Design and Analysis of Secure Quantum Network System with Trusted Repeaters

Yao Zhang, Qiang Ni
{y.zhang70, q.ni}@lancaster.ac.uk
School of Computing and Communications, InfoLab 21, Lancaster University
LA1 4WA, Lancaster, United Kingdom

***Abstract*—Quantum key distribution (QKD) has received great attention towards future secure communication systems. Since the laws of the quantum mechanics make sure the security and it cannot be cracked by using any mathematical method, there is a great deal of research work in this area which achieves groundbreaking progress. However, some obvious issues are still the obstacle of the daily use of QKD, such as the distance of communications. Using trusted repeaters is a promising approach to extend the range of QKD. This paper proposes a possible QKD system with current network structures and comes up with a novel method of using trusted repeaters to satisfy the requirement of secure QKD network.**

***Index Terms*—Quantum key distribution, trusted repeaters.**

I. Introduction

The communication security is becoming increasingly important since our world never needs to communicate as frequently as it does today. Variety of cryptography algorithms are adopted in our communications to make sure that our messages and information are secure. The traditional cryptography is based on the mathematical complexity, for example, the RSA public-key cryptography. It is impossible to decrypt a cipher text which is encrypted by RSA algorithm in reasonable time. However, with the development of quantum computing, particularly the Shor's algorithm, which can crack the keys generated by RSA in polynomial time [1], [2], the encryption will not be secure any longer. In this case, a completely different percept of communications based on the laws of quantum mechanics is addressed, which is widely known as the quantum communication.

One type of quantum communications, also as the most maturely developed one, the quantum key distribution (QKD) has been exploited by many research groups all over the world in last decades and it has been proved that QKD provides a promising security in communications [3]. On the other hand, a plenty of experiments on QKD have been completed or are ongoing. Very recently, a long distance quantum communication between outer space and the ground makes the distance of the QKD implementation be raised up to 1,200 kilometres via wireless channel by quantum communication satellite and ground stations [4]. In addition, the Beijing-Shanghai Backbone Network in China, which is the QKD link spanning over 2,000 kilometres has also been put in use. This is the longest distance implemented the QKD around the world currently. In addition, plenty of applications of different types of QKD are been researching and developing.

As these practical implementations of QKD are rapidly maturing, it is reasonable to believe that the QKD used in people's daily lives will be the trend in the near future. Thus, this paper proposes a novel idea of combining QKD with modern networks as its main contribution. Furthermore, a new method of using trusted repeaters to extend the range of QKD is proposed as well.

The rest of this paper is arranged as follows. In section II, it reviews QKD, especially the original BB84 protocol, which is the fundamental of current implementations of QKD. In section III, the system description is given, including the protocol of using trusted repeaters. Finally, the conclusion is shown in section IV.

II. Quantum key distribution

Bennett and Brassard proposed the first QKD protocol, which is well known as BB84 protocol [5]. The BB84 protocol now is widely researched and even used, and there are many practical implementations using some advanced techniques, such as the decoy-state QKD (DSQKD) and the measurement-device-independent QKD (MDIQKD). For realising the original BB84 protocol, the quantum bit or qubit needs to be described. The qubit is the minimum information for quantum computation and quantum information, which typically represents a microscopic system and corresponds to 'bit' in the classical computation, such as an atom or a polarized photon. Two orthogonal states, for example, the polarization of a photon, both direction of vertical/horizontal and direction of 45 degree/-45 degree can be encoded as the bit 0 and 1. Conventionally the qubit is denoted by Dirac symbol as $|0\rangle$ and $|1\rangle$. Therefore, the correspondence of photon polarization and qubits is depicted as Fig. 1 (a). Because of the uncertainty principle of quantum mechanics, it must be measured when there comes a qubit so that it is able to be known what the state of the qubit is. Therefore, in quantum information, another necessary processing is the measurement. Suppose that there is a communication system between Alice and Bob, and Alice as the transmitter, wants to send a photon to Bob. The photon is polarized as vertical or horizontal to represent qubit $|0\rangle$ or $|1\rangle$. Bob can decode the qubit via measuring the transmitted photon by using the vertical/horizontal measuring basis perfectly. But he only has 50% probability to get the correct result if the other measuring basis is used. In other words, it is impossible to achieve information by the measurement of using diagonal

