Quantum Key Distribution in Computer Networks

Maedeh Abbasi [*1], Ahmad Shariati [1], and Reza Mohammadi [2]
1. Faculty of Physics, Alzahra University, Tehran, Iran
2. Department of engineering and technology, Abu Ali Sina, Hamedan, Iran

E-mail: Ma.abbasi@alzahra.ac.ir

Abstract
The secure transfer of keys between two parties, is one of the primary problems in cryptography. The possibility that the key can be manipulated or intercepted by way of an eavesdropper is the cause for the concern. A promising way to this problem is Quantum Key Distribution (QKD). The secure distribution of keys that may be used to encrypt and decrypt messages is made feasible by this approach, which makes use of the idea of quantum mechanics. QKD offers a degree of protection that can not be done by means of classical cryptography techniques, and has remarkable capability for application in a scope of fields in which secure correspondence is crucial. QKD is a field of study that has brought various conventions pointed toward empowering the safe alternate of cryptographic keys between two parties, Alice and Bob. Two key protocols within this field are the BB84 which was designed by Bennett and Brassard and E91 which was proposed by Ekert. While other protocols have been developed, many draw inspiration from these two foundational approaches. We focused specifically on the E91 protocol and explored its potential for the safe transfer of entangled pairs within computer networks. This protocol utilizes entanglement between particles as a means of verifying the security of the key exchange. Our investigation centered around testing the entanglement swapping for two particles using the E91 protocol, with the aim of developing a novel method for the secure transmission of entangled pairs via computer networks. Our findings suggest promising avenues for future work in implementing secure entanglement swapping in practical applications.

Keywords: QKD, entanglement, swapping, Cryptography, Quantum Cryptography

1. Introduction

In contemporary times, information security is an imperative consideration in numerous applications. Such security practices can be classified into different categories such as network security, application security, cryptography etc. Cryptography serves two crucial purposes, the first one is that, enabling far-flung entities Alice and Bob to communicate with each other and the second one, by use of quantum mechanics this communication happens confidently without interference from a third party (Eve). In protocols that fulfill these two goals, Alice transmits a sequence of randomized bits to Bob via an unsecured communication field whilst ensuring the integrity of the message throughout the transmission. Both objectives can be achieved through secure means if Alice and Bob possess identical, confidential random bit sequences, known as a "key". Utilizing said key, they can execute encryption and decryption processes on the message.

Hence, one of the principal challenges encountered in encryption pertains to the complex predicament of key distribution. Specifically, the core concern centres on the procurement of private keys by Alice and Bob, who do not initially exchange secure information, thereby ensuring Eve's complete inability to access even minute fragments of sensitive data. Regrettably, conventional methods have proved insufficient in addressing this problem, thereby necessitating the employment of quantum mechanics as a means of resolution.

The preservation of records in a classical format is ensured by the ability to examine and replicate it without discernible modifications. However, if the records are stored in an indeterminate quantum state, their duplication is not possible due to the "No-cloning theorem" [3]. The area of quantum computation presents an inherently challenging technological landscape. The accelerated advancement of novel and inventive technologies, rooted in the potent capacities and resources of quantum mechanics, such as quantum entanglement and superposition, enable instantaneous manipulation and measurement of atomic and subatomic information, culminating in exceptionally robust information processing and communication technologies[4].

However, by utilizing the principles of quantum mechanics, a solution to the issue of secure data exchange can be realized. This implies that the creation of an exact

replica of a given quantum state is unfeasible. The aforementioned implies that the key cannot be accessed by Eve. Any attempt on her part to acquire the key will be promptly detected. Accordingly, Quantum Key Distribution(QKD) refers to a procedure whereby keys are exchanged between communication entities through a quantum channel. In essence, QKD capitalizes on qubits, which are constituted by polarized photons that are used to represent bits.

One acclaimed cryptographic technique that has emerged is Quantum Key Distribution (QKD). The principal function of QKD is to establish a secure connection between two parties through cryptographic protocols. It is noteworthy that there are two vital QKD protocols - BB84[1] and E91[2] - that are extensively utilized in this regard. In 1984, Bennett and Brassard introduced the BB84 protocol that capitalizes on the polarization of individual photons. In contrast, the E91 protocol proposed by Ekert in 1991 leverages entangled photons' polarization.

