Journal of Engineering and Applied Sciences 13 (22): 9784-9788, 2018
ISSN: 1816-949X

Multi-Party Quantum Key Distribution (QKD) without Entanglement

Salah Albermany Iqtidar Zohair
Faculty of Mathematics and Computer Science, University of Kufa, Kufa, Iraq

Abstract: Quantum Key Distribution (QKD) is a technique used to generate a secret shared key randomly between two or more parties. It depends on the quantum coding in preventing eavesdroppers from acquiring any information and due to the rapid development of internet services both free space and internet can be exploited as channels to transfer the data. In this study, a secret shared key has been generated which can be used in any other encryption and decryption method.

Key words: QKD, secret key, BB84, quantum cryptography, randomly, development

INTRODUCTION

Cryptography is the technique of exchanging confidential information secretly using physical or mathematical mean (Shenoy-Hejamadi *et al*., 2017).

Furthermore, cryptography studies the methods of sending and receiving messages secretly. The process of transferring message into some encoded form is called encryption. Converting plain text to cipher text requires the use of a key known as an encryption key and the procedure of transforming the encrypted message back into the original one is called decryption. The encryption key plays a reasonably important role in cryptography and depending on the type of the key used, the cryptographic algorithms can be classified (Kute and Desai, 2017).

In classical cryptography, two persons communicate using either symmetric or asymmetric key cryptography. In symmetric key cryptography, both encryption and decryption use the same key also known as the secret key cryptosystem while in asymmetric key cryptography also called public key cryptography, two pairs of keys are used. The first key is a private key which is kept secret and a public key which is freely available to the public (Al-Juboori and Al-Mandilawi, 2013).

The secure communication link has widely been used and becomes the most important method in our modern days (Sarath *et al*., 2012) and with the increased number of email and internet users, we note that they sometimes transmit important information over the network on which it would be easy for the hackers to eavesdrop (Ranganathan *et al*., 2010). Despite encrypting this information using classical cryptography it remains vulnerable. Modern cryptography is influenced by both technological progress in the power of the computer and evolution in mathematics to quickly inverse one-way functions for instance that of factoring large integers (Zhao *et al*., 2008). To solve this problem and make the transmission of information between two or more persons more secure it is crucial to use quantum cryptography which is eliminated owing to that the information photons are destroyed during hacking. The most well-known topic of quantum cryptography is Quantum Key Distribution (QKD) which is a vital and fruitful area of research for modern cryptography (Goldreich, 1998).

The physics of elementary particles is judged by laws of quantum mechanics, discovered at the beginning of the twentieth century by gifted physicists. Quantum mechanics have changed the way that we see our world in. Both position and momentum of a particle cannot be measured accurately. The more precisely one of these values can be known, the less precisely the other can. This theorem is called the "uncertainty principle" (Paterson *et al*., 2004). Quantum mechanics comprise two principles (Qaisar *et al*., 2016).

No cloning theorem states which means that no one is able to create a copy of an unknown state of quantum.

The principle of photon polarisation describes how the photons can be polarised in such a way that prevents an eavesdropper from measuring the quantum state (Al-Juboori and Al-Mandilawi, 2013).

The uncertainty principle invented by Heisenberg suggests that no one can accurately measure the position and momentum of a particle simultaneously. When special information is encoded into the properties of a photon, any attempt to monitor it would change its properties and will be detectable (Mogos and Radu, 2015).

Literature review

Previous work in quantum domain: Wiesner (1983) was the first one who used quantum information in cryptography (Bhatt *et al*., 1956) when he submitted his paper "conjugate coding" also called [Wie83] and quantum coding (Shor and Preskill, 2000).

The principle of conjugate coding associates a qubit with a photon and uses a photon polarisation. Photon can be polarised horizontally ($|\_\_\rangle$) or vertically ($|\rangle$),

diagonally to the right (|/⟩) or diagonally to the left (|\⟩). These four bases are called (Rectilinear (R) and Diagonal (D), respectively) where, |||⟩ = |1⟩, |___⟩ = |0⟩, |/⟩:

$$|/\rangle = \frac{1}{\sqrt{2}}((0(-(1()$$

and

$$|\backslash\rangle = \frac{1}{\sqrt{2}}((0(+(1()$$

Wiesner (1983) proposed that quantum information could be used to originate non-forgeable banknotes. Banknotes in Wiesner's idea should consist of a sequence of single qubits that are randomly chosen from the above state (R, D). Therefore, genuine banknotes could be identified, hence, preventing any possibility of counterfeiting (Diep, 2017). The method of Wiesner can be illustrated in Table 1 by taking a sequence of bits (001011000) for instance.

