Science Bulletin

Measurement-device-independent quantum communication without encryption

Peng-Hao Niu, Zeng-Rong Zhou, Zai-Sheng Lin, Yu-Bo Sheng, Liu-Guo Yin and Gui-Lu Long

Citation: Science Bulletin **63**, 1345 (2018); doi: 10.1016/j.scib.2018.09.009

View online: http://engine.scichina.com/doi/10.1016/j.scib.2018.09.009

View Table of Contents: http://engine.scichina.com/publisher/scp/journal/SB/63/20

Published by the Science China Press

Science Bulletin 63 (2018) 1345–1350

Contents lists available at ScienceDirect

Science Bulletin

journal homepage: www.elsevier.com/locate/scib

Science Bulletin
www.scibull.com

Article

Measurement-device-independent quantum communication without encryption

Peng-Hao Niu [a,b,c,d], Zeng-Rong Zhou [a,b,c,d], Zai-Sheng Lin [e,f], Yu-Bo Sheng [g,h,i], Liu-Guo Yin [e,f,*], Gui-Lu Long [a,b,e,f,*]

[a] State Key Laboratory of Low-dimensional Quantum Physics, Beijing 100084, China
[b] Department of Physics, Tsinghua University, Beijing 100084, China
[c] Collaborative Innovation Center of Quantum Matter, Beijing 100084, China
[d] Beijing Academy of Quantum Information Sciences, Beijing 100193, China
[e] Beijing National Research Center for Information Science and Technology, Beijing 100084, China
[f] School of Information and Technology, Tsinghua University, Beijing 100084, China
[g] Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
[h] College of Telecommunications & Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
[i] Key Laboratory of Broadband Wireless Communication and Sensor Network Technology, Nanjing University of Posts and Telecommunications, Ministry of Education, Nanjing 210003, China

ARTICLE INFO

Article history:
Received 14 July 2018
Received in revised form 24 August 2018
Accepted 3 September 2018
Available online 15 September 2018

Keywords:
Quantum secure direct communication
Measurement-device-independent
Quantum dialogue
Encryption
Cryptography

ABSTRACT

Security in communication is vital in modern life. At present, security is realized by an encryption process in cryptography. It is unbelievable if a secure communication is achievable without encryption. In quantum cryptography, there is a unique form of quantum communication, quantum secure direct communication, where secret information is transmitted directly over a quantum channel. Quantum secure direct communication is drastically distinct from our conventional concept of secure communication, because it does not require key distribution, key storage and ciphertext transmission, and eliminates the encryption procedure completely. Hence it avoids in principle all the security loopholes associated with key and ciphertext in traditional secure communications. For practical implementation, defects always exist in real devices and it may downgrade the security. Among the various device imperfections, those with the measurement devices are the most prominent and serious ones. Here we report a measurement-device-independent quantum secure direct communication protocol using Einstein-Podolsky-Rosen pairs. This protocol eradicates the security vulnerabilities associated with the measurement device, and greatly enhances the practical security of quantum secure direct communication. In addition to the security advantage, this protocol has an extended communication distance, and a high communication capacity.

1. Introduction

Confidential communication is widely required in modern societies. A general secure communication picture is shown in Fig. 1. It consists of a key distribution channel and a ciphertext channel. A plaintext is encoded into ciphertext by sender Alice, and sent to receiver Bob through the classical channel. The ciphertext is then decoded to plaintext by Bob again. In the encryption and decryption process, a key is required, which is distributed through the key distribution channel. Usually, a ciphertext is encoded by the advanced encryption standard [1], and the key is distributed by the RSA public key scheme [2]. In this structure, there are three potential security loopholes, as indicated in Fig. 1, namely: (1) loss of key during the distribution process. Eve can intercept the key during its distribution. With a quantum computer at hand, Eve can steal all the key with ease using the Shor algorithm [3]; (2) loss of key in storage and management. It is one of the most difficult part in cryptography. To overcome this, both high storage technology and strict human management system are required; (3) interception of ciphertext for later cryptanalysis. It is well-known that the one-time-pad encryption scheme [4,5] is perfectly secure as long as the key is kept perfectly secure. In order to ensure the security, it is vital to reduce potential security loopholes.

Quantum key distribution (QKD) [6] allows two parties to establish a shared secret key. It eliminates the security loophole associated with key distribution. However, the other two security loopholes still exist. Eve can in principle intercept all the ciphertext, and can either perform cryptanalysis now or at a later time.