Quantum entanglement remains one of the most remarkable features of quantum mechanics. In spite of violating Einstein's idea of localities[5], quantum entanglement has become an instrumental technology due to its key characteristics in quantum mechanics. While initially having significant implications within the theory itself, quantum entanglement has found new applications in emerging areas of research like quantum information[6] and computing[7].

One of the most renowned forms of entanglement involves a bilateral sharing of qubits between two parties, specifically in the form of EPR or Bell states[8]. The significance of entanglement between two qubits extends beyond its implications for quantum fundamentals and quantum information. Moreover, exploring entangled states that involve a greater number of qubits necessitates the development of a new protocol for quantum information. [9].

In the realm of quantum mechanics, the concept of entanglement is used to describe the behavior of particles whose individual states cannot be accurately described without reference to the states of other particles. This property is characterized by an inseparability of states among the particles in question. Notably, any attempt to measure the state of one entangled particle will necessarily alter the state of all of the entangled particles. The phenomenon of entanglement has been identified as a key concept in quantum applications such as quantum teleportation, ultra-dense coding, and related areas of quantum computing research.

The application of entanglement in the field of quantum cryptography and the potential implications for this area of research have piqued our interest and motivated our exploration.

In this paper, we consider two qubits entanglement swapping[12],[17]-[19]. The article is organized as follows. first, some details that may be required in the future will be mentioned, in section 2 we consider entanglement swapping between 2 particles and will show that in which situation can we see Entanglement swapping then in section 3, we see the application of this method in theory, in section 4, we briefly mention the related works that have been done in this field, The conclusions are given in section 5.

1.1 Qubits

A qubit is a state like |Ψ> over the complex Hilbert space C^2 and it is equivalent to the classical bit. Most of the time a quantum two state system is called a qubit.

1.2 Pure quantum state

For two-dimensional Hilbert space, there is a set of two pure states |0>, |1>, which are orthogonal and so form orthonormal bases in H^2. If we assume that state |Ψ> is a linear combination of basis vectors |0>, |1>, with

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}, |1\rangle = \begin{pmatrix}0\\1\end{pmatrix} \quad (1)$$

superposition of two

$$|\Psi\rangle = \alpha|0\rangle + \beta\,|1\rangle \quad (2)$$

Then it satisfies the condition for being a pure quantum state. In other words, a pure quantum state over Hilbert space H, is denoted by a vector like $|\Psi\rangle \in$ H with unit length, i.e. $\langle\Psi|\Psi\rangle = 1$. If a vector is not unit, normalization can be applied in order to convert a vector to a pure quantum state. In quantum mechanics, a quantum state of a system is a complete description of the system. If the system is a particle, the quantum state accounts for all possible measurements that could be made on the particle.

To offer an example of different bases for the Hilbert space H^2, if we consider rectilinear bases and assign the vertical polarization of a photon 0 ° to $|0\rangle$ and the horizontal polarization 90 ° to $|1\rangle$, then the polarization of diagonal or 45 ° is $|+\rangle = \frac{1}{\sqrt{2}}(|0> + |1>)$ and for polarization of 135 ° is $|-\rangle = \frac{1}{\sqrt{2}}(|0> - |1>)$. Since |+> and |−> are orthogonal, the basis $\{|+\rangle, |-\rangle\}$ is orthonormal.

1.3 Entangled state and Bell state

If we consider H_1 and H_2 as Hilbert spaces and $|\Psi\rangle \in H1 \otimes H2$ be a pure state, the state $|\Psi\rangle$ is a product state in $H = H_1 \otimes H_2$ if there are pure states $|\Psi\rangle 1 \in$ H1 and $|\Psi\rangle 2 \in$ H2 so that $|\Psi\rangle = |\Psi\rangle_1 \otimes |\Psi\rangle_2$, then the pure state $|\Psi\rangle$ is separable if it is a product state in H, otherwise the state $|\Psi\rangle$ is entangled.

