International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 03 | June-2015 www.irjet.net p-ISSN: 2395-0072

Architecture of Multicast Network Based on Quantum Secret Sharing and Measurement

Ahmed F. Metwaly[1], M. Z. Rashad [2], Fatma A. Omara[3] , Adel A. Megahed [4]

1 Senior lecturer, Information Technology Department, AL-Zahra College for women, Oman
2 Professor of Computer Sciences , Faculty of Computer and Information Sciences, Mansoura University, Egypt
3 Professor of Computer Sciences, Faculty of Computer and Information Sciences , Cairo University, Egypt
4 Professor of Engineering Mechanics, Faculty of Engineering, Cairo University, Egypt

---

Abstract - *Multicast Classical transmission means that the channels and transmitted messages are both classical. This type of transmission deteriorate from many difficulties, the most important is network cryptography problems. For solving multicast classical* ***network cryptography problems', the quantum*** *approach has been investigated but Quantum approach requires additional resources to work in an effective way. In this paper, Generation and measuring shared entangled pair keys between the communicated peers in a multicast network is achieved by Quantum Multicast shared distribution and measurement centre "* QM_{SDM} *" and quantum gates. Encoding of transmitted quantum messages is handled by the basis of quantum teleportation. Teleportation or encoding at sender side will be accomplished by* C_{NOT} *and a* $Hadamard$ *gates. Decoding the teleported message is achieved by performing the correction action on received entangled pair. On the receiver side decoding will be accomplished by* X *and* Z *gates. If two members within the same multicast group need to communicate, they can by using entangled shared key pair. If two members in a different groups need to communicate, they can by complete or partial support of* QM_{SDM}*. By full support of* QM_{SDM} *the responsibility of* QM_{SDM} *is decoding /encoding the teleported / original transmitted quantum message between the communicated members. Optical clock synchronization is used for improving the transmission of generated entangled keys as well key update.*

Key Words: Quantum Key Distribution, Teleportation, Measurement, Secret Sharing

1. Introduction

The pioneering work of Bennett and Brassard [2] has been developed for the purpose of quantum cryptography. Quantum cryptography is one of the most significant prospects associated with laws of quantum mechanics in order to ensure unconditional security [3, 4, 5, 6, 10]. The quantum cryptography proves unconditional security characteristic through no cloning theory [1] as the transmitted quantum bit can't be replicated or copied but its state can be teleported. The most used quantum principles are quantum teleportation and dense coding. In quantum teleportation the quantum information can be transmitted between distant parties based on both classical communication and maximally shared quantum entanglement among the distant parties [1, 2, 3, 4]. In Dense coding the classical information can be encoded and transmitted between distant parties based on both one quantum bit and maximally shared quantum entanglement among the distant parties as each quantum bit can transmit two classical bits [1,2]. There are number of approaches and prototypes for the exploitation of quantum principles' to secure the communication between two parties and multi-parties. While these approaches used different techniques for achieving a private communication among authorized users but still most of them depend on generation of a secret random keys. At present, there're two approaches of quantum private communication. One is a hybrid of classical cryptosystem and quantum key distribution. In this approach, the employed encoding and decoding algorithms come from classical. Whilst the generated keys for message encoding and decoding which act as significant role in the cryptosystem derives from a distinguished quantum key distribution scheme. The other approach applies a completely quantum cryptosystem with natural quantum physics laws. In this approach, the encoding and decoding algorithms are quantum one and the keys for message encoding and decoding derives from a distinguished quantum key distribution scheme. The quantum communication system can be described using the same way of classical model. The messages in quantum system represented by quantum state which can be pure or mixed [3, 4, 5, 6, 7]. The most three principal components for designing a quantum communication system are cryptosystem, authentication and key management system. All included processes in these components may be classical or quantum but in any case at minimum one of these components has to apply a quantum features and

laws [3, 4, 5, 6, 7]. Recently, quantum secure direct communication concept is introduced for transmitting the secured messages between the communicated participants without establishing secret keys to encode them [16, 17, 19, 20, 21, 22, 18, 23, 24, 25, 33, 34 , 35 , 36 ,37 , 38 , 39 , 40 , 41]. In [16] a ping pong protocol is introduced for directly decrypted the transmitted encoded bits between the communicated participants in every corresponding transmission without the need of QKD. In [40] enhances the capability of ping pong protocol by adding two more unitary operations. In [19] a two-step quantum secure direct communication is proposed for transferring of quantum information by utilizing EPR pair blocks for secure the transmission. In [8] the authentication and communication process performed using GHZ states. Firstly, GHZ states are used for authentication purpose then the remaining GHZ will be used for directly transmitting the secret message. In [31] architecture of centralized multicast scheme is proposed based on hybrid model of quantum key distribution and classical symmetric encryption. The proposed scheme solved the key generation and management problem using a single entity called centralized Quantum Multicast Key Distribution Centre. In [32] a novel multiparty concurrent quantum secure direct communication based on GHZ states and dense coding is introduced. In [11] a managed quantum secure direct communication protocol based on quantum encoding and incompletely entangled states. Different quantum authentication approaches have been developed for preventing various types of attack and especially man in the middle attack [26, 27, 28, 29, 30]. In this paper, Generation and measuring shared entangled pair keys between the communicated peers in a multicast network is achieved by Quantum Multicast shared distribution and measurement centre " QM_{SDM} " and quantum gates. Encoding of transmitted quantum messages is handled by the basis of quantum teleportation. Teleportation or encoding at sender side will be accomplished by C_{NOT} and a $Hadamard$ gates. Decoding the teleported message is achieved by performing the correction action on received entangled pair. On the receiver side decoding will be accomplished by X and Z gates. If two members within the same multicast group need to communicate, they can by using entangled shared key pair. If two members in a different groups need to communicate, they can by complete or partial support of QM_{SDM}. By full support of QM_{SDM} the responsibility of QM_{SDM} is decoding /encoding the teleported / original transmitted quantum message between the communicated members.