Quantum cryptography: Quantum cryptography is the science and art of using the quantum mechanical effect to perform cryptographic tasks (Brassard, 2005).

It offers skilfully secure data transmission because it depends on the laws of physics which we believe to be true. Quantum cryptography is only used in solving key distribution problem by transmitting photon light through fiber optics or free space (Kaur *et al*., 2011).

Because of the two principles mentioned in section 1, quantum cryptography aims to prevent eavesdroppers from decoding the value of key bits when they try to measure the polarisation of a photon (Al-Juboori and Al-Mandilawi, 2013). Even though this does not prevent eavesdropping it will be detectable by the communicating parties. Should any of the parties detected an eavesdropper they could then neglect the current key without losing anything noteworthy as it was randomly generated key (Kaur *et al*., 2011). Thus, the most important application of quantum cryptography is Quantum Key Distribution (QKD). It is used to produce and distribute a key and not transmit any message data. After the key is introduced it can be used with any chosen encryption algorithm (Pratap *et al*., 2016). QKD is unconditionally secure, i.e., it is secure even with an unlimited computational power eavesdropper (Paterson *et al*., 2004). The most famous QKD protocol is a BB84 protocol that was proposed in 1984 (Qaisar *et al*., 2016).

Table 1: Example of conjugate coding for sequence of bits (001011000)

Encoding bits	Basis choice	Quantum encoding
0	R	||⟩
0	D	|/⟩
1	D	|\⟩
0	D	|/⟩
1	R	|-⟩
1	R	|-⟩
0	D	|/⟩
0	R	||⟩
0	R	||⟩

MATERIALS AND METHODS

BB84 protocol: The first protocol of quantum cryptography was proposed in 1984 by H. Bennet and Gilles Barssard. They started from Wiesner (1983) work "Conjugate Coding" and then developed this research to key distribution protocol using photon's polarisation (Mogos and Radu, 2015). The polarisation states represent both orthogonal bases for linear polarisation (+) and diagonal bases for diagonal polarisation (×). They use the following notation in which (___) denotes photon in a vertically polarised state or 0°, (|) denotes a photon in horizontal polarised state or 90°, (/) denotes a photon in 45° polarised state and (\) denotes a photon in 135° polarised state. The 0 value is represented by 0° and 45° and 1 value is represented by 90° and 135° (Bhatt *et al*., 1956) (Fig. 1).

In this protocol, the two participants, traditionally called Alice and Bob wish to agree on a secret key with which no eavesdropper, traditionally called Eve can obtain significant information (Shor and Preskill, 2000). Alice generates a random sequence of bits and sends it with different polarisation bases to Bob. When Bob receives this sequence, he would randomly choose the state of each bit and only the bit that is similar to Alice bases will be used as the secret key, hence, disregarding other bits. Exchanging the sequence of bits between Alice and Bob is done via. a quantum channel whereas comparing the bits between them is done by public channel (Table 2).

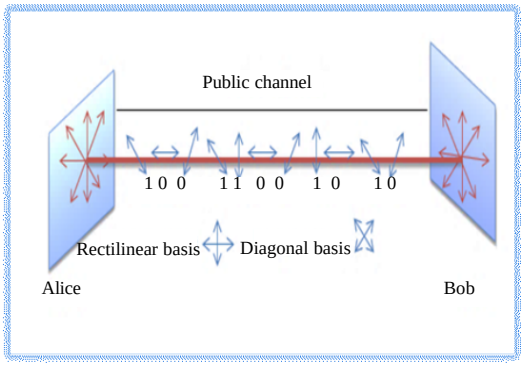

Fig. 1: Rectilinear and diagonal bases

Table 2: Polarisation state of quantum bits

State	Bases	Values	Polarisation angle
| 0>	+	0	0°
| 1>	+	1	90°
| 0>+| 1>	×	0	45°
| 0>-| 1>	×	1	135

RESULTS AND DISCUSSION

Multiparty quantum key distribution: Multiparty QKD means that Alice sends the same key to n-1 users (Diep, 2017). More than one researcher supposed that the three parties could communicate with each other (Matsumoto, 2007; Gao *et al*., 2011; Alshowkan *et al*., 2013). By Alshowkan *et al*. (2013) the researcher proposed three-party, Alice and Bob want to communicate with each other with a quantum key distribution centre and once they agree (through a classical channel) on the bases that are sent by QKD (through the quantum channel) to both of Alice and Bob, the parties can form a secret key. The process relies upon the key size and the required level of accuracy which can determine the number of rounds needed to obtain the required length of the key. They supposed three probabilities as illustrated.