If we sent two qubits, then the joint state of these qubits can be one of the state $|00\rangle$, $|11\rangle$, $|01\rangle$, $|10\rangle$, in what follows, we show that how a joint state can be written as a tensor product of two single qubits separately. At times, it is not possible to express a state as a product state of two single qubits. An example of such a state is $|\phi\rangle = |00\rangle + |11\rangle$, which represents the identical polarization of two photons. These states are known as inseparable states.

The Tensor product space $C^2 \otimes C^2$ is also a Hilbert space with the set of vectors $\{|01\rangle = |0\rangle \otimes |1\rangle, |10\rangle = |1\rangle \otimes |0\rangle, |00\rangle = |0\rangle \otimes |0\rangle, |11\rangle = |1\rangle \otimes |1\rangle\}$, where

$$(|0> \otimes |1>) = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, (|1> \otimes |0>) = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, \quad (3)$$

$$(|0> \otimes |0>) = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, (|1> \otimes |1>) = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

This basis is formed by orthogonal vectors and is correspond with the basis in C^4 so that $C^4 = C^2 \otimes C^2$, and so the quantity of elements of the basis is increased with the quantity of tensored Hilbert spaces. In particular, for complex Hilbert space of qubits C^2, as the number of qubits increases, the dimension grows exponentially and hence, n-qubit states are in 2^n dimensional complex Hilbert space C^{2n}.

It is necessary to notice that for simplicity $\otimes$ sign is often disappeared and two kets are decreased to one single ket so that $|0\rangle \otimes |1\rangle = |0\rangle|1\rangle = |01\rangle$. If we consider two arbitrary states $|\phi\rangle 1 = \alpha 1\ |0\rangle + \beta 1\ |1\rangle$ and $|\phi\rangle 2 = \alpha 2\ |0\rangle + \beta 2\ |1\rangle \in C^2$, then an arbitrary product state $\phi \in C^4$ can be written as

$$|\phi\rangle = |\phi\rangle_1 \otimes |\phi\rangle_2 = \alpha 1\alpha 2\ |00\rangle + \alpha 1\beta 2\ |01\rangle + \alpha 2\beta 1\ |10\rangle + \beta 1\beta 2\ |11\rangle \quad (4)$$

If the state $|\Phi>^+ = \frac{1}{\sqrt{2}}(|00> + |11>) \in H^4$ be a product state, it follows that $\alpha_1\beta_2$ and $\alpha_2\beta_1$ are equal to zero, and thus either $\alpha_1 = 0$ or $\beta_2 = 0$, $\alpha_2 = 0$ or $\beta_1 = 0$ so $\alpha_1\alpha_2$ or $\beta_1\beta_2$ vanish and that contradicts with the assumption that$|\Phi>^+$ is a product state and so it can be concluded that $|\Phi>^+$ is inseparable or entangled and thus, it shows that entangled states exist. so if and only if we have an inseperable state, we will have an entangled state. In the field of communications, entanglement is regarded as correlation among non-local measurements. The state $|\Phi>^+$ is called a Bell state. There are four Bell states and all of them are maximally entangled state of a two-qubit system and orthogonal, so they form an orthonormal basis in Hilbert space H^4. these states are

$$|\Phi\rangle^{\pm} = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle \pm |1\rangle \otimes |1\rangle) \quad (5)$$

And

$$|\Psi\rangle^{\pm} = \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle \pm |1\rangle \otimes |0\rangle) \quad (6)$$

They shape a maximally entangled basis, referred to as the Bell basis, of the 4-dimensional Hilbert space for two-qubit. Note that the Bell basis is not unique. In fact, any unitary transformation of the Bell states gives another set of mutually orthogonal states.