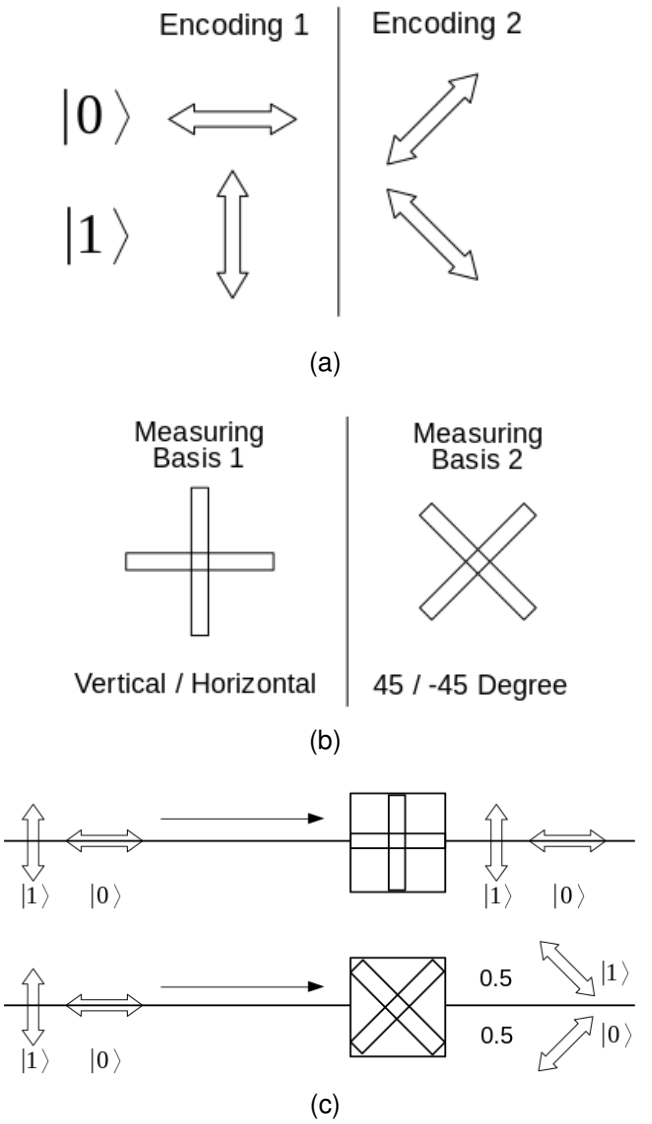

Fig. 1. (a) Qubits encoded by the directions of the photon polarization. The qubit $|0\rangle$ corresponds to the horizontal polarization or 45 degree polarization, and the qubit $|1\rangle$ corresponds to the vertical polarization or -45 degree polarization. (b) Two orthogonal measuring basas. (c) Prepared vertical/horizontal polarized photon is measured by different basis, it is 0.5 chance to get qubit $|0\rangle$ or $|1\rangle$ if using the wrong basis.

Polarization Alice	|	／	|	|	＼	／	|	＼	|	—	|	＼	|	—	|
Sent sequence Alice	1	0	1	1	1	0	1	1	1	0	1	1	1	0	1
Measuring basis Bob	+	×	+	×	+	×	+	+	×	×	+	+	×	+	×
Measured results Bob	1	0	1	0	1	0	1	0	1	1	1	0	1	0	1
Sifted results Alice & Bob	1	0	1	-	-	0	1	-	-	-	1	-	-	0	-

Fig. 2. The demonstration of BB84 flow.

basis. In this case, the measuring basis and the measuring process are depicted in Fig. 1 (b) and (c).

To sum up, a general discription of BB84 protocol is given below:

1. The transmitter (Alice) generates 4 types of keys (vertical, horizontal, 45 degree and -45 degree) randomly, then the state of the key has been determined.
2. The receiver (Bob) measures the key that Alice sent to him, by using two types of measuring basis randomly to decode the key. Since Bob's measuring basis is chosen randomly, there is half chance to use the wrong basis. Fig. 2 demonstrates the result of a bit stream has been transmitted and received. From Fig. 2, the transmitted sequence and the received sequence are listed below separately:
   - 101110111011101
   - 101010101110101.