* Corresponding authors.
E-mail addresses: yinlg@tsinghua.edu.cn (L.-G. Yin), gllong@tsinghua.edu.cn (G.-L. Long).

https://doi.org/10.1016/j.scib.2018.09.009
2095-9273/

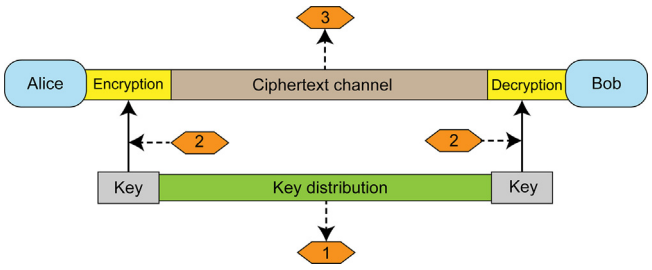

Fig. 1. (Color online) Structure of conventional secure communication and the security loopholes. Orange polygons with numbers represent: (1) leakage of key during distribution; (2) leakage of key in storage and management; (3) ciphertext interception.

Though it happens very rarely, key may leak to Eve. Then she would obtain the secret information encoded in the ciphertext.

Quantum secure direct communication (QSDC) [7–9] is a cryptographic scheme that does not require key and encryption. In the first QSDC protocols [7,8], Alice and Bob, establish a secure quantum channel by sending a block of single photons, each from an Einstein-Podolsky-Rosen (EPR) pair, from the sender to the receiver. In the efficient-QSDC protocol [7], information is encoded in the quantum states. In the two-step-QSDC protocol [8], information is encoded in the dense coding operation. The procedure in the efficient-QSDC protocol is simpler than that of the two-step QSDC protocol. However, the two-step-QSDC protocol is easier to generalize, and it has been developed into a quantum direct dialogue protocol [10]. Using block of single photons, a QSDC protocol was also proposed [9]. Single photon based QSDC protocol is easier to implement than those based on EPR pairs.

The fundamental difference between QKD and QSDC is that QSDC establishes the security of the quantum channel first, whereas the security is known only after the key distribution session is completed in QKD. Taking the two-step QSDC protocol [8] as an example. Alice first prepares a block of EPR pairs, where each pair is in state $|\psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$. She takes one photon from each pair to form one ordered sequence, and the remaining qubits form another ordered sequence. She then sends the first ordered sequence to Bob. At this stage, Alice and Bob choose some of the qubits to make single qubit measurements in either the σ_Z basis or the σ_X basis and compare the results so as to establish the security of the quantum channel. Up to know, any eavesdropping will be found, and Eve could not obtain any information. After ensuring the security of the channel, the sender, either Alice or Bob, can encode her/his message by dense coding operations, and then sends the ordered qubits to the receiver. After receiving the ordered qubits sequence, the receiver can make collective measurements to read out the message. In this QSDC process there is no key distribution, the established secure quantum channel are the shared EPR pairs, with Alice holding half of the qubits, while Bob holding the other half of the partner qubits. Since there is no key, there is no need for key storage and management. The encoding is simply the dense coding operation. If Eve tried to intercept the ordered sequence in the second transmission, when the sender has already encoded the message, she will obtain a sequence of complete random numbers, random not only to Eve, but also to the sender and the receiver. Hence QSDC is a novel secure communication system, without key distribution, without key storage and management and without ciphertext. This can offer great security advantage, and provides a new alternative in the zoo of cryptographic technology.

Remarkable achievements in both theory and experiment of QSDC have been achieved recently. A modulation frequency encoding method was introduced into the single-photon based DL04-QSDC protocol [9], which can realize secure direct communication in a noisy and lossy channel, and it has been experimentally demonstrated [11]. The efficient-QSDC and the two-step QSDC protocols [7,8], which employ EPR pairs, have been successfully demonstrated in two experiments [12,13]. Using the state-of-the-art atomic quantum memory, Zhang et al. [12] demonstrated the EPR-based QSDC protocols with high fidelity. Using fiber-photonics devices, Zhu et al. [13] demonstrated QSDC over a meaningful distance of 500 m.