2. Entanglement swapping in two-level systems

Quantum Entanglement Swapping, which is a particular phenomenon that proposed by Zukowski and et al.[12], it has been experimentally demonstrated using a variety of different physical systems, including photons, atoms, and superconducting qubits. One notable demonstration was performed by Pan et al. in 1998[19], where they used entanglement swapping to teleport a photon across a distance of 10 kilometers. The potential applications of entanglement swapping include quantum repeaters for long-distance communication, secure QKD, and quantum teleportation. Many research groups around the world are currently investigating these and other potential applications of entanglement swapping. Sometimes entanglement swapping is known as quantum teleportation of entangled states. Quantum teleportation could be a method to transfer quantum information from supply to destination over long distances in a secure manner by using entangled states. This phenomenon is incapable of transferring the physical form of a quantum entity. Instead, it achieves the transfer of quantum information by probabilistically transmitting the precise quantum state of a teleportee to a remote location. It also takes advantage of the Entanglement feature in Bell states (EPR Pair) to transfer an arbitrary state between two observers (Alice and Bob). The difference between quantum teleportation and Entanglement swapping, is that, in teleportation the purpose is to transfer an unknown state of one quantum system to another, but in Entanglement Swapping the purpose is to create entanglement between two distant quantum system[13].

In the paradigmatic entanglement swapping scenario, two entangled particles (A, C) are shared between Alice and Charlie, while Bob and Harry share another entangled pair of particles (B, H). It is assumed that there is no entanglement between Alice's and Bob's particles (A, B), as indicated in Figure 1a. In entanglement swapping, a joint measurement is performed on particles C and H through Charlie and Harry who are located in the same place after retaining their entanglement with their respective partners, make measurement in an appropriate basis at the pair (C, H). The effects of the joint measurement are classically communicated to Alice and Bob, which allows the creation of an entangled state between particles A and B. This phenomenon helps the transfer of entanglement among remote particles that were initially uncorrelated. As it is shown above entanglement is swapped between particles A and B and so Alice and Bob can share an entangled pair.

Quantum communication via an unknown state is established between two pairs without sending each other any quantum information. This can be referred to as entanglement swapping[14]. What we will follow, is considering two parties and observing entanglement swapping between two pairs of qubits. Bell operator [10] acts on these two qubits, which we show with α and β, and project it onto one of the "Bell states". By use of this technique, Alice encodes the state she desires to send into a quantum system and sends it to Bob. The entanglement is used to create the desired quantum state at a distance. Then the quantum state teleports from Alice to Bob and entanglement also teleports "entanglement swapping". Entanglement swapping is a way of sharing quantum information without sharing quantum information. What we are able to do, is entangling two pairs of qubits and then swap entanglement between the pairs. Unlike Figure 1, we show the equations for two parties and suppose that every party has two entangled particles by him/herself. To get rid of disarray, we put equations related to entanglement swapping between Alice and Bob in Appendix A,

In the next section we want to propose a scheme, in which entanglement swapping is applied.

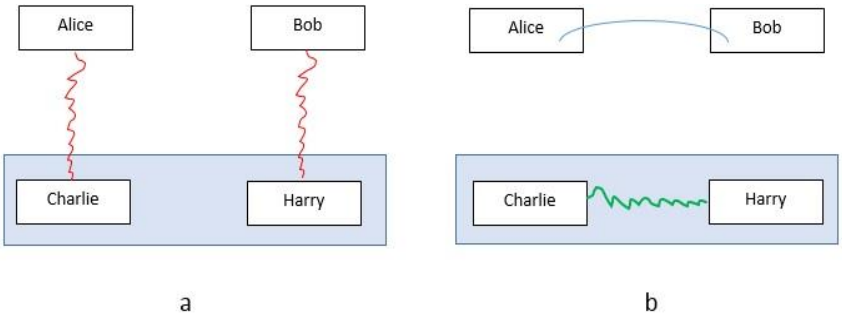

Figure 1: Entanglement Swapping. First in Fig. (a) There are 2 entangled pairs, one between Alice and Charlie, and the other one between Bob and Harry. There is no entanglement between Alice and Bob. However in Fig (b), the measurement on Charlie and Harry's qubits project the entanglement between Alice and Bob.