First, probability when both parties have the same bases and correct value in n round. Second, probability when they use the wrong bases but the result is the correct value. Third, when both receivers get a wrong bases and wrong value.

From these three probabilities and using the value of accuracy 99% they calculated the number of rounds n required as equation when the length of the key is m:

$$n = -\log 2\left(1-(0.99)^{\frac{1}{m}}\right)-2 \quad (1)$$

From Eq. 1, they could use the number of rounds that determined the times of repetition of sending the sequence until they get the key length they desire.

Three-party quantum key distribution protocol: Suppose that we have three parties: centre server, Alice and Bob. They want to communicate using quantum channel (e.g., free space or fiber optic) and public or classical channel (e.g., internet). Center server will send the sequence of bits with the sequence of its polarisation that will form the qubit to both Alice and Bob through the quantum channel. When Alice and Bob receive the sequence, they will attempt to measure the qubit state by estimating the polarisation chosen by the center server and obtain the bits. After that, the center server will communicate with either party through the public channel and compare the state of polarisation that they used and the bits that they get (Fig. 2).

Table 3: Polarisation state of quantum bits that we used

State	Bases	Values	Polarisation angle	The state corresponding to each of polarising state that we used
| 0>	+	0	0°	0
| 1>	+	1	90°	1
| 0> + | 1>	×	0	45°	2
| 0> - | 1>	×	1	135°	3

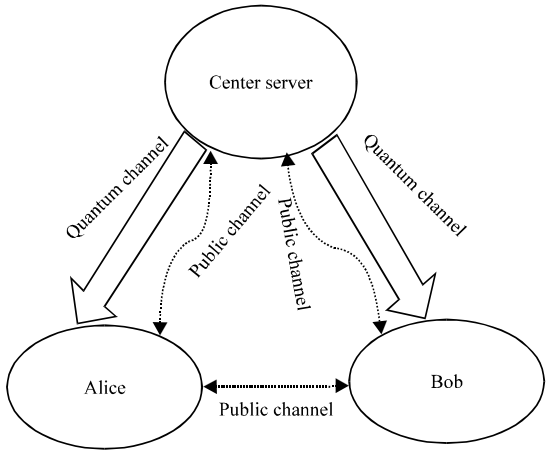

Fig. 2: Three parties communicate

The common state among these three parties will be used as a secret shared key and the rest bits will be neglected in order to get the required secret key with less disregarded bits returned to the center server by both Alice and Bob. The center server will re-polarise the bits in order to generate a new sequence of qubits and re-send that new sequence to other parties you can see the way that we used for polarisation in Table 3. In our case can use one of these two methods:

First method: By calculating the number of rounds using Eq. 1 by Alshowkan *et al*. (2013). And to do this, we need to divide this equation by two to reduce the number of disregarded bits.

Second method: In another way, the center server can choose randomly many numbers of lengths and calculate the average in order to determine an appropriate sequence length with less number of lost qubits using in Eq. 2:

$$б = \sum_{i=1}^{n} \frac{n}{i} \quad (2)$$

Where:

n = The vector of the i element and each represents length that chooses randomly

б = The mean get it

Center server will choose in random the vector n by determine the beginning and ending of this vector with the two simple equation as:

$$1 = 2r \quad (3)$$

$$n = 8*r/2+2r \quad (4)$$

Algorithm 1; Multi-party QKD:

Input: a sequence of the qubit
Output: a secret shared key
Step 1: Centre server will choose a random number of sequence bits length

$$6 = \sum_{i=1}^{n} \frac{n}{i}$$

Step 2: Centre server chooses at random both bits and the bases of each photon and sends the photon to other parties, namely Alice and Bob by a quantum channel. The polarisation of the photon is either rectilinear horizontal (—) or vertical (|) or diagonal (/ or \). Centre server polarisation will be represented in 4 directions (0 = 0, 90 = 1, 45 = 2, 135 = 3), respectively
Step 3: Alice receives the sequence of photons and determines the polarisation of each photon randomly and then determines her basis depending on her polarisation
a- if polaris_Alice equals zero or 2 then basis_Alice ←0
b- else if polarise_Alice equals 1 or 3 then basis_Alice ←1
Step 4: Bob doing the same in step 3
a - if polaris_Bob equals zero or 2 then bases_Bob ←0
b - else if polarise_Bob equals 1 or 3 then bases_Bob ←1
Step 5: The center server will be connected with two other parties (Alice and Bob) by the public channel to check the polarisation of the photon and the bases that they determine
Step 6: If the qubits are equal in all three parties
a secret shared key←centre server-basis
Shard key bit Shard key bit +1
Step 7: Discard all the qubits that are not equal in all three parties
Discard-sequence-bit = centre server-basis
Step 8: If not get the required key, return the disregarded-sequence-bit to the centre server then, Go to step 2

CONCLUSION

A protocol multi-party quantum key distribution is a method that is used to generate a key. By increasing QKD algorithm steps through return the sending, the length of the shared key will increase. Accordingly, this protocol can provide the ability of authentication and transfer data more securely.