   It is easy to see, there must be some incorrect measurements. The incorrect rate can be calculated as $50\%(wrong\ \ basis) * 50\%(correct\ rate\ in\ wrong\ basis) = 25\%$.
3. Bob tells Alice what type of measuring basis he chose for each encoded qubit via the public channel which can be eavesdropped by the eavesdropper Eve. Then, according to this public information, Alice is able to know which basis is right and which is wrong from comparing with her own polarization of photons she just sent.
4. Finally, Alice tells Bob which results of wrong basis need to be discarded via the public channel. The remained results Bob measured are the final sifted results. These two remained sequences are all the same in both Alice's and Bob's sides, and the same sequence is the generated secret key.

From the description above, the rest of the story becomes very clear. Even though Eve obtains all the information from the public channel, she needs to eavesdrop the quantum channel as well to get the whole information restored. However, if she did so, the state of the transmitted photon would be destroyed and this would result in that the error rate increases rapidly and becomes much higher than the threshold, so that both communication sides are able to perceive the existance of the eavesdropper. Therefore, because of the no-cloning principle of quantum mechanics, the BB84 protocal can build an absolutely secure communication system theoretically.

In practical implementation of BB84 protocol, due to some imperfect factors of real-life implementations, the distance of peer-to-peer QKD is roughly limited. For solving this problem, the trusted repeater method is one of usually adopted solutions [6]–[8]. The basic model of this method is illustrated as Fig. 3. In this model, the repeater node is supposed trusted beforehand, or it cannot guarantee the security. This model is simply able to be regarded as two parts separately—QKD between Alice and the repeater, and QKD between the repeater and Bob. It will generate two different secret keys—K1 and K2, individually, in these two QKD processes. Thus, at first, the message flows from Alice to the repeater by being encrypted with K1. Secondly, it is decrypted in the repeater. Then the message is encrypted again with K2 that generated by the repeater and Bob. Finally, Bob receives the encrypted message

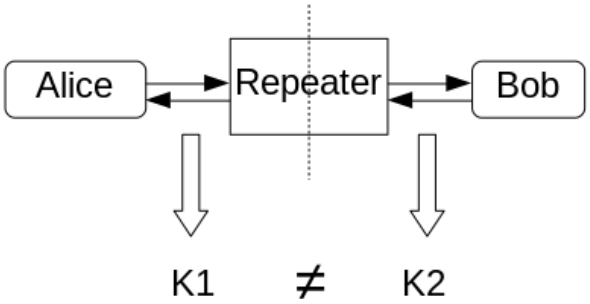

Fig. 3. Normal trusted repeater model.

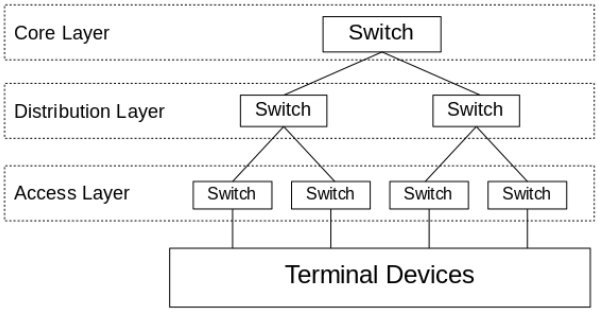

Fig. 4. Layer 3 network structure

and decrypts it using K2. Obviously, it adds an encryption-decryption process when it adds one more repeater node. In this paper, we propose a different protocol that allows Alice and Bob share the secret key and the encryption-decryption is needed only once.

III. System description

In the modern life, present network communications involve a layer structure based on Open System Interconnection (OSI) model that defines the functions of 7 layers of communication protocols. Or specifically, a simplified version treated as TCP model is adoped in most of network scenarios, the Internet for example. To reference the TCP model, the most of network devices are working on the second and the third layer, such as switches and routers. Usually, constructing a network will consider a hierarchical internetworking model, which is formed by three layers—the access layer, distribution layer and core layer. These three layers are classified by the logical topology of the network. If all of these three layers are deployed in a network, then the network is called layer 3 network. Otherwise, if there is no core layer in the network, this is called layer 2 network. A typical topology of the whole layer 3 network is sketched in Fig. 4.