3. Application of Entanglement Swapping in Quantum Key Distribution

If a group of users in a network, need to communicate with every other, in an effort to send a message, they need to apply encryption and authentication algorithms to communicate securely. There are symmetric and asymmetric algorithms. Symmetric algorithms are more useful for computational purposes. In these algorithms, users use common key for encryption, decryption and authentication the message to be sent, before starting the communication. So the question is how to design a protocol, in order to generate a common key to be used by the group of users to communicate securely. there are several scheme to this purpose, one of them is the scheme based on a trusted third party. This scheme plays an important role to manage a common key between group of users. The more regular strategy to enable a group of users to establish a common key, is the one which is consisting of Key Distribution Center(KDC). In fact KDC is a server, who is responsible to create and distribute a common key. The process is that every user has a secure channel with KDC. If one user wants to communicate securely with other user in a group, sends a request to the center. At first KDC checks the membership of the user and after authentication, distributes an encrypted common key to every member of the group[15], [16]. This method frequently used in cryptography. By use of this strategy we can see the application of entanglement swapping in QKD. One problem in Cryptography is how two remote parties Alice and Bob can communicate in a form that's incomprehensible to a third party, Eve, and to demonstrate that the message was not modified in travel. If both Bob and Alice own the "key", both objectives can be fulfilled securely.

Before we consider our scheme, in order to better understand the process and get rid of complication, we propose step by step the procedure and we show that, despite the absence of any channel between the two parties, they can share a Key with use of KDC. For this purpose, they should perform these steps:

First-we consider that Alice and Bob create a series of N entangled particles in the quantum state $|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$

2nd-Alice and Bob, keep one particle by themselves and send another to the KDC via a public channel.

3rd-KDC measures the state of the particles sent from Alice and Bob in one of the bases |0>, |1>, |+>, |−> and then Alice and Bob also measure their qubits by the use of one of the basis above randomly.

4th-KDC checks Alice's and Bob's selected bases respectively via classical channel, and if the bases are the same, uses that for the next step, otherwise neglect it. We consider that KDC has i similar bases with Alice and j similar bases with Bob. For $i \leq j$, KDC selects i bases from each party to go to the next step.

5th-By the use of i particles that KDC gathers from each parties, composed them, and with the help of Bell state measurement, it establishes i two-qubit system.

6th-At this step, i entangled states will share between Alice and Bob, because of KDC's measurement.

7th-KDC announces its result to Alice and Bob via classical channel.

8th-Alice and Bob also measure the qubits, which are in their hands in one of the bases |0>, |1>, and finally with use of KDC result, they create a series, and in order to gain a key, they compare their own results with KDC's result, for example Alice record her own state as if her basis choices are |0> she records 0, and for |1>, she records 1 , and it is regardless to KDC's state information. But Bob takes the different way, for example if the KDC states are |Φ⟩±, he records 0 for his |0> basis choice, and 1 for |1> basis choice. And for |Ψ⟩±, he records 0 for his |1> basis choice, and 1 for |0> basis choice.

By taking advantage of these Rules, Alice and Bob can reach to the string of identical Key.

4. Related Works

Entanglement swapping is a fundamental phenomenon in quantum mechanics that has found numerous potential applications. Here are some examples and references for each:

1. Quantum teleportation: Entanglement swapping enables teleportation of quantum states across longer distances that exceed the intrinsic distance of quantum channels. This technique was demonstrated in 1998 by Jian-Wei Pan and colleagues[19], who used entanglement swapping to teleport a photon across 10 km of optical fiber.

2. Quantum Cryptography: Entanglement swapping can be used to establish secure communication channels in quantum cryptography. This application takes advantage of the quantum mechanics concept of entanglement to generate secure keys for encryption. Entanglement

swapping has been used to implement practical QKD protocols, as demonstrated by Sang-Wook Han et al.[20]

3. Quantum Computation: Entanglement swapping can be used in quantum computing applications to efficiently distribute quantum entanglement across multiple qubits, thereby improving the efficiency of certain types of quantum algorithms. This application was explored in a theoretical paper by Daniel Gottesman and Isaac L. Chuang [21].

4. Quantum Repeater Networks: Entanglement swapping can be used to enable long-distance communication via quantum channels, for example in quantum repeater networks, where the distribution of entanglement between distant parties is a crucial component of the system. This application was demonstrated experimentally by scientists at the University of Geneva and the University of Vienna in 2012 [22].

Generally, entanglement swapping has an extensive variety of potential applications in quantum information technology and era, from quantum teleportation and cryptography to quantum computing, metrology, and assessments of fundamental physics.