REFERENCES

Al-Juboori, F.A.S. and N.K.J.A. Al-Mandilawi, 2013. Increasing the protocol gain of quantum cryptography. Eng. Technol. J., 31: 2680-2691.

Alshowkan, M., K. Elleithy, A. Odeh and E. Abdelfattah, 2013. A new algorithm for three-party quantum key distribution. Proceedings of the 3rd International Conference on Innovative Computing Technology (INTECH), August 29-31, 2013, IEEE, London, UK., ISBN:978-1-4799-0047-3, pp: 208-212.

Bhatt, M., A. Aneja and S. Tripathi, 1956. Classical cryptography v/s quantum cryptography a comparative study. Intl. J. Electron. Comput. Sci. Eng., 1: 121-129.

Brassard, G., 2005. Brief history of quantum cryptography: A personal perspective. Proceedings of the IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, October 16-19, 2005, IEEE, Awaji Island, Japan, pp: 19-23.

Diep, D.N., 2017. Multiparty quantum telecommunication using quantum fourier transforms. J. Telecom. Mange., 1: 1-11.

Gao, F., S.J. Qin, F.Z. Guo and Q.Y. Wen, 2011. Dense-coding attack on three-party quantum key distribution protocols. IEEE J. Quantum Electron., 47: 630-635.

Goldreich, O., 1998. Secure multi-party computation. MCS Thesis, Weizmann Institute of Science, Rehovot, Israel.

Kaur, N., A. Singh and S. Singh, 2011. Enhancement of network security techniques using quantum cryptography. Intl. J. Comput. Sci. Eng., 3: 1960-1964.

Kute, S.S. and C.G. Desai, 2017. Quantum cryptography: A review. Indian J. Sci. Technol., 10: 1-5.

Matsumoto, R., 2007. Multiparty quantum-key-distribution protocol without use of entanglement. Phys. Rev. A., 76: 1-8.

Mogos, G. and G. Radu, 2015. QKD protocols-software implementation bennet-brassard vs. Bruss. Rev. Air Force Acade., 1: 81-84.

Paterson, G., F. Piper and R. Schack, 2004. Why quantum cryptography? Quantum physics, quant ph/0406147. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.74.1170&rep=rep1&type=pdf.

Pratap, M.S., D. Nair, P. Narayanan, N. Kamar and C. V Aneesa, 2016. Three party authentication using quantum key distribution protocol. Proceedings of the 1st International CSE, RRCE Conference on Innovations in Computing & Networking (ICICN16), May 12-13, 2016, Rajarajeswari College of Engineering, Bengaluru, India, pp: 74-77.

Qaisar, S., J. Ur Rehman, Y. Jeong and H. Shin, 2016. [Distributed multiparty quantum key distribution]. Proc. Korean Inst. Commun. Sci. Conference, 11: 585-586 (In Korean).

Ranganathan, S., N. Ramasamy, S.K.K. Arumugam, B. Dhanasekaran and P. Ramalingam *et al*., 2010. A three party authentication for key distributed protocol using classical and quantum cryptography. Intl. J. Comput. Sci. Issues, 7: 1-148.

Sarath, R., A.S. Nargunam and R.P. Sumithra, 2012. Dual channel authentication in cryptography using quantum stratagem. Proceedings of the 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET), March 21-22, 2012, IEEE, Kumaracoil, India, ISBN:978-1-4673-0211-1, pp: 1044-1048.

Shenoy-Hejamadi, A., A. Pathak and R. Srikanth, 2017. Quantum cryptography: Key distribution and beyond. Quanta, 6: 1-47.

Shor, P.W. and J. Preskill, 2000. Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett., 2: 441-444.

Wiesner, S., 1983. Conjugate coding. ACM SIGACT News, 15: 78-88.

Zhao, Y., B. Qi and H.K. Lo, 2008. Quantum key distribution with an unknown and untrusted source. Phys. Rev. A., 77: 1-31.