Security of QSDC is provable under ideal circumstances [7–9,14,15]. However, apparatus used in practical quantum communication system have some defects, and these imperfections, especially defects in the measurement devices, can lead to leakage of information and offer eavesdroppers means to steal secret information without being found. For instance, in QKD systems, Eve can use loopholes of photon detectors to steal the secret key without being caught [16–19]. They constitute a serious security threat to practical quantum communication systems. One way to solve this problem is the measurement-device-independent (MDI) technique, which has been proposed in QKD [20], and very recently in QSDC protocol using single photons and EPR pairs [21]. In MDI protocols, though the quantum source is prepared by authentic communicating parties, all the measurements of quantum states during a communication are performed by a third party. This third party can be untrusted, or even an eavesdropper. Thus all loopholes in the measurement devices will be eliminated.

In this work, we put forward a MDI-QSDC protocols based on the two-step QSDC protocol [8]. This protocol uses EPR pairs, encoded in dense coding operation, and has a higher capacity. This MDI-QSDC protocol also doubles the communication distance, as the measurement performer is in the middle between the sender and receiver. With linear quantum optical devices, Bell analyzer can only distinguish two of the four Bell-basis states and the MDI-QSDC protocol with full Bell-basis analyzer could not be applied directly. Thus we also propose a MDI-QSDC protocol based on linear optical devices. As this operation encoded QSDC protocol is symmetric between the sender and receiver, we also generalize the MDI-QSDC protocol into an MDI quantum direct dialogue protocol.

2. Results

2.1. MDI-QSDC protocol

There are three parties in our protocol. Alice and Bob are the legitimate message sender and receiver, and Charlie is an untrusted third party, who performs the measurement. They use the EPR pairs, which can be in one of the following four Bell states,

$$\begin{aligned} |\phi^+\rangle &= (|00\rangle + |11\rangle)/\sqrt{2}, \\ |\phi^-\rangle &= (|00\rangle - |11\rangle)/\sqrt{2}, \\ |\psi^+\rangle &= (|01\rangle + |10\rangle)/\sqrt{2}, \\ |\psi^-\rangle &= (|01\rangle - |10\rangle)/\sqrt{2}. \end{aligned} \tag{1}$$

The MDI-QSDC protocol is illustrated in Fig. 2. The detailed steps are given below.

Step (1). Alice prepares n EPR photon pairs, randomly in $|\psi^+\rangle$ and $|\psi^-\rangle$. Alice takes one photon from each EPR pair to form an ordered photon sequence, S_A. Afterwards, Alice prepares m single photons, each randomly in one of the four states, $|0\rangle, |1\rangle, |+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$, and inserts them in random positions of the ordered sequence which is comprised of remaining partner photons of the EPR pairs, and we call the new sequence C_A. Now S_A has n particles, and C_A has $n+m$ particles. Likewise, Bob prepares two ordered sequences, S_B with