5. Conclusion

Entanglement swapping and BB84 are both QKD protocols that enable two parties to securely exchange cryptographic keys over an insecure communication channel. While BB84 is a well-established and widely used protocol, entanglement swapping is a more recent development that promises some advantages over BB84. One of the main advantages of entanglement swapping is that it can generate longer secret keys with higher rates of efficiency. This is because entanglement swapping can use pre-shared entangled pairs of qubits, which can be created and distributed beforehand, instead of randomly generated qubits that are used in BB84. Moreover, entanglement swapping is immune to certain types of attacks, such as the intercept-resend(Eve intercepts every photon intended for Bob, randomly select a basis to measure in, and she receives an end result, and sends an identical photon to Bob. Eve's measurement collapses the superposition of the $|\Psi\rangle$ state and ruins her attack), which can potentially compromise the security of BB84. However, entanglement swapping requires a more complex setup and longer measurement times than BB84, which can make it more difficult to implement in practice. Here we compare entanglement swapping with BB84 protocol in terms of their speed and security for QKD:

Speed: Entanglement swapping can transmit entanglement over long distances, but it requires the manipulation of four qubits, which can slow down the process. | The BB84 protocol is faster than the E91 protocol as it does not require the same level of entanglement purification. It is a relatively fast QKD method.

Security: Entanglement swapping is a secure means of transmitting quantum information as it is based on the principles of quantum mechanics, ensuring that any eavesdropping will be detected. The distribution of entangled pairs enables secure key exchange. The BB84 protocol is highly secure as it relies on the uncertainty principle of quantum mechanics to encode and transmit quantum information. It is less susceptible to eavesdropping and provides a high level of security for QKD.

Efficiency: The entanglement swapping protocol requires the manipulation of four qubits, which can limit its efficiency compared to other QKD methods. The BB84 protocol is more efficient as it allows for the transfer of multiple bits of information per photon, which allows for faster key generation.

In summary, both entanglement swapping and BB84 protocol provide secure means for QKD, while entanglement swapping may offer some advantages over BB84 in terms of efficiency and security, the practicality of implementing it may depend on the specific application and resources available.

In the absence of a direct communication channel between Alice and Bob, we leveraged this lack to prevent Eve from intercepting the communication, noting that Eve does not possess any entangled pair with either of them. In scenarios where more users are involved, the deployment of a key distribution center (KDC) could enable us to create a quantum key in a network. As with any method, this approach has both advantages and disadvantages, but before examining these, it is essential to ascertain whether we have created a secure communication path.

It is widely recognized that the Eckert protocol, which relies on quantum entanglement, has been employed in each of the aforementioned steps, thus ensuring the security of the process. However, during the final stages when the Key Distribution Center (KDC) communicates with both Alice and Bob and shares the entangled particles, Eve may potentially intercept the information through the classical channel. Nevertheless, any information she may obtain would be irrelevant without the complementary entangled particle, thereby eliminating any cause for concern regarding a security breach at this stage, and even for the network, with more users. A notable benefit of this approach is that the KDC eliminates the requirement for various sources, and user authentication can be accomplished exclusively through the KDC. Additionally, the utilization of star topology and the creation of multiple channels can be avoided, allowing cost savings by having only a single channel between each user and the KDC. Nevertheless, this method can be problematic in the event of KDC failure, as communication between users becomes impossible.

Acknowledgement

This work was supported by the Alzahra university, Iran. The content of this documentation reflects the views only of their authors. The Alzahra university are not responsible for any use that may be made of the information it contains.

Appendix A

In order to better understand the concept of entanglement swapping and for simplicity, two similar states are initially considered. Entanglement swapping, at this step, can be shown with an example. By considering equations 5 and 6,

$|\Phi\rangle^{\pm}_{\alpha1\beta1} \otimes |\Phi\rangle^{\pm}_{\alpha2\beta2} = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)_{\alpha1\beta1} \otimes \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)_{\alpha2\beta2} = \frac{1}{2}(|0000\rangle \pm |0011\rangle \pm |1100\rangle + |1111\rangle)_{\alpha1\beta1\alpha2\beta2}$

(7) $S_1(|\Phi\rangle^{\pm}_{\alpha1\beta1}\,|\Phi\rangle^{\pm}_{\alpha2\beta2}) = \frac{1}{2}(|0000\rangle \pm |0101\rangle \pm |1010\rangle + |1111\rangle)_{\alpha1\alpha2\beta1\beta2} = \frac{1}{2}(|00\rangle_{\alpha1\alpha2}\,|00\rangle_{\beta1\beta2} \pm |01\rangle_{\alpha1\alpha2}\,|01\rangle_{\beta1\beta2} \pm |10\rangle_{\alpha1\alpha2}|10\rangle_{\beta1\beta2} + |11\rangle_{\alpha1\alpha2}|11\rangle_{\beta1\beta2})$.

