An Efficient Quantum Secure Dialogue Scheme without Information Leakage by Using Single Photons

ZhenChao Zhu¹,², AiQun Hu¹ and AnMin Fu³
¹Information Security Research Center
Southeast University
Nanjing, China
²State Key Laboratory of Information Security, Institute of Information Engineering
Chinese Academy of Sciences
Beijing, China
³School of Computer Science and Technology
Nanjing University of Science and Technology
Nanjing, China

Abstract—A quantum dialogue protocol based on single photons is proposed in this paper, two legitimate dialogue parties can send their secret messages to each other simultaneously. The protocol is secure against the denial of service attack, the delay-photon Trojan horse attack and invisible photon eavesdropping attack. Moreover, it can overcome the information leakage problem existed in most previous quantum dialogue protocols. Compared with the only secure quantum dialogue protocol based on single photons which also can overcome the information leakage problem as far as we know, our protocol has a higher efficiency for qubits. The protocol is experimentally feasible within current technologies.

Keywords—Quantum dialogue; Single photon; Information leakage; Non-orthogonal base

I. INTRODUCTION

As that described in the literature [1], the marriage between quantum mechanics and information science gave birth to a beautiful daughter named quantum information science. One of the most matured branches of quantum information science is quantum cryptography [2] which provides an unconditional way of secure communication. The pioneering works of Bennett and Brassard published in 1984 [3] showed how to exploit quantum resources for cryptographic purposes. They presented the concept of quantum key distribution (QKD), which provides a novel way for two legitimate parties to establish a completely random secret key over a long distance. Combined with the one-time-pad scheme in which the private key is as long as the messages, secret messages can be communicated safely from one place to another. As its unconditional secure character is guaranteed by the laws of physics, QKD has attracted much attention [4-10]. In the meanwhile, some new research branches, such as quantum signature (QS) [11], quantum identification (QI) [12], quantum secret sharing (QSS) [13] and so on, have been brought to researcher’s attentions. In 2001, Long and Liu used Einstein-Podolsky-Rosen (EPR) pairs to put forward a quantum secure direct communication (QSDC) protocol [14], in which the confidential messages are directly transmitted between two authorized parties without creating a private key. As the adoption of QSDC protocols, it does not have to set up the session key before the real quantum private communication. This is a great improvement to the classical communication mode in which the private key have to be created before the secure communication. Since then, QSDC protocols were widely studied, accompanied by many kinds of protocols being put forward [15-22]. However, in QSDC protocols, the messages only can be transmitted in a single direction way, in other words, one is the sender of messages, and the other is the receiver. In 2004, to solve the problem that messages can’t be bidirectional transmitted, Nguyen put forward the first quantum dialogue protocol (Here, we call it NBA protocol for simplicity) [23] based on entanglement, in which two communication parties, both Alice and Bob are not only the senders of messages, but also the receivers. Unfortunately, In 2005, Man et al. showed that an eavesdropper can steal the messages without being detected if he/she adopts the intercept-and-resend attack strategy in the NBA protocol, then they gave an improved protocol (MAN protocol) [24]. In 2006, Ji et al. proposed a quantum dialogue scheme [25] using N batches of single photons (JI protocol). In 2007, Xia et al. presented a controlled secure quantum dialogue protocol (XIA protocol) [26] using non-maximally (pure) entangled Greenberger-Horne-Zeilinger (GHZ) states. However, it needs a trusted controller in this protocol, and no one can tolerate that he/she has to communicate with the trusted controller before the real dialogue today. In 2007, Yang et al. proposed a quasi-secure quantum dialogue protocol using single photons (YANG protocol) [27], the protocol is quasi-secure as one party’s announcement of the measurement results will disclose the correlation information between two parties. In 2008, Tan and Gao systematically analyzed this kind of insecurity problem called “classical correlation” or “information leakage” in quantum dialogue schemes independently [28, 29]. The literature [29] also showed that this kind of problem widely