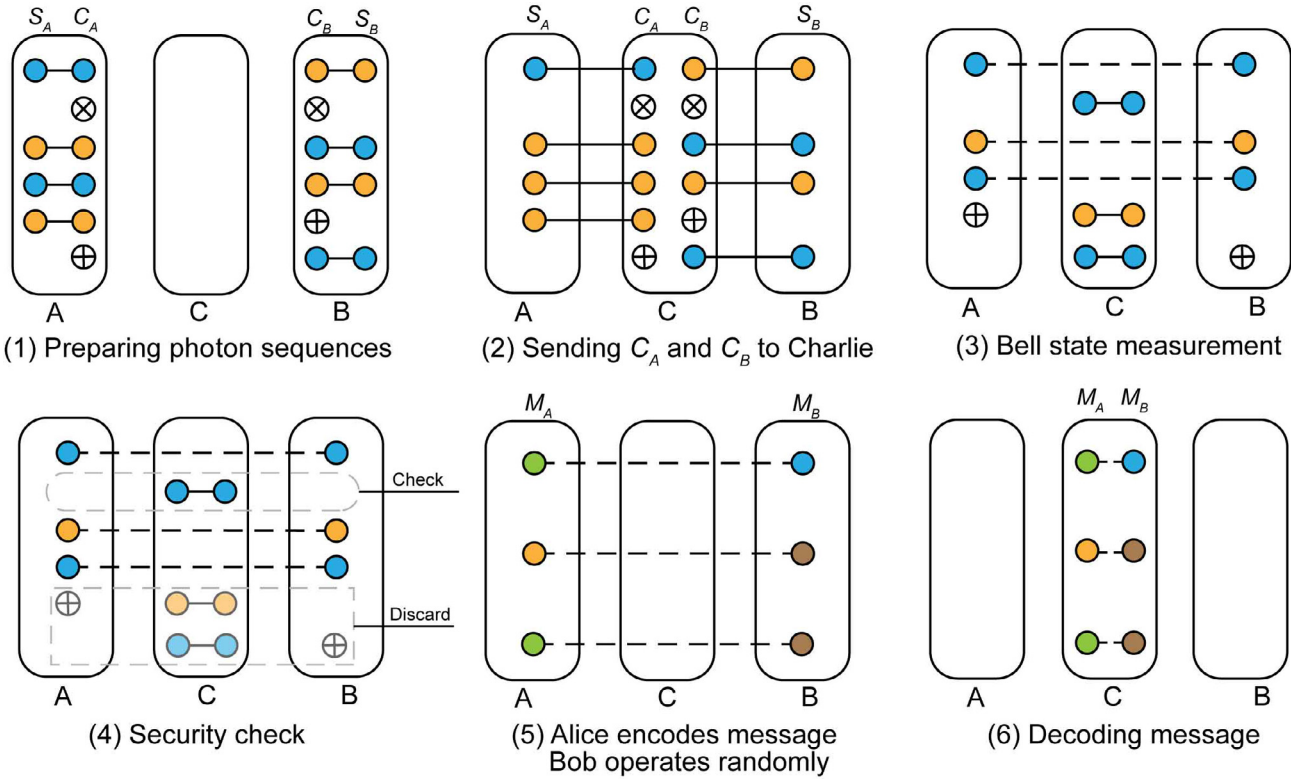

Fig. 2. Illustration of the MDI-QSDC protocol. A, B, C stand for Alice, Bob and Charlie respectively. Orange and blue circles represent state $|\psi^+\rangle$ and $|\psi^-\rangle$ pairs respectively. (+) and (×) mean *R-basis* ($|0\rangle, |1\rangle$) and *D-basis* ($|+\rangle, |-\rangle$) respectively. Solid lines and dashed lines represent prior (solid) and swapped (dashed) entanglement. In (4), photons encircled by a frame labeled by "check" are used for security check. Photons surrounded in the frame labeled by "discard" are discarded. In (5), different colors of the photons represent the different encoding operations U_0 (orange), U_1, U_2, U_3 (green). Bob also performs random operations I or σ_z on each of the photon, which is represented by brown for σ_z. For details, see the text for description.

n photons who are partner particles of EPR pairs, and C_B with $n+m$ photons, which are mixture of EPR partner photons and single photons randomly in one of the four states, $|0\rangle, |1\rangle, |+\rangle$ and $|-\rangle$. S_B has n particles and C_B has $n+m$ particles. This step is shown as (1) in Fig. 2.

Step (2). Alice and Bob send C_A and C_B to Charlie respectively, while keeping S_A and S_B in their hands.

Step (3). After receiving C_A and C_B, Charlie makes a Bell measurement on each pair of them and announces measured results. For photons who are the partners of EPR pairs, the Bell-basis measurement will make the corresponding partner photons in S_A and S_B entangled, due to the quantum entanglement swapping [22], as shown in Eq. (2),

$$\begin{aligned}
|\psi_{AC}^+\rangle \otimes |\psi_{BD}^+\rangle &= \frac{1}{2}\big(|\psi_{AB}^+\rangle|\psi_{CD}^+\rangle - |\psi_{AB}^-\rangle|\psi_{CD}^-\rangle \\
&\quad + |\phi_{AB}^+\rangle|\phi_{CD}^+\rangle - |\phi_{AB}^-\rangle|\phi_{CD}^-\rangle\big), \\
|\psi_{AC}^-\rangle \otimes |\psi_{BD}^+\rangle &= \frac{1}{2}\big(|\psi_{AB}^-\rangle|\psi_{CD}^+\rangle - |\psi_{AB}^+\rangle|\psi_{CD}^-\rangle \\
&\quad + |\phi_{AB}^-\rangle|\phi_{CD}^+\rangle - |\phi_{AB}^+\rangle|\phi_{CD}^-\rangle\big), \\
|\psi_{AC}^+\rangle \otimes |\psi_{BD}^-\rangle &= -\frac{1}{2}\big(|\psi_{AB}^-\rangle|\psi_{CD}^+\rangle - |\psi_{AB}^+\rangle|\psi_{CD}^-\rangle \\
&\quad + |\phi_{AB}^+\rangle|\phi_{CD}^-\rangle - |\phi_{AB}^-\rangle|\phi_{CD}^+\rangle\big), \\
|\psi_{AC}^-\rangle \otimes |\psi_{BD}^-\rangle &= -\frac{1}{2}\big(|\psi_{AB}^+\rangle|\psi_{CD}^+\rangle - |\psi_{AB}^-\rangle|\psi_{CD}^-\rangle \\
&\quad - |\phi_{AB}^+\rangle|\phi_{CD}^+\rangle + |\phi_{AB}^-\rangle|\phi_{CD}^-\rangle\big).
\end{aligned} \tag{2}$$

