nature of the quantum entanglement phenomena is the feature of non-local connections between broadly detached particles that have been intermingled in the past. In other words, to create entangled particles, it is important to allow them to intermingle at some point. Consequently, as Lee, 2005 stated clearly that "the non-local characteristic of entanglement phenomena is pre-generated from the local characteristic of interaction" [8].

Measurements of physical characteristics of the quantum photons like; position, polarization, spin, momentum, etc. applied to entangled photons are found to be properly correlated. As an example; in case if there is a pair of photons that is created in certain method such that the total sum of their spin is measured to be equal to zero, and we find one of them is having a clockwise direction relative to a specific axis, then the other one's spin is measurement relative to the same axis will detected to be counter clockwise.

However, according to the nature of quantum measurements, any measurement of any feature of an element can be observed as working on that element, so in the case of entangled elements, the overall entangled system will be affected with that action. Thus, it looks like that any one element of any *entangled pair* will realize what manipulation or evaluation action has been made on the second element, and with which result, although there aren't any known ways for this knowledge to could be exchanged between these elements, because in the moment of this measurement they are mostly apart by subjectively big distance.

Albert Einstein, 1935 had addressed this subject in his paper with Boris Podolsky and Nathan Rosen [9], were that phenomena has been considered, defining what happened to be widely known as the **EPR paradox**, and shortly thereafter some other papers by Erwin Schrödinger also mention that [10][11]. Einstein and others had believed that this alike behaviour is to be unfeasible, as it breached the local radical view of causation (Einstein pointed to that as **"spooky action at a distance"**) and contended that the agreed equations of quantum mechanics should be accordingly incomplete.

In 1964 physicist **John Stewart Bell** offered his revolutionary paper, "On the Einstein Podolsky Rosen paradox"[12], he presented an identity "based on the spin measurements on pairs of entangled electrons" to EPR's hypothetical oxymoron. Acting their logic, he revealed that the selecting of a measurement setting in one side should not affect the result of a measurement in the other side (and vice versa). Based on this, he proposed an algebraic formulation of locality and realism, and demonstrated some particular situations that this would be incompatible with the estimates of QM theory. Then Bell states his theorem;

***The Bell's theorem*** in its simplest form states that:

"No physical theory of local hidden variables can ever reproduce all of the predictions of quantum mechanics" [13]

For example; the local hidden variables represent the case of the Moon doesn't appear, but that doesn't mean it is not found.

However later, the counterintuitive predictions of quantum mechanics were proved experimentally. Measuring the polarization "or spin of entangled photons" in different directions has been applied experimentally, which show statistically that the local radical view cannot be correct – that making violations of **Bell's inequality**. This has been clarified that even if the measurements are applied faster than the speed of light it could travel in between the fields of measurement: there is no light speed or less effect that can go through the entangled photons [14].

For instance, we can use a quantum gate called the universal **controlled NOT** gate with the **Walsh-Hadamard gate** to create two entangled *qubits*.

### 2.1 The Maximally entangled Bell states with the high efficiency transmission using the *Super-dense* coding technique

According to the above discussion John S. Bell had generate a fully entangled qubits by using the orthogonal basis of the quantum space, and these states are generated by using two qubits one representing the '0' bit and the other representing the '1' bit as $|0\rangle$ and $|1\rangle$. And for four different cases of their maximally entangled states he generated the following superposition states:

$$00 \rightarrow |\phi^{+}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad (1)$$

$$10 \rightarrow |\phi^{-}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \qquad (2)$$

$$01 \rightarrow |\psi^{+}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \qquad (3)$$

$$11 \rightarrow |\psi^{-}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \qquad (4)$$

Deng, 2008 had obviously explain the super dense coding technique as an easy model of the use of quantum entanglement teleportation, this technique is used to transmit two classical bits by transmitting only a unique quantum bit (*qubit*), so the efficiency and effectiveness of the transportation will be increased.

In this technique, before starting the transmission, a third party (or even one of the two parties as in the protocol [15]) should generate an entangled state (two pairs of particles maximally entangled), one of the Bell entangled state, then a pair of the two particles of the entangled *qubits* will be sent to (or being in possession of) the sender "Alice" and the other will be sent to the receiver "Bob".