This work is supported by the National Science Foundation of China (Grant Nos. 61202448, 61202352 and 61271174), the National High-Tech Research and Development Program of China (Grant No. 2013AA014001), and the National Key Technology R&D Program (Grant No. 2012BAH38B05).
In the previous quantum dialogue schemes, such as in the NBA protocol [23], MAN protocol [24] and JI protocol [25]. Since unconditional security is not only the advantage but also the crucial requirement of quantum cryptography, the information leakage problem has significantly reduced the security advantages of quantum cryptography. Since then, whether the protocol has the information leakage problem was considered as an important security evaluation index during the design of quantum dialogue protocols, and several QD protocols without information leakage have been proposed successfully. They are SHI protocol [30], GAO protocols [31], SHI protocol [32], WANG protocol [33], YANG protocols [34], ZHOU protocol [35] and so on. Through analyzing these protocols, we find that GAO protocols [31] are based on swapping the entanglement of Bell states, WANG protocol is based on the two-qutrit entangled states, YANG protocols are based on four-qubit DF states and ZHOU protocol is based on W States, although the emergence of these protocols are another demonstrations of rich applications of entanglement states, the inherent low efficiency in the preparation of entanglement states may block their practical application. SHI protocol [32] proposed based on single photons. However, it needs 2N photons to transmit N bits classical information in the SHI protocol [32]. We cannot help thinking whether an efficient quantum dialogue protocol based on single photons which can simultaneously overcome the drawback “information leakage” exists, we’ll answer this question in this paper.

In this paper, we put forward an efficient quantum secure dialogue protocol by using single photons, the protocol features the following characteristics: (1) information leakage problem does not exist, (2) the protocol only uses batches of single photons, (3) the protocol has a high efficiency for qubits. We will also show that the protocol is secure against denial of service attack, the delay-photon Trojan horse attack and invisible photon eavesdropping attack. The relevant researches show that the protocol is experimentally feasible within current technologies.

II. OUR QUANTUM DIALOGUE PROTOCOL

In our protocol, legitimate dialogue parties are Alice and Bob respectively, who send their secret messages to each other; and the secret messages are transmitted simultaneously. Alice prepares an initial single photons sequence according to her secret message, and then sends this sequence to Bob. Bob encodes on the single photons in the sequence according to his secret message and then sends the sequence to Alice. Alice measures the single photons in the sequence and calculates Bob’s secret information. Alice operates on the single photons in the sequence according to Bob’s secret information and then sends the sequence to Bob. Bob receives Alice’s secret information.

Now, let us give the details of the protocol. We suppose that the legitimate dialogue party Alice wants to transmit an n-bits secret message \( M_1 = \{ j_1, \cdots, j_m \} \) to Bob and Bob wants to transmit an m-bits secret message \( M_2 = \{ k_1, \cdots, k_n \} \) to Alice simultaneously, \( j_i, k_i \in \{0,1\} \). Without loss of generality, we suppose that n is equal to m.

1. Preparation: Alice prepares an initial single photons sequence \( M \) according to her secret message as follows. If the ith classical bit is 0, Alice prepares the single photon randomly in the state \( |0\rangle \) or \( |+\rangle \). In contrast, if the ith bit is 1, Alice prepares the single photon randomly in the state \( |1\rangle \) or \( |\rangle \), where \( |0\rangle \) and \( |1\rangle \) are the up and down eigenstates of the Pauli operator \( \sigma_z \), \( |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \) and \( |\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \) are the eigenstates of the Pauli operator \( \sigma_x \). To check eavesdropping, Alice prepares some photons randomly in one of the above four non-orthogonal states to form sequence \( S_{AB} \) and then inserts these single photons randomly into sequence M. Alice sends the new sequence \( S_{AB} \) to Bob.

2. Checking the security of the quantum channel from Alice to Bob: After having received the photons, Bob stores them in a certain order. He uses a filter and a photon number splitter (PNS) to avoid two kinds of Trojan horse attack strategies, i.e., the invisible photon eavesdropping attack [36] and the delay-photon Trojan horse attack [2,3,7]. Bob asks Alice for the positions of the checking photons, and then he randomly chooses one of the two bases \( \{ |0\rangle, |1\rangle \} \) or \( \{ |+, |\rangle \} \) to measure the sample photons in the checking sequence \( S_{AB} \). Bob publishes his measuring bases and results. Alice analyzes the error rate statistically to determine whether there is an Eve on-line. If the channel is secure, Alice and Bob continue to the next step.