2. Quantum State and Entanglement

The classical bit is the fundamental element of information. It is used to represent information by computers. Nevertheless of its physical realization, a classical bit has two possible states, 0 and 1. It is recognized that the quantum state is a fundamental concept in quantum mechanics. Actually, the quantum bit is the same as the quantum state. The quantum bit can be represented and measured using two states $|0>$ and $|1>$ which well known as Dirac notation [5, 7]. In classical computer all information is expressed in terms of classical bit. Classical bit can be either 0 or 1 at any time. On the other hand quantum computer uses quantum bit rather than a bit. It can be in a state of 0 or 1, also there is usage of a form of linear combinations of state called superposition state. Quantum bit can take the properties of 0 and 1 simultaneously at any one moment.

Quantum bit definition is described as follow: Definition: A quantum bit, or qubit for short, is a 2 dimensional Hilbert space H_2. An orthonormal basis of H_2 is specified by $\{|0>,|1>\}$. The state of the qubit is an associated unit length vector in H_2. If a state is equal to a basis vector then we say it is a pure state. If a state is any other linear combination of the basis vectors we say it is a mixed state, or that the state is a superposition of $|0>$ and $|1>$ [8, 9]. In general, the state of a quantum bit is described by Eq. (1) Where $|\psi>$ is a quantum state, α and β are complex numbers:

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

The quantum bit can be measured in the traditional basis equal to the probability of effect for α^2 in $|0>$ direction and the probability of effect for β^2 in $|1>$ direction [18, 20] which α and β must be constrained by Eq. (2) and Figure.1

$$\alpha^2 + \beta^2 = 1 \quad (2)$$

As well a quantum message can be represented as quantum state in a 3-dimension Hilbert space H_3 (see Eq. (3, 4))

$$|\Psi>= \alpha|0> + \beta|1> + \gamma|2> \quad (3)$$

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1 \quad (4)$$

For a quantum system consists of multi-particle, the mixture system is equal to the tensor product of the physical elements of system state space. So, if we have two quantum states are denoted by Eq. (3, 4)

$$|\Psi_1> = \alpha_1|0> + \beta_1|1> \quad (5)$$

$$|\Psi_2> = \alpha_2|0> + \beta_2|1> \quad (6)$$

So the composite system can be written as

$$|\Psi> = |\Psi_1> \otimes |\Psi_2>$$

$$= \alpha_1\alpha_2|00> + \alpha_1\beta_1|01> + \beta_1\alpha_1|10> + \beta_1\beta_2|11> \quad (7)$$

If the decomposition of the multi-particle quantum system is unachievable, in this case the quantum system can be referred as entanglement state. The well-known two particles entanglement states are called Bell states. The Bell states are one of the main theories in quantum information processing which denote the entanglement concept [12, 13, 14, 18]. Bell states are certain extremely entangled quantum states of two particles denoted by EPR. As the two entangled particles will have interrelated physical characteristics even though they're disjointed by distance. Bell states are entitled in many applications but the most useful examples are quantum teleportation and dense coding [4, 5].

The four Bell states (EPR pairs) are defined by (Eq. (8))

$$|\Phi^{\pm}> = \frac{1}{\sqrt{2}}(|00> \pm |11>)$$

$$|\psi^{\pm}> = \frac{1}{\sqrt{2}}(|01> \pm |10>) \quad (8)$$

Bell states can be generated by utilizing the properties of both $Hadamard$ gate and $Controlled - NOT$ gate. The four possibilities of Bell states (EPR) according to the input bits. While the input bits are 00, 01, 10 and 11 then the generated EPR states given by (Eq. (9))

$$|\Phi^{+}> = \frac{1}{\sqrt{2}}(|00> + |11>),$$
$$|\psi^{+}> = \frac{1}{\sqrt{2}}(|01> + |10>),$$
$$|\Phi^{-}> = \frac{1}{\sqrt{2}}(|00> - |11>),$$
$$|\psi^{-}> = \frac{1}{\sqrt{2}}(|01> - |10>) \quad (9)$$