The sender "Alice" will work on her own qubit to encode two classical bits of information and then send to the receiver "Bob". On Bob's side, he will operate with the reverse action on the received qubit of Alice to using his own qubit (that's the maximally entangled pair of the received qubit) to get back the two classical bits of information that Alice transmitted to him.

For this way of transmission two spatially separated quantum communication lines should be used to create less and less probability of eavesdropping with the more efficiency of transmission by sending the double amount of information that could be sent using the ordinary classical bits transmission. These lines mainly will use the fiber optics cables that are dedicated to the transmission of the light photons and they are quite fast and secure in carrying the content of data, and very hard to be interrupted and almost impossible for the contents data (quantum data) to be intercepted.

## III. QUANTUM SECURE DIRECT COMMUNICATION (QSDC)

Referring to the above discussion we can use quantum teleportation to directly communicate between two sides, with the real message encrypted by qubits instead of the transmission of a key first, which saves time and cost and even the wasting of the precious generation of the quantum bits just to be used as a key not the real message information bits [4].

Also, the use of per-shared key technique to encrypt messages (either in the classical or quantum communications) could make the message transmission vulnerable to dedication in case of the transmission of the key itself has been broken and discovered.

Accordingly, we can deduce that the QSDC is more beneficial from all sides; and we can drive the main advantages of it as following [4]:

1. It doesn't require a pre-transmission of any number of qubits to be used as a key, so it saves time, complicated computations, complicated precautions for the security procedures for other transmission rather than the main data transmission, then respectively it saves cost for the whole process.
2. It grants unconditionally secure transmission of data directly without relying on other combination of lengthy code to help in encryption or to grant more security.
3. It doesn't have a ciphertext with its complications of creating it and decrypting it on the other side.
4. It has the ultimate security features because it's not only detecting the eavesdropping but also preventing it by making its job quite impossible.
5. It has no leakage of information as from the start point of the communication until the end the whole data of the message is transmitted through a perfectly closed transmission lines that any trial of breaking will cause the loss of the data.
6. Due to the nature of the transmitting media, it has no possible expectations of intercepting the data or recording it, as any attempt of this will also destroy the data and for sure will be discovered.

## IV. RESULTS AND DISCUSSIONS

Eventually, we can say that, the use of the quantum teleportation is requiring that the media to be used for this transportation should be in the highest sharpest media that will likely be a coasty one, like fibre optics lines, but which -at the same moment- have the highest characteristics of transmission lines, and grantee a very high quality of unconditionally secure transportation, and that is accomplished by the following procedure's requirements:

- As the two transmitted pairs are send on two different quantum channels that are assumed to be **long distance spatially separated**, then the job of the intruder "Eve" to catch the complete state of the transmitted signal **simultaneously** will be **quite impossible.** she should get both qubits transmitted on the two channels at the same time exactly.
- Then she should **synchronize** her measurements in the same time of intercepting the signal –which is a very hard task- to get the correct transmitted state in that particular instant.

If we assume that Eve can do this hard job successfully, let's then consider the probability of that success:

- ***First***: if she could access the first quantum channel and make her measurement on it, she will get 0 or 1 with prob of ½ for each.
- ***Second***: if she could make the same for the second channel **simultaneously**, then she could get the whole state with prob of ¼.
- Now, for our assumption of using the uniformly generated four Bell states each with prob ¼, then the total probability for Eve to catch the correct transmitted state will be **1/16**.

So, in such situations, for reasonably long messages, the **probability of eavesdropping will definitely reach zero**, whereas for a message that has length **N**, the probability for Eve to get it correctly will be:

$$\left(\frac{1}{16}\right)^{N/2}=\left(\frac{1}{4}\right)^{N} \qquad (5)$$

And finally, to make the correct measurement Eve must know the original **encoding circuit** that is used in the encoding process to get the reversed **decoding circuit** to measure the state she got –as Bob (the legitimate receiver) doing- to get the original equivalent input bits.