The layer 3 network includes a core layer. The core layer is very important since it is the backbone and the data-transfer-channel of the whole network. It should provide high reliability and high efficiency of the data transportation across a network. Communications in the layer 3 network are able to span multiple collision domains via IP routing. Therefore, for this

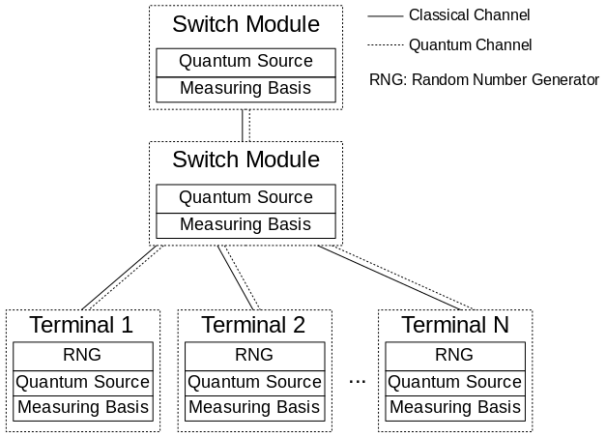

Fig. 5. A simplest QKD combined network model. There are two links between each terminal and the switch module. The quantum channel can be treated as a virtual logical link, which is used to transmit qubits (photons).

reason, constructing a large-scale network usually considers adopting this structure.

The layer 2 network, which only has the access layer and the distribution layer, is relatively more simple than the operation of the layer 3 network. In the layer 2 network, switches forward all the data packages according to MAC address tables. All the terminal devices are located in the same collision domain in the layer 2 network. This means it limits the expansion of the layer 2 network to a large extent. Therefore, layer 2 network is always used to build the small-scale local area network (LAN).

To simplify the analysis of the network structure that combined with QKD, the layer 2 networt will be considered at first.

As Fig. 5 shows, terminals and the switch module are connected by two links, which are classical channel and quantum channel separately. The classical channel is used to transfer the classical data as usual, while the quantum channel is used to transmit quantum information. Since the adopted quantum source is polarized photons, for the reason of cost efficiency, the quantum channel is supposed to be the reuse of the classical optical fiber. It is worth noticing that the switch module can exist in both the access layer or the distribution layer for the layer 2 network.

The difference between terminals and switch modules is in terminals, the quantum source sends qubits according to random numbers that generated by random number generators (RNGs), while switch modules do not need RNGs. The reason for this difference is that we only need to initialise the encoded key at the stage of that the transmitter sending qubits according to random numbers. The basic idea of the whole QKD procedure is depicted as the flow diagram in Fig. 6. According to the diagram, the protocol can be described as below.

1. Alice chooses some quantum states randomly and sends them to trusted repeater 1. Then repeater 1 sends the measurement results back to Alice. Alice then knows in

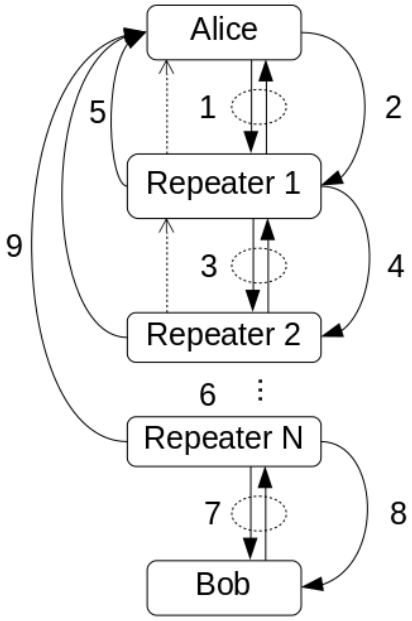

Fig. 6. QKD procedure with trusted repeaters.

which positions the bits should be kept and stores the positions as the mask.