As well the well-known three particles entanglement state is called GHZ given by (Eq. (10))

$$|\Psi> = \frac{1}{\sqrt{2}}(|000> \pm |111>) \quad (10)$$

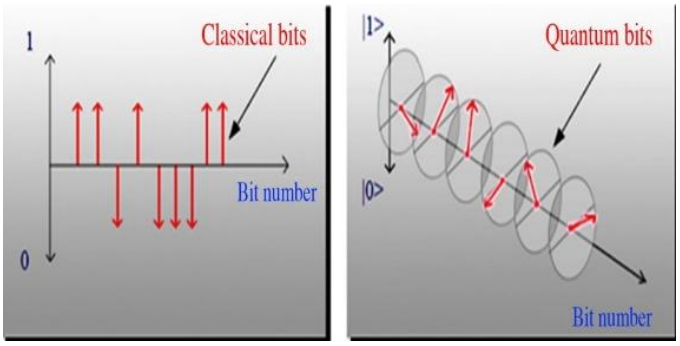


Figure 1 - Classical and Quantum Bits

3. Generate Shared Asymmetric Keys

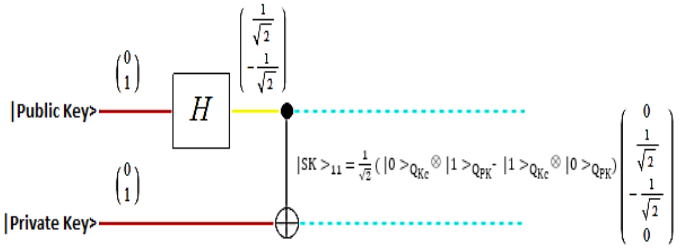
This process consists of the steps required for generating and distributing shared Asymmetric keys between two members. The process begins with generating public and private keys as string of $|0>$ and $|1>$ through QM_{SDM}. Therefore, the H circuit selects a single public key quantum bit from the upper input and generates a single quantum bit output. The C_{NOT} circuit operates public key as control input to affect the private key which is target quantum bit. If the public key is $|0>$ then the private key output is as same as private key input. If the public key is $|1>$ then the private key output is the private key input flip-flopped as shown in Fig. 2 and given by (Eq. (11)).

$$|S_k>_{00} = \frac{1}{\sqrt{2}}(|0>_{Q_{Kc}} \otimes |0>_{Q_{PK}} + |1>_{Q_{Kc}} \otimes |1>_{Q_{PK}})$$

$$|S_k>_{01} = \frac{1}{\sqrt{2}}(|0>_{Q_{Kc}} \otimes |1>_{Q_{PK}} + |1>_{Q_{Kc}} \otimes |0>_{Q_{PK}})$$

$$|S_k>_{10} = \frac{1}{\sqrt{2}}(|0>_{Q_{Kc}} \otimes |0>_{Q_{PK}} - |1>_{Q_{Kc}} \otimes |1>_{Q_{PK}})$$

$$|S_k>_{11} = \frac{1}{\sqrt{2}}(|0>_{Q_{Kc}} \otimes |1>_{Q_{PK}} - |1>_{Q_{Kc}} \otimes |0>_{Q_{PK}}) \quad (11)$$



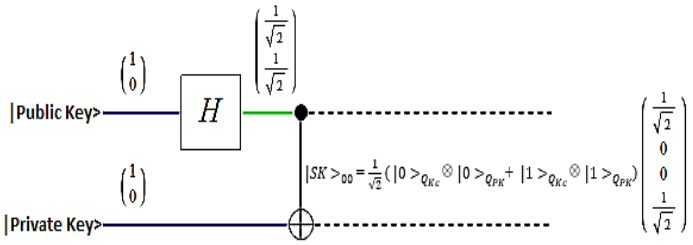


Figure 2 - Generate Shared Asymmetric Keys

4. Measuring Generate Shared Asymmetric Keys

This process consists of the steps required by Member 2 for measuring received generated Asymmetric keys. Measuring is achieved by performing C_{NOT} gate and a $\mathbf{H}$ gate receptively. Result of measuring is a couple of classical bits , so Member 2 can detect which one of the four bell states is used to generate Asymmetric keys. The really essential phase for quantum teleportation and dense coding is Bell measurement. The outcome of Bell measurement is a couple of classical bits, which can be used for retrieve the original state. Bell measurement is used in Communication Process for determining which unitary operation is used to transform the original classical message so the receiver can retrieve it as shown in Fig. 3