For those with a single photon from one side and a partner photon of an EPR pair from the other side, the Bell-basis measurement realizes a teleportation process, apart from a unitary operation. These in principle can be used for sending information, just as in the case of Ref. [21]. Because the number of single photons m is usually small, and for simplicity of the protocol, these instances are discarded. For those cases where each side provides a single photon, they are used for eavesdropping check, which is described in the next step. Different situations of particle combinations in the Bell-basis measurement is summarized in Table 1.

Step (4). Security check. After Charlie announces the measurement results, Alice and Bob announce the positions of the single photons in C_A and C_B, respectively. There will be $m+\delta$ cases where at least one of the photons is a single photon, corresponding to the situations of rows 2–4 in Table 1. Alice and Bob then exchange the basis information of those m single photons, and only measurement results corresponding to both sides are single photons will be used for security check. For single photons with the same basis, some of decompositions in terms of Bell states are shown in Eq. (3),

$$\begin{aligned}
|0\,0\rangle &= \big(|\phi^+\rangle + |\phi^-\rangle\big)/\sqrt{2}, \\
|0\,1\rangle &= \big(|\psi^+\rangle + |\psi^-\rangle\big)/\sqrt{2}, \\
|+\,+\rangle &= \big(|\phi^+\rangle + |\psi^+\rangle\big)/\sqrt{2}, \\
|+\,-\rangle &= \big(|\phi^-\rangle - |\psi^-\rangle\big)/\sqrt{2},
\end{aligned} \tag{3}$$

Table 1
Bell measurement on different combinations of photons and their functions.

C_A	C_B	Functions
E	E	Entanglement swapping for message transmission
S	S	Security check
E	S	Teleportation that is discarded for simplicity
S	E	

E means a photon from an entangled pair, and S stands for a single photon.

and results for $|11\rangle$ and $|--\rangle$ will be similar. Eve's interception can change the single photon state, which results in different Bell-basis measurement results. Using the measurement results of the single photons with identical basis, Alice and Bob can estimate error rate, hence security of the quantum channel, to judge whether continue communicating or not.

Step (5). Message coding. After security check, Alice and Bob will discard the photons in S_A and S_B that are not entangled, namely some of the photons in S_A and S_B are the left-over photons in a Bell-basis measurement involving a single photon and a partner photon from an EPR pair, as the case in row 3 and 4 of Table 1. The remaining $n-\delta$ photons of S_A form a ordered sequence M_A, and the remaining $n-\delta$ photons of S_B form another ordered sequence M_B.

To send the message, Alice first performs σ_z operations on photons whose initial states are $|\psi^+\rangle$. It is easy to see from Eq. (2) that this procedure is equivalent to preparing all the initial states of Alice in the $|\psi^-\rangle$ state. After that, M_A only contains photons whose initial state is $|\psi^-\rangle$. For M_B, it contains photons whose initial states are $|\psi^+\rangle$ and $|\psi^-\rangle$ randomly. Photon pairs of (M_A, M_B) are all in Bell states due to entanglement swapping. The states of M_A and M_B are only known to Bob now. Alice uses the four dense coding operations on photons in M_A to encode messages, namely, $U_0 = I$ for 00, $U_1 = \sigma_x$ for 01, $U_2 = i\sigma_y$ for 10 and $U_3 = \sigma_z$ for 11. To prevent Eve to perform the intercept and resend attack, Bob implements σ_z or I randomly on photons from M_B. To ensure the integrity of the message, Alice also encodes some random check numbers on some of photons in M_A at random positions.