Finally, we can summarize our point of view in the comparison between the quantum communications performance & advantages and the classical communications performance & advantages in the following table:

Table 1 Performance factors

| Communication's performance factors | Quantum comm. | Classical comm. |
|---|---|---|
| Security | Excellent | Dependent on the technique |
| Capacity | Very high - minimum the double. | Dependent on the media |
| Efficiency | Full efficiency | Dependent on the media |
| Speed | Very high (speed of light particles) | Limited to the media type |
| Mathematical computations | None | Very high and complicated |
| Implementation | Light photons with quantum gates and quantum transmission media | Electric field with any type of transmission media |
| Media of trans. | Special quantum lines | Different upon the choice |

## CONCLUSIONS

This paper introduced a brief explanation for the reason of using the new trend of quantum communication that based on the quantum mechanics in the instead of the classical way of communication. Main important characteristics of the quantum mechanics is demonstrated and also some important features of their physical phenomena, showing the difference between quantum communication (using the nature of the quantum signal in representing the *qubit*) and the ordinary classical communication using classical bit representation.

After that it is shown how the science make use of those features to introduce the Direct Secure Quantum Communication (QSDC) without going in any details of the transmission protocols that are used in this field. But it has been exhibited the main advantages of the QSDC that based on the pure maximally entangled Bell states to assure unconditional security. Also, for efficiency purposes we have explore the bases of the super-dense coding technique that's also used in the QSDC.

### *Future work*

The quantum mechanics area is a very interesting area that is rich with a lot of surprising features related to the nature of the light photons, and physicians are sincerely working in it to discover all those features and how could we use it. On the other side we (communication engineers) are anxiously working on those properties to get use of them to reach as maximum security in communication networks as much as we could.

So, in our upcoming researches we are going to focus on the ***Quantum teleportation,*** protocols, transmission distance, equipment of quantum logic gates for encryption and decryption, and of course the guided transmission media. And this field is gained its importance even more than the quantum computation because it's the main branch in quantum mechanics that support transmission of data thought computer networks.

### *Abbreviations*

**(QKD)** Quantum Key Distribution.

**(QSDC)** Direct Secure Quantum Communication

### *References*

[1] Vignesh, R.S., Sudharssun, S., Kumar, K.J.J, (2009) Limitations of Quantum & Versatility of Classical Cryptography: A Comparative Study. 2009 IEEE International Conference on Environmental and Computer Science, 333-337.

[2] Goyal, A., Aggrwal, S., Jai, A., (2011) Quantum Cryptography and its Comparison with Classical Cryptography: A Review Paper. 5th IEEE International Conference on Advanced Computing & Communication Technologies, 428-423.

[3] Moizuddin, M., Winston, Dr. J., Qayyum, M., (2017) A Comprehensive Survey: Quantum Cryptography, 978-15090-5814-3/17 IEEE.

[4] Hegazy, O., Bahaa Eldin, A., Dakroury, Y., 2009. Quantum Secure Direct Communication Using Entanglement and Super-Dense Coding. *SECRYPT 2009*, International conference on Security and Cryptography, *July 2009*, Milan, Italy.

[5] Bennett, C.H. and Brassard, G., (1984) Quantum Cryptography: Public Key Distribution and Coin Tossing. Proceedings of IEEE Inter-national Conference on Computers, Systems and Signal Processing, p. 175.

[6] Nielsen, M.A., Chuang, I.L., (2000) Quantum computation and quantum information. Cambridge University press, Cambridge.

[7] Hayashi, M., (2006) Quantum Information, An Introduction. Springer.

[8] Lee, H. at el, (2005) Entanglement Generates Entanglement: Entanglement transfer by interaction.

Physics letters A 338 (2005), 192-196.

[9] Einstein A., Podolsky B., Rosen N., (1935) Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? Phys. Rev. 47 (10): 777–780.

[10] Schrödinger E., Born, M. (1935) Discussion of probability relations between separated sys-tems. Mathematical Proceedings of the Cam-bridge Philosophical Society 31 (4): 555–563.

[11] Schrödinger E., Dirac, P. A. M., (1936) Prob-ability relations between separated systems. Mathematical Proceedings of the Cambridge Philosophical Society 32 (3): 446–452.

[12] Bell, J. S., (1964) On the Einstein Podolsky Rosen Paradox. Physics 1 (3): 195–200.

[13] C.B. Parker (1994). McGraw-Hill Encyclopae-dia of Physics (2nd ed.). McGraw-Hill. p. 542. ISBN 0-07-051400-3

[14] Francis, M., (2012) Quantum entanglement shows that reality can't be local. Ars Technica, 30 October 2012

[15] Deng, F.G., Li, X.H., Li, C.Y., et al., (2008) Quantum Secure Direct Communication Net-work with Einstein-Podolsky-Rosen Pairs. quant-ph/0508015.