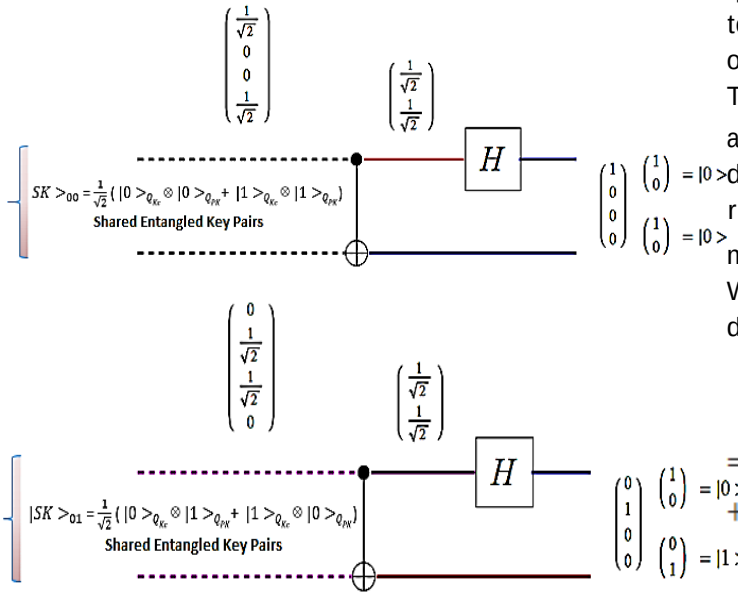


Figure 3 - Measuring Generated Shared Asymmetric Keys

5. Encoding and Decoding of Transmitted Quantum Messages by Partial Support

Teleportation approaches are not restricted to two-communicator teleportation, but also generalized to several communicators quantum teleportation. One of the most used multi-communicators quantum teleportation approaches is controlled teleportation (CT). In this approach, the sender shares previous entanglement with the receiver and as a minimum one trusted center (TC). Subsequently, if the sender succeeds for teleporting the unknown quantum state to both the receiver and trusted center, afterward only one of them can create a copy of the transmitted unknown quantum state with the support of the other. As a consequence, the transmitted information is fragmented between the sender and the trusted center, so both will cooperated together for retrieving the transmitted unknown state by the sender. Meanwhile, the trusted center control the whole teleportation process the protocol is denoted as controlled teleportation (CT).

In Fig.3 shows an illustrative example of perfect teleportation as $|\psi^+>=\frac{1}{\sqrt{2}}(|00>+|11>)$ *is used as a quantum channel of Asymmetric keys between sender and receiver. Currently, sender would like to transmit the unknown quantum state* $|\psi>=\alpha|0>+\beta|1>$ *to receiver. The unknown state will move through the teleportation circuit with a* $Controlled-NOT$ *gate and a* $Hadamard$ *gate.* Sender can encode the status of one quantum message bit to member 2 on the basis of quantum teleportation. Receiver can decode the teleported message by performing the correction action on his entangled pair. In our designed circuit, Teleportation or encoding at sender side will be accomplished by C_{NOT} and $\mathbf{H}$ gates. On the receiver side decoding will be accomplished by X and Z gates. The steps required for encoding and decoding the original quantum message Ψ_μ have be illustrated below in (Eq. (12, 13)). With the unknown state the initial state of the system is defined by (Eq. (12))

$$|\psi>_1=\alpha|0>+\beta|1>\otimes\frac{1}{\sqrt{2}}(|00>+|11>)$$
$$=\left(\alpha|0>\frac{1}{\sqrt{2}}(|00>+|11>)+\beta|1>\frac{1}{\sqrt{2}}(|00>+|11>)\right) \quad (12)$$

Subsequently the action of the $CNOT$ gate (using sender quantum bit as the control one and receiver quantum bit as the target one) the state becomes (Eq. (13))

$$|\psi>_2 = \left(\alpha|0> \frac{1}{\sqrt{2}}(|00>+|11>)+\beta|1> \frac{1}{\sqrt{2}}(|10>+|01>)\right) \quad (13)$$

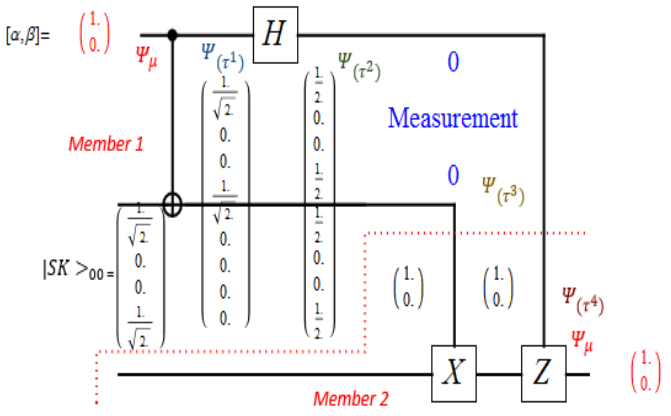
Since sender transmits the first quantum bit of the quantum state over the $Hadamard$ gate. So the state of overall system can be transformed as shown in (Eq. (14))

$$|\psi>_3 = \begin{pmatrix} \alpha\frac{(|0>+|1>)}{\sqrt{2}}\frac{1}{\sqrt{2}}(|00>+|11>) \\ +\beta\frac{(|0>-|1>)}{\sqrt{2}}\frac{1}{\sqrt{2}}(|10>+|01>) \end{pmatrix}$$

$$= \frac{1}{2}\begin{pmatrix} |00>(\alpha|0>+\beta|1>)+|01>(\alpha|1>+\beta|0>) \\ +|10>(\alpha|0>-\beta|1>)+|11>(\alpha|1>-\beta|0>) \end{pmatrix} \quad (14)$$