Step (6). Alice and Bob send M_A and M_B to Charlie, who makes Bell measurement and publishes the results. Bob then can use these measurement results to decode the message and random check numbers encoded by Alice. Then Alice announces the positions and values of the random check numbers, and Bob compares them with Alice to check the integrity of messages. If the random number series has a high error rate, it means an eavesdropper attacks the communication of M_A and M_B in their way to Charlie or in the measurement device. Eavesdroppers' actions do not obtain any information on the message, only disturb the communication. On the other hand, if the random number series is correct with an acceptable error rate, the message transmission is correct, and the communication process is completed.

2.2. MDI-QSDC protocol using linear optical devices

The MDI-QSDC protocol needs a full Bell-basis measurement that distinguishes all four kinds of Bell states. Full Bell-basis measurement is impossible to realize using linear quantum optical devices. In fact, the protocol can be simplified by using only two of the four Bell states, $|\psi^+\rangle$ and $|\psi^-\rangle$. This can be realized using just linear optical devices, as shown in Fig. 3. In Fig. 3, the orange circles represent EPR pairs and purple circles represent single photons. Quantum memory is used to store entangled photon pairs after entanglement swapping before the process of security check is finished. Wave plates are used as modulators for message encoding. All optical devices in Charlie side are used for Bell-basis measurement, which can distinguish two Bell states, $|\psi^+\rangle$ and $|\psi^-\rangle$. This linear optical realization will need a slight modification to the full Bell-basis MDI-QSDC protocol. Specifically, Steps 1, 2, 3 and 6 will be the same. The following change has to be made. When Charlie makes Bell measurement, only results of $|\psi^\pm\rangle$ will be announced as successful counts and other detection events are discarded. Consequently, in Step 4, some measurement results of single photons will lead to no click events of the detector, whereas security check is still effective. In Step 5, Alice will only use operation U_0 and U_3 to encode message, and the communication capacity reduces to 1 bit per EPR pair as only half of the states can be distinguished. This protocol makes MDI-QSDC feasible with present technologies, and it is a big step forward towards its practical realization.

When the number of photons in the sequences reduces to 1, the corresponding protocols become deterministic MDI-QKD protocols.

2.3. An MDI quantum direct dialogue protocol

It is natural to generalize the one-way communication to a two-way direct dialogue protocol. Here, we will introduce an MDI-quantum dialogue (QD) protocol. In this MDI-QD protocol, Steps 1–4 are the same as the MDI-QSDC protocol. The following is the remaining steps.

Step (5). Message coding. After generating M_A and M_B, Alice and Bob divide these entangled photons into two parts. One part is M_A^1