2. Alice sends the mask to repeater 1. Repeater 1 then knows which bits should be kept as well.
3. Repeater 1 sends quantum states to repeater 2 according to the key it sifted with Alice at the first stage and receives measurement results from repeater 2. Then it knows which bits should be kept and stores positions as the mask.
4. Repeater 1 sends the mask to repeater 2. Repeater 2 then knows which bits should be kept and stores positions as the mask as well.
5. Repeater 1 sends the mask it stored back to Alice and lets Alice update her mask.
6. Repeat process 3 and 4 between two adjacent repeaters, and the mask will be sent back to Alice via previous repeaters in each stage.
7. Repeater N iterates the same QKD process with Bob.
8. Repeater N tells Bob the remained sequence. At this stage, Bob achieves the final secret key.
9. Repeater N sends the mask back to Alice via other repeaters to let Alice update her mask again. Finally, Alice knows the final secret key.

This procedure also needs repeaters be trusted and it makes the key shorter and shorter from the raw key randomly generated by Alice. Because of the sifted key has approximately half of the length of the raw key in each QKD process, the final key length l can be expressed as

$$l = L \cdot (\frac{1}{2})^{n-1},$$

where L is the raw key length that Alice transmitted and n is the number of all nodes in the cummunication, which includes

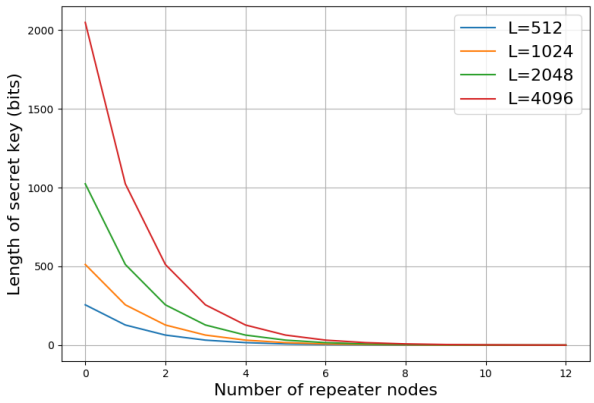

Fig. 7. Secret key length with different numbers of repeaters.

Alice and Bob themselves. So $n-2$ represents the number of trusted repeater nodes. The relationship between secret key lengths and numbers of trusted repeater nodes can be seen in Fig. 7 clearly. From Fig. 7, it is easy to know when the length of secret key is specified, it needs a relative long raw key that generated by Alice. Furthermore, the number of trusted repeaters affects the length of the raw key seriously. Since a longer secret key is able to provide higher security, this protocol will have more effectivity and efficiency when the number of trusted repeaters is not too large.

IV. Conclusion

This paper proposes a potential application of QKD in current network by combining the QKD with typical network structure, and designs a new protocol using trusted repeaters, which is different from the normal trusted repeater method, so that it can reduce the number of encryption and decryption in communications.

References

[1] P. W. Shor, "Proceedings of the 35th annual symposium on foundations of computer science," *IEE Computer society press, Santa Fe, NM*, 1994.
[2] T. Monz, D. Nigg, E. A. Martinez, M. F. Brandl, P. Schindler, R. Rines, S. X. Wang, I. L. Chuang, and R. Blatt, "Realization of a scalable shor algorithm," *Science*, vol. 351, no. 6277, pp. 1068–1070, 2016.
[3] H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and a proof of its unconditional security," *J. Crypto.*, vol. 18, no. 2, pp. 133–165, 2005.
[4] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li *et al.*, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, p. 43, 2017.
[5] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. 1984 IEEE International Conf. Comput. Syst. Signal Process.*, 1984, pp. 175–179.
[6] L. Salvail, M. Peev, E. Diamanti, R. Alléaume, N. Lütkenhaus, and T. Länger, "Security of trusted repeater quantum key distribution networks," *J. Comput. Secur.*, vol. 18, no. 1, pp. 61–87, Jan. 2010.
[7] D. Elkouss, J. Martinez-Mateo, A. Ciurana, and V. Martin, "Secure optical networks based on quantum key distribution and weakly trusted repeaters," *Journal of Optical Communications and Networking*, vol. 5, no. 4, pp. 316–328, 2013.
[8] O. Maurhart, "Qkd networks based on q3p," in *Applied Quantum Cryptography*. Springer, 2010, pp. 151–171.