Table 1 - Relationship between Sender Measurement and Receiver's Operation

Sender Measurement	*Status of Receiver's Quantum Bit*	*Receiver's Operation*	*Status of Receiver Quantum Bit after Pauli Operation*
00	$\alpha\|0>+\beta\|1>$	I	$\alpha\|0>+\beta\|1>$
01	$\alpha\|1>+\beta\|0>$	X	$\alpha\|1>+\beta\|0>$
10	$\alpha\|0>-\beta\|1>$	Z	$\alpha\|0>-\beta\|1>$
11	$\alpha\|1>-\beta\|0>$	$ZX = iY$	$\alpha\|1>-\beta\|0>$



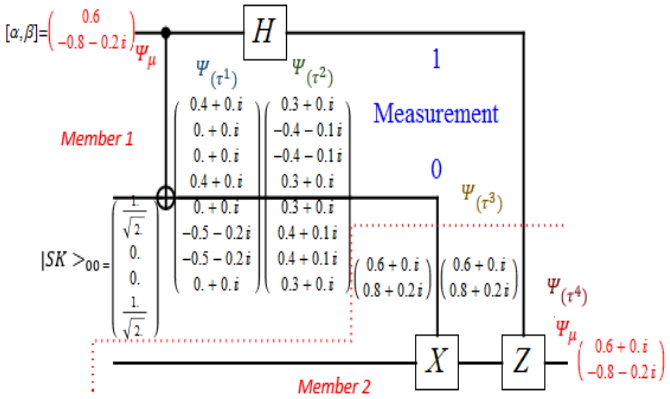


Figure 4 - Encoding and Decoding of Transmitted Quantum Messages by Partial Support

Afterward, sender computes the first two quantum bits and publish the result of his measurement through the classical channel. When receiver receives the two classical bits, he will conclude which unitary operation should be applied for restructuring the transmitted original unknown quantum state sent by sender as shown in Table.1

6. Encoding and Decoding of Transmitted Quantum Messages by Full Support

This procedure describes the required steps for a secured communication of two members in a different groups by complete support of QM_{SDA} . The responsibility of QM_{SDA} is divided into two process. The first process is decoding of received teleported messages from member 1 which located in group 1, so now QM_{SDA} retrieves the original message. The second process, QM_{SDA} is encoding the original message and send it to member 2 which is located in group 2. Now, member 2 in group 2 retrieves the original message which was sent by member 1 in group 1 by performing the correct action. The required steps are shown in Figs. 5, 6 respectively.

The protocol is then as follows:

Process 1

1) An Entangled shared key pair is generated, a separate quantum bit transmitted to member 1 and other to QM_{SDA}
2) At Member 1, measuring the Asymmetric key quantum bit and quantum message Ψ_μ by performing a C_{NOT} gate and thenceforth with a $Hadamard$ gate which resulting one of four possibilities, which can be encoded in two

classical bits of information (00, 01, 10, and 11). Member 1 removes both quantum bits.

3) Member 1 transmits the resulted two classical bits to QM_{SDA} through a classical channel
4) Based on received classical bits, QM_{SDA} can perform the correct action on his entangled pair with X and Z operations. So, the result is a quantum bit identical to the message Ψ_μ which was chosen to be teleported.

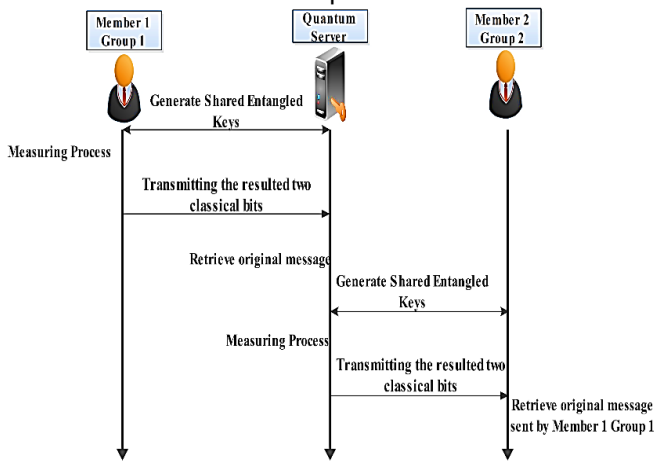


Figure 5 - Encoding and Decoding of Transmitted Quantum Messages by Full Support

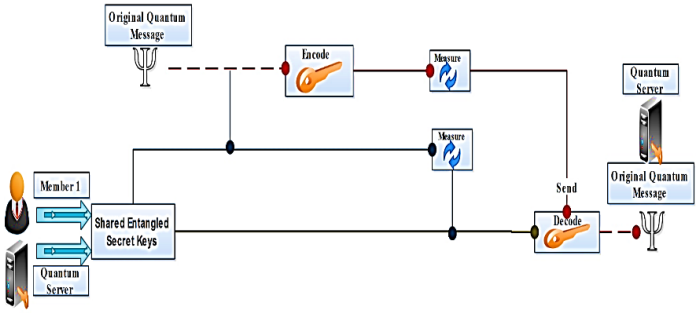


Figure 6 - Full Support Process 1

Process 2

1) The input is the retrieved quantum message Ψ_μ from process 1. An Entangled shared key pair is generated , a separate quantum bit transmitted to QM_{SDA} and other to member 2
2) At QM_{SDA}, measuring the Entangled shared key quantum bit and quantum message Ψ_μ by performing a $CNOT$ gate and thenceforth with a $Hadamard$ gate which resulting one of four possibilities, which can be encoded in two classical bits of information (00, 01, 10, and 11). QM_{SDA} removes both quantum bits.
3) QM_{SDA} transmits the resulted two classical bits to member 2 through a classical channel
4) Based on received classical bits, member 2 can perform the correct action on his entangled pair with X and Z operations. So, member 2 retrieves the original quantum message Ψ_μ which was chosen to be teleported by member 1