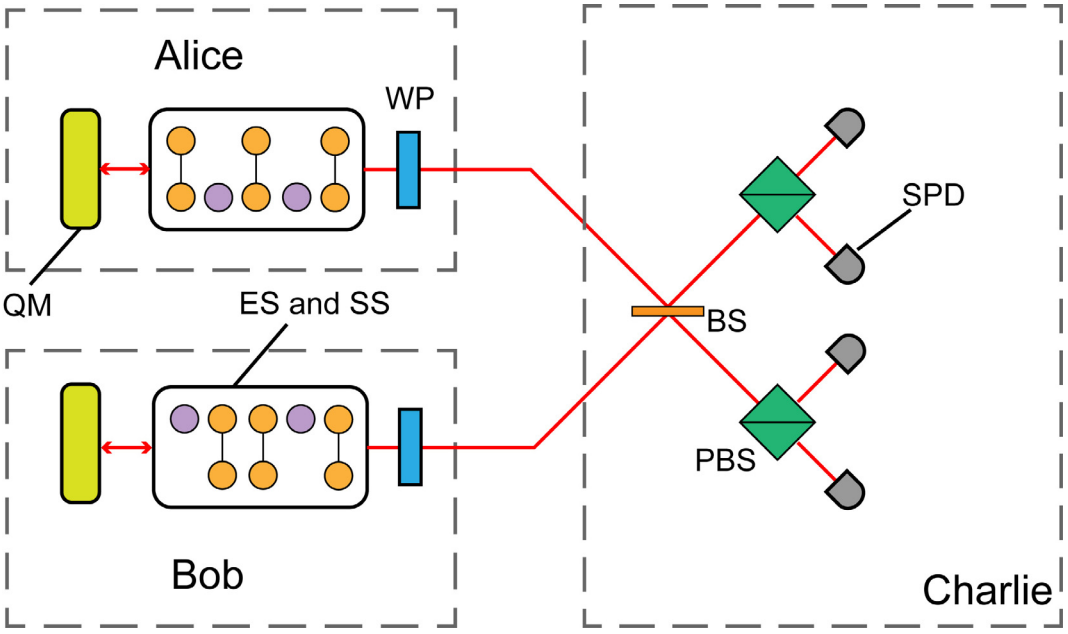

Fig. 3. Illustration diagram of MDI-QSDC with linear quantum optical devices. ES: entanglement photon source, SS: single photon source, QM: quantum memory, WP: wave plate, BS: beam splitter, PBS: polarization beam splitter, SPD: single photon detector.

and M_B^1, which is used for transmitting messages from Alice to Bob. Another part is M_A^2 and M_B^2, which is used for transmitting messages from Bob to Alice. Then the message coding process are the same as the original protocol. For M_A^1 and M_B^1, Alice first transforms initial states of photons in M_A^1 into $|\psi^-\rangle$. Then Alice encodes messages using four unitary operations U_0, U_1, U_2, and U_3, or only two of them, U_0 and U_3, using the linear optical devices. Bob will operate σ_z randomly on M_B^1 for covering. As for M_A^2 and M_B^2, Alice and Bob's operation will be opposite to the case for M_A^1 and M_B^1. That is, Bob will first transform initial states of photons in M_B^2, and encode messages in M_B^2. Alice will finish the covering process.

Step (6). Alice/Bob send M_A^1/M_B^1 and M_A^2/M_B^2 to Charlie, and Charlie makes the Bell measurement and announces the results to Alice and Bob. Then Alice and Bob can decode messages and complete a quantum dialogue.

From steps above, we can find that about half of M_A and M_B is used to transmit messages from one party to another. As a direct generalization of QSDC, this MDI-QD protocol can complete a quantum dialogue without any encryption process.

3. Discussion and conclusion

MDI-QSDC protocol uses an untrusted third party Charlie to make Bell measurements, and Charlie or an eavesdropper Eve may try tricks to get the information transformed between Alice and Bob. Generally, they can use two strategies. One is trying to find the exact Bell states of M_A and M_B before message encoding, and another one is trying to find the exact operations Alice used to messages in M_A. However, both of these two strategies can be resisted. For the first strategy, if Eve wants to know the Bell states of M_A and M_B, she also needs to know the Bell state of S_A/C_A, and S_B/C_B. This will be forbidden, because during the process of entanglement swapping, eavesdropping will be found. Not only entangled photons from C_A and C_B are sent to Charlie for measurements, but also single photons. Eve is unable to distinguish these different cases, if she tries to do some measurements, errors will be introduced and the eavesdropping behavior will be found in the security check. Besides, before sending M_A and M_B to Charlie, Bob will operate σ_z on some photons in M_B, which will cover the true Bell states in M_A and M_B. Bob's operation is only known by himself, and that will protect encoded messages from leaking to eavesdroppers.

For the second strategy, one possible method is that Charlie pretends to complete the Bell measurement by announcing fake measurement results of C_A and C_B. By doing this, Charlie can keep Bell states in S_A and C_A (also S_B and C_B) unchanged in order to find the operation of message encoding, because there are only photons with initial state $|\psi^-\rangle$ in M_A right before the message coding. However, this trick will also be blocked because there are some single photons in C_A and C_B in random positions, and are indistinguishable for Charlie. If Charlie announces fake Bell measurement results, this trick will cause an extra error rate and be found by the legitimate users. In general, the Shor-Preskill type of security proof [23] could be adopted here, and using the CCS code in the asymptotic limit, the tolerable rate of error is 11%.

In summary, we have proposed an MDI-QSDC protocol based on EPR pairs. We also gave a version with linear quantum optical devices, which can be implemented with present-day technologies. MDI-QSDC with EPR pairs protocol effectively eliminated loopholes caused by defects in detection devices, which have threatened security of practical QSDC systems. This protocol is a quantum communication process without encryption, and has a high communication capacity. We also modified the protocol and generalized it to a quantum dialogue protocol. Our protocols combined the advantage of MDI technique with QSDC scheme, most importantly, eliminated security loopholes associated with practical measurement devices.

Finally, it is worth pointing out that in practice, information security has different classes and requirement according to scenarios. QSDC, together with variants, are new members in the secure communication zoo. They provide a new choice for secure communications.