Where α_1, β_1 are entangled particles which hold by Alice, and α_2, β_2 are entangled particles which are in Bob's side. The mathematical basis for entanglement swapping is the idea of "entanglement swapping operators", which describe the transformation of two qubits from an unentangled state to an entangled state. These operators have been used to predict and analyze the results of entanglement swapping experiments. We called this operator S_1 in the above equation.

In what follows, we consider two different Bell states

$|\Phi\rangle^{\pm}_{\alpha1\beta1} \otimes |\Psi\rangle^{\pm}_{\alpha2\beta2} = (|00\rangle \pm |11\rangle)_{\alpha1\beta1} \otimes (|01\rangle \pm |10\rangle)_{\alpha2\beta2} = (|0001\rangle \pm |0010\rangle \pm |1101\rangle + |1110\rangle)_{\alpha1\beta1\alpha2\beta2}$

(8) $S_1(|\Phi\rangle^{\pm}_{\alpha1\beta1} \otimes |\Psi\rangle^{\pm}_{\alpha2\beta2}) = (|0001\rangle \pm |0100\rangle \pm |1011\rangle + |1110\rangle)_{\alpha1\alpha2\beta1\beta2} = (|00\rangle\alpha1\alpha2\,|01\rangle\beta1\beta2 \pm |01\rangle\alpha1\alpha2\,|00\rangle\beta1\beta2 \pm |10\rangle\alpha_{1\alpha2}\,|11\rangle\beta_{1\beta2} + |11\rangle\alpha_{1\alpha2}\,|10\rangle\beta_{1\beta2})$.

By changing the state place in equation, we'll have

$|\Psi\rangle^{\pm}_{\alpha1\beta1} \otimes |\Phi\rangle^{\pm}_{\alpha2\beta2} = (|01\rangle \pm |10\rangle)_{\alpha1\beta1} \otimes (|00\rangle \pm |11\rangle)_{\alpha2\beta2} = (|0100\rangle \pm |0111\rangle \pm |1000\rangle + |1011\rangle)_{\alpha1\beta1\alpha2\beta2}$

(9) $S_1(|\Psi\rangle^{\pm}_{\alpha1\beta1} \otimes |\Phi\rangle^{\pm}_{\alpha2\beta2}) = (|0010\rangle \pm |0111\rangle \pm |1000\rangle + |1101\rangle)_{\alpha1\alpha2\beta1\beta2} = (|00\rangle_{\alpha1\alpha2}\,|10\rangle_{\beta1\beta2} \pm |01\rangle_{\alpha1\alpha2}|11\rangle_{\beta1\beta2} \pm |10\rangle_{\alpha1\alpha2}\,|00\rangle_{\beta1\beta2} + |11\rangle_{\alpha1\alpha2}\,|01\rangle_{\beta1\beta2})$,

And finally

$|\Psi\rangle^{\pm}_{\alpha1\beta1} \otimes |\Psi\rangle^{\pm}_{\alpha2\beta2} = (|01\rangle \pm |10\rangle)_{\alpha1\beta1} \otimes (|01\rangle \pm |10\rangle)_{\alpha2\beta2} = (|0101\rangle \pm |0110\rangle \pm |1001\rangle + |1010\rangle)_{\alpha1\beta1\alpha2\beta2}$

(10) $S_1(|\Psi\rangle^{\pm}_{\alpha1\beta1} \otimes |\Psi\rangle^{\pm}_{\alpha2\beta2}) = (|0011\rangle \pm |0110\rangle \pm |1001\rangle + |1100\rangle)_{\alpha1\alpha2\beta1\beta2} = (|00\rangle_{\alpha1\alpha2}\,|11\rangle_{\beta1\beta2} \pm |01\rangle_{\alpha1\alpha2}\,|10\rangle_{\beta1\beta2} \pm |10\rangle_{\alpha1\alpha2}\,|01\rangle_{\beta1\beta2} + |11\rangle_{\alpha1\alpha2}\,|00\rangle_{\beta1\beta2})$.