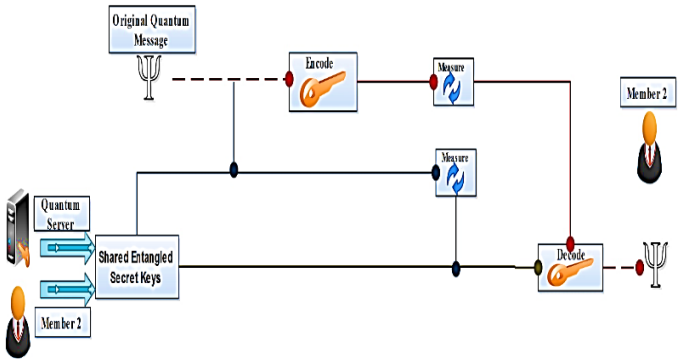


Figure 7 - Full Support Process 2

Truth Table for measuring received generated Asymmetric keys. Measuring is achieved by performing CNOT gate and a $Hadamard$ gate receptively. Result of measuring is a couple of classical bits and probabilities for retrieving each state according to results are shown in Fig. 8.

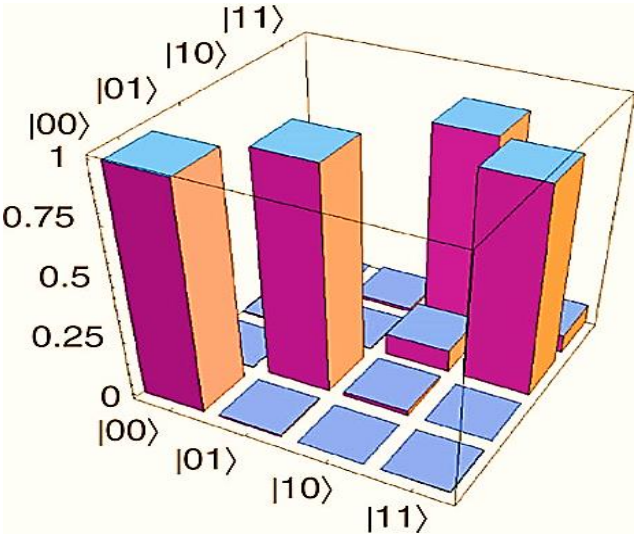


Figure 8 - Truth Table for measuring received generated Asymmetric keys

The secured entangled shared key rate evaluated by applying Koashi's method and parameter approximating according to Rice and Harrington method. The formula for evaluation of secured entangled shared key rate between QM_{SDA} and communicated members is given by (Eq. (15))

$$S_R = \frac{[\,P_S\,(1 - H(P_{e1}) - P_{EFC}\,(P_e)H(P_e) + P_S\,(0)]}{t} \quad (15)$$

Where S_R is the approximate secured entangled shared key rate between QM_{SDA} and communicated members, P_S represents the estimation amount of sifted keys by a single photon form QM_{SDA} to communicated members, P_{e1} represents the estimation amount of errors which generated by a single photon , P_e represents the total number of sifted generated keys between QM_{SDA} and communicated members , P_{EFC} represents the probability of the error correction efficiency , $P_S\,(0)$ represents the estimation amount of sifted keys by a 0 photon pulses form QM_{SDA} to communicated members , $H(P_e)$ and $H(P_{e1})$ represent the binary entropy function and t represent the duration of established sessions between QM_{SDA} and communicated members. The relation between generated entangled shared and purified keys rated in Kbits/s as function of the distance between communicated peers in km is illustrated in Fig.9. The relation between key rate and distance is conversely which implies as long distance enlarged the key rate is reduced.

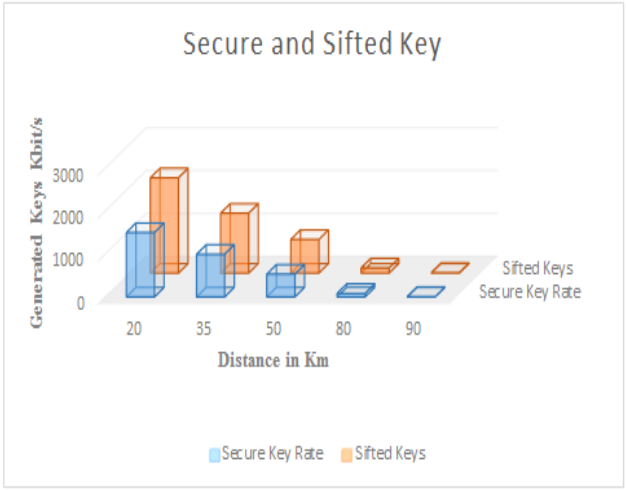


Figure 9 - The relation between generated Asymmetric keys rated in Kbits/s as function of the distance between communicated peers in km