Conflict of interest

The authors declare that they have no conflict of interests.

Acknowledgments

This work was supported by the National Basic Research Program of China (2017YFA0303700 and 2015CB921001), the National Natural Science Foundation of China (61726801, 11474168 and 11474181) and in part by the Beijing Advanced Innovation Center for Future Chip (ICFC).

References

[1] Rijmen V, Daemen J. Advanced encryption standard. Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology; 2001. p. 19–22.
[2] Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM 1978;21:120–6.
[3] Shor PW. Algorithms for quantum computation: discrete logarithms and factoring. In: 35th Annual symposium on foundations of computer science; 1994. p. 124–34.
[4] Miller F. Telegraphic code to insure privacy and secrecy in the transmission of telegrams. CM Cornwell; 1882.
[5] Vernam GS. Secret signaling system patent. US patent 1919;1,310,719.
[6] Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. 1984;175–9, Bangalore, India.
[7] Long GL, Liu XS. Theoretically efficient high-capacity quantum-key-distribution scheme. Phys Rev A 2002;65:644-3.
[8] Deng FG, Long GL, Liu XS. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys Rev A 2003;68:661–6.
[9] Deng FG, Long GL. Secure direct communication with a quantum one-time pad. Phys Rev A 2004;69:357-4.
[10] Zheng C, Long GF. Quantum secure direct dialogue using Einstein-Podolsky-Rosen pairs. Sci China Phys Mech Astron 2014;57:1238–43.
[11] Hu JY, Yu B, Jing MY, et al. Experimental quantum secure direct communication with single photons. Light Sci Appl 2016;5:e16144.
[12] Zhang W, Ding DS, Sheng YB, et al. Quantum secure direct communication with quantum memory. Phys Rev Lett 2017;118:220501.
[13] Zhu F, Zhang W, Sheng YB, et al. Experimental long-distance quantum secure direct communication. Sci Bull 2017;62:1519–24.
[14] Li J, Sun FQ, Pan ZS, et al. The security analysis of two-step quantum direct communication protocol in collective-rotation noise channel. Chin Phys Lett 2015;32:080301.
[15] Lu H, Fung CF, Ma XF, et al. Unconditional security proof of a deterministic quantum key distribution with a two-way quantum channel. Phys Rev A 2011;84:042344.
[16] Makarov V, Hjelme DR. Faked states attack on quantum cryptosystems. J Mod Opt 2005;52:691–705.
[17] Makarov V, Anisimov A, Skaar J. Effects of detector efficiency mismatch on security of quantum cryptosystems. Phys Rev A 2006;74:022312.
[18] Zhao Y, Fung CF, Qi B. Quantum hacking: experimental demonstration of time-shift attack against practical quantum-key-distribution systems. Phys Rev A 2008;78:325-5.
[19] Lydersen L, Wiechers C, Wittmann C, et al. Hacking commercial quantum cryptography systems by tailored bright illumination. Nat Photon 2010;4:686–9.
[20] Lo HK, Curty M, Qi B. Measurement-device-independent quantum key distribution. Phys Rev Lett 2012;108:130503.
[21] Zhou ZR, Sheng YB, Niu PH, et al. Measurement-device-independent quantum secure direct communication. arXiv:1805.07228; 2018.
[22] Żukowski M, Zellinger A, Horne MA, et al. Event-ready-detectors Bell experiment via entanglement swapping. Phys Rev Lett 1993;71:4287–90.
[23] Shor PW, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. Phys Rev Lett 2000;85:441.

Peng-Hao Niu is a Ph.D. candidate at Department of Physics in Tsinghua University. His research interests are quantum communication theories and experiments.

Liuguo Yin received his B.S. degree from Beijing University of Aeronautics and Astronautics and his Ph.D. degree from Tsinghua University. Since 2005, he has been with the School of Information Science and Technology, Tsinghua University, where he is currently a professor. His research interests include information theory, channel coding, satellite communications, and quantum secure communication systems.

Gui-Lu Long is a professor at Tsinghua University, fellow of IoP (UK) and fellow of APS (US), President of Associations of Asian Pacific Physical Societies (2017–2019), Vice-chair of C13 of IUPAP (2015–2017). He received his B.Sc. degree from Shandong University in 1982, and Ph.D. degree from Tsinghua in 1987 respectively. His research interests include quantum communication and computing and optical microcavity.