And one can easily see that for having entangement swapping in 2-levels systems, the initial Bell states in both 2 parties should be the same. For more than 2 entangled state, we have the GHZ state[11], which is a maximally entangled quantum state for 3-particles and it can be shown as:

(11) $|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$

The generalized GHZ state is an entangled state for more than 2 subsystems, and when each of this subsystems being two dimensional, for n qubits, one can write:

(12) $|GHZ\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} + |1\rangle^{\otimes n})$

References

1. C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175, page 8. New York, 1984.
2. A. K. Ekert, Phys. Rev. Lett. 67, 661 (1991).
3. W. K. Wootters and W. H. Zurek, Nature (London) 299 ,802 (1982).
4. R. Horodecki, P. Horodecki, M. Horodecki, K. Horodecki, Quantum entanglement, Rev. Mod. Phys.81, 865 (2009).
5. Einstein, A. and Podolsky, B. and Rosen, N"Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?", Phys.rev.47, 777-780 (1935).
6. M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, 10th Anniversary edition published 2010, Vol. 1 (Cambridge university press, 2000).
7. S. Barnett, Quantum information, Vol. 16 (Oxford University Press, 2009).
8. J.S.Bell, "ON THE EINSTEIN PODOLSKY ROSEN PARADOX", Physics Vol. 1, No. 3, pp. 195-290, (1964).
9. P.-X. Chen, S.-Y. Zhu, and G.-C. Guo, General form of genuine multipartite entanglement quantum channels for teleportation, Phys. Rev. A 74, 032324 (2006).
10. S. L. Braunstein, A. Mann, and M. Revzen, Phys. Rev.Lett. 68 , 3259 (1992).
11. Daniel M. Greenberger; Michael A. Horne; Anton Zeilinger (2007), Going beyond Bell's Theorem, arXiv:0712.0921
12. M. Zukowski, A.Zeilinger, M. A.Horne, and A.K.Ekert, "Event-Ready-Detectors" Bell Experiment via Entanglement Swapping, Physical Review Letters, Vol.71, 1993.
13. J. M. Torres, J. Z. Bernad, G. Alber, Quantum teleportation and entanglement swapping of matter qubits with coherent multiphoton states, Phys.Rev.A Vol.90 012304 (2014).
14. K Shannon, E Towe, and O Tonguz, On the Use of Quantum Entanglement in Secure Communications: A Survey, Book,(2020).
15. R. M. Needham and M. D. Schroeder, Using Encryption for Authentication in Large Networks of Computers, Communications of the ACM, vol. 21, pp. 993-999, 1978.

16. Carlo Blundo and Paolo D'Arco, Analysis and Design of Distributed Key Distribution Centers, Journal of Cryptography 18:391-414, 2005.
17. C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. 70, 1895 (1993).
18. S. Bose, V. Vedral, and P. L. Knight, Phys. Rev. A 57,822 (1998).
19. Jian-Wei Pan, Dik Bouwmeester, Harald Weinfurter, and Anton Zeilinger, Phys. Rev. Lett. 80, (1998).
20. Kang Min-Sung, Heo Jino, Hong Chang-Ho, Yang Hyungjin, Moon Sung, Sang-Wook, Response to "Comment on Controlled mutual quantum entity authentication with an untrusted third party", Journal of "Quantum Information Processing" Vol.19, (2020).
21. Daniel Gottesman, Isaac L. Chuang, "Quantum Teleportation is a Universal Computational Primitive", Nature 402, 390-393 (1999).
22. Rodney Van Meter, Takahiko Satoh, Thaddeus D. Ladd, William J. Munro, Kae Nemoto, "Path Selection for Quantum Repeater Networks", Networking Science, Volume 3, Issue 1-4, pp 82-95, (December 2013).