Conclusion

A proposed architecture for public quantum cryptography is investigated. The proposed architecture focus on Generation and measuring shared entangled pair keys between the communicated peers in a multicast network by Quantum Multicast shared distribution and measurement centre " QM_{SDM} " and quantum gates. Encoding of transmitted quantum messages is handled by the basis of quantum teleportation. Teleportation or encoding at sender side will be accomplished by C_{NOT} and a $Hadamard$ gates. Decoding the teleported message is achieved by performing the correction action on received entangled pair. On the receiver side decoding will be accomplished by X and Z gates. If two members within the same multicast group need to communicate, they can by using entangled shared key pair. If two members in a different groups need to communicate, they can by complete or partial support of QM_{SDM}. By full support of QM_{SDM} the responsibility of QM_{SDM} is decoding /encoding the teleported / original transmitted quantum message between the communicated members. Optical clock synchronization is used for improving the transmission of generated entangled keys as well key update.

REFERENCES

1. Wootters, W., & Zurek, W. (1982). A single quantum cannot be cloned. Nature, 299(5886), 802-803. doi:10.1038/299802a0
2. Bennett, C., & Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. Theoretical Computer Science, 560, 7-11. doi:10.1016/j.tcs.2014.05.025
3. Liang, H., Liu, J., Feng, S., & Chen, J. (2013). Quantum teleportation with partially entangled states via noisy channels. Quantum Inf Process, 12(8), 2671-2687. doi:10.1007/s11128-013-0555-3
4. Nielsen, M., & Chuang, I. (2000). Quantum computation and quantum information. Cambridge: Cambridge University Press.
5. Zeng, G.H. (2006) Quantum cryptology : Science Press
6. Van Assche, G. (2006). Quantum cryptography and secret-key distillation. Cambridge: Cambridge University Press.
7. Zeng, G. (2010). Quantum private communication. Beijing: Higher Education Press.
8. Barenco, A., Bennett, C., Cleve, R., DiVincenzo, D., Margolus, N., & Shor, P. et al. (1995). Elementary gates for quantum computation. Physical Review A, 52(5), 3457-3467. doi:10.1103/physreva.52.3457
9. Hirvensalo, M. (2001). Quantum computing. Berlin: Springer.

10. Sharbaf, M. S. (2009, April). Quantum cryptography: a new generation of information technology security system. In Information Technology: New Generations, 2009. ITNG'09. Sixth International Conference on (pp. 1644-1648). IEEE.
11. Jin, X. M., Ren, J. G., Yang, B., Yi, Z. H., Zhou, F., Xu, X. F., ... & Pan, J. W. (2010). Experimental free-space quantum teleportation. Nature Photonics, 4(6), 376-381.
12. Bell, J. S. (1964). On the einstein-podolsky-rosen paradox. Physics, 1(3), 195-200.
13. Aspect, A., Dalibard, J., & Roger, G. (1982). Experimental test of Bell's inequalities using time-varying analyzers. Physical review letters, 49(25), 1804.
14. Shimizu, K., & Imoto, N. (1999). Communication channels secured from eavesdropping via transmission of photonic Bell states. Physical Review A,60(1), 157.
15. Einstein, A., Podolsky, B., & Rosen, N. (1935). Can quantum-mechanical description of physical reality be considered complete?. Physical review, 47(10), 777.
16. Boström, K., & Felbinger, T. (2002). Deterministic secure direct communication using entanglement. Physical Review Letters, 89(18), 187902.
17. Deng, F. G., & Long, G. L. (2004). Secure direct communication with a quantum one-time pad. Physical Review A, 69(5), 052319.
18. Man, Z. X., Xia, Y. J., & An, N. B. (2006). Quantum secure direct communication by using GHZ states and entanglement swapping. Journal of Physics B: Atomic, Molecular and Optical Physics, 39(18), 3855.
19. Deng, F. G., Long, G. L., & Liu, X. S. (2003). Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block.Physical Review A, 68(4), 042317.
20. Lucamarini, M., & Mancini, S. (2005). Secure deterministic communication without entanglement. Physical review letters, 94(14), 140501.
21. Yan, F. L., & Zhang, X. Q. (2004). A scheme for secure direct communication using EPR pairs and teleportation. The European Physical Journal B-Condensed Matter and Complex Systems, 41(1), 75-78.
22. Cai, Q. Y. (2004). The Ping-Pong protocol can be attacked without eavesdropping. arXiv preprint quant-ph/0402052.
23. Zhu, A. D., Xia, Y., Fan, Q. B., & Zhang, S. (2006). Secure direct communication based on secret transmitting order of particles. Physical Review A, 73(2), 022338.
24. Xue, P., Han, C., Yu, B., Lin, X. M., & Guo, G. C. (2004). Entanglement preparation and quantum communication with atoms in optical cavities. Physical Review A, 69(5), 052318.
25. Lee, H., Lim, J., & Yang, H. (2006). Quantum direct communication with authentication. Physical Review A, 73(4), 042305.
26. Curty, M., & Santos, D. J. (2001). Quantum authentication of classical messages. Physical Review A, 64(6), 062309.
27. Dušek, M., Haderka, O., Hendrych, M., & Myška, R. (1999). Quantum identification system. Physical Review A, 60(1), 149.
28. Zeng, G., & Zhang, W. (2000). Identity verification in quantum key distribution. Physical Review A, 61(2), 022303.
29. Ljunggren, D., Bourennane, M., & Karlsson, A. (2000). Authority-based user authentication in quantum key distribution. Physical Review A, 62(2), 022305.
30. Biham, E., Huttner, B., & Mor, T. (1996). Quantum cryptographic network based on quantum memories. Physical Review A, 54(4), 2651.
31. Metwaly, A. F., Rashad, M. Z., Omara, F. A., & Megahed, A. A. (2014). Architecture of multicast centralized key management scheme using quantum key distribution and classical symmetric encryption. The European Physical Journal Special Topics, 223(8), 1711-1728.
32. Ying, S., Qiao-Yan, W., & Fu-Chen, Z. (2008). Multiparty Quantum Chatting Scheme. Chinese Physics Letters, 25(3), 828.
33. Metwaly, A. F., & Mastorakis, N. E. (2015). Architecture of Decentralized Multicast Network Using Quantum Key Distribution and Hybrid WDM-TDM. Advances In Information Science And Computer Engineering, 504-518.
34. Metwaly, A., Rashad, M. Z., Omara, F. A., & Megahed, A. A. (2012, May). Architecture of point to multipoint QKD communication systems (QKDP2MP). In Informatics and Systems (INFOS), 2012 8th International Conference on (pp. NW-25). IEEE.
35. Farouk, A., Omara, F., Zakria, M., & Megahed, A. (2015). 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.
36. Ting, G., Feng-Li, Y., & Zhi-Xi, W. (2005). A simultaneous quantum secure direct

communication scheme between the central party and other M parties.Chinese Physics Letters, 22(10), 2473.
37. Wang, C., Deng, F. G., & Long, G. L. (2005). Multi-step quantum secure direct communication using multi-particle Green–Horne–Zeilinger state. Optics communications, 253(1), 15-20.
38. Wang, J., Zhang, Q., & Tang, C. J. (2006). Quantum secure direct communication based on order rearrangement of single photons. Physics Letters A, 358(4), 256-258.
39. Qing-Yu, C., & Bai-Wen, L. (2004). Deterministic secure communication without using entanglement. Chinese Physics Letters, 21(4), 601.
40. Cai, Q. Y. (2006). Eavesdropping on the two-way quantum communication protocols with invisible photons. Physics Letters A, 351(1), 23-25.
41. Long, G. L., Deng, F. G., Wang, C., Li, X. H., Wen, K., & Wang, W. Y. (2007). Quantum secure direct communication and deterministic secure quantum communication. Frontiers of Physics in China, 2(3), 251-272.

BIOGRAPHIES

Ahmed F. Metwaly, is currently a Ph.D. candidate at Mansoura University, Egypt. He is working as senior lecturer at AL-Zahra College for women. He has publications in international journals and conferences held by IEEE, Springer and IACSIT. He is reviewer and editor board member for prestigious journals published by Springer, IEEE, Nature, indersciences, IAENG, and SDIWC. He also members in many prestigious association like IEEE and IACSIT. His interests are Quantum Communication, Quantum Cryptography and Cloud Computing.

Prof. Magdi Z. Rashad is Professor in the Computer Science Department and Vice Dean for Community Affairs and Development in the Faculty of Computers and Information, Mansoura University. He has published over 100 research papers in prestigious international journals, and conference proceedings. He has served as Chairman and member of Steering Committees and Program Committees of several national Conferences. He has supervised over 50 PhD and M. Sc thesis.

Prof. Fatma A. Omara is Professor in the Computer Science Department and Vice Dean for Community Affairs and Development in the Faculty of Computers and Information, Cairo University. She has published over 45 research papers in prestigious international journals, and conference proceedings. She has served as Chairman and member of Steering Committees and Program Committees of several national Conferences. She has supervised over 30 PhD and M. Sc thesis. Prof. Omara is a member of the IEEE and the IEEE Computer Society. Prof. Omara interests are Parallel and Distributing Computing, Parallel Processing, Distributed Operating Systems, High Performance Computing, Cluster, Grid, and Cloud Computing

Prof. Adel A. Megahed is emeritus Professor, Dept. of Engineering Math. And Physics, Faculty of Engineering, Cairo University, since January 2004. He has published over 45 research papers in prestigious international journals, and conference proceedings. He translated physics books into Arabic language. He is reviewer, editor abroad and member for many prestigious associations. He invited for participating and keynote speaker for many international and national

conferences. His interests are Quantum Communication, Computational Fluid-Dynamics, Multi-Rigid bodies Dynamics and Modelling of Pollution Dispersion.