3. Encoding Bob’s secret message on the photons in the sequence \( M \): Bob encodes his classical bit 0(1) by performing operation \( I (i \sigma_y) \) to the photons in the sequence \( M \), where \( I = |0\rangle\langle 0| + |1\rangle\langle 1| \) and \( i \sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0| \). To guarantee the security of the quantum channel from Bob to Alice, Bob prepares some single photons randomly in one of the above four non-orthogonal states to form sequence \( S_{AB} \), and then he inserts these single photons randomly into the sequence \( M \). Bob sends the sequence \( S_{AB} + M \) to Alice.

4. Checking the security of the quantum channel from Bob to Alice: Alice and Bob check the security of the quantum channel from Bob to Alice as that in the step 2. If the channel is secure, they continue to the next step.

5. Secret information recovery: Alice measures the photons in the sequence \( M \) with the original bases to get Bob’s secret message, the details are described in Table I. Alice operates on the photons in the sequence \( M \) according to Bob’s secret information as follows: in the situation that Bob’s ith classical bit is 0, if Alice’s measurement result is \( |0\rangle \) or \( |1\rangle \), Alice selects the operation \( I \), if Alice’s measurement result is \( |+\rangle \) or \( |\rangle \), Alice selects the operation \( H \). In the situation that Bob’s ith classical bit is 1, if Alice’s measurement result is \( |0\rangle \)
or $|\bar{1}\rangle$, Alice selects the operation $H$. If Alice’s measurement result is $|+\rangle$ or $|\bar{-}\rangle$, Alice selects the operation $I$, these can be tabulated to table II.

| $|0\rangle$ | $|1\rangle$ | $|+\rangle$ | $|\bar{-}\rangle$ |
|---------|---------|---------|---------|
| 0       | 1       | Null    | Null    |
| $|1\rangle$ | 1       | 0       | Null    |
| $|+\rangle$ | Null    | Null    | 0       | 1       |
| $|\bar{-}\rangle$ | Null    | Null    | 1       | 0       |

In Table I, “Null” means that the situations do not exist. For example, if the initial state of Alice’s preparing photon is $|0\rangle$, Bob encodes his classical bit on the received photons by applying operation $I$ or operation $\sigma$, whose nice feature that the operations just flip the states in both measuring bases and do not change the basis of the states, Alice’s initial state $|0\rangle$ belongs to the rectilinear basis while $|+\rangle$ and $|\bar{-}\rangle$ belong to the diagonal basis, so the situations do not exist.

| $|0\rangle$ | $|1\rangle$ | $|+\rangle$ | $|\bar{-}\rangle$ |
|---------|---------|---------|---------|
| 0       | 1       | 1       | 1       |
| 1       | 0       | 0       | 0       |

After Alice has performed operations on the photons in the sequence $M$ according to Bob’s secret information, it seems that the bases of the photons’ states in the sequence $M$ are uncertain to Bob. However, through the analyzing the Table II, we find that Bob’s secret information has determined the bases of the photons’ states in the sequence $M$ received from Alice, that is, if his secret information is 0, the states of the photons are in the basis $\{|0\rangle,|1\rangle\}$, if his secret information is 1, the states of the photons are in the basis $\{|+\rangle,|\bar{-}\rangle\}$. To check eavesdropping, Alice also prepares some sample photons randomly in one of the above four non-orthogonal states to form sequence $S_{a\rightarrow b}'$, and then inserts these single photons randomly into the sequence $M$. Alice sends the new sequence $S_{a\rightarrow b} + M$ to Bob.

(6) After having ensured the security of the channel from Alice to Bob (the process is similar to that in the step (2) and step (4)). Bob selects a proper measurement basis to measure the photon in the sequence $M$ according to his own secret information. That is, if his ith bit is 0, he selects the basis $\{|0\rangle,|1\rangle\}$, if his ith bit is 1, he selects the basis $\{|+\rangle,|\bar{-}\rangle\}$. Then Bob can learn the XOR value of their secret information with certainty. Thus, he can get Alice’s secret further.

### III. Security Analysis

Up to now, we have presented our quantum dialogue protocol. Now let us analyze the security of the protocol. We know that the secret information is transmitted in the steps 3 and 5, even if Eve can capture the photons in sequence $S_{a\rightarrow b} + M$ or $S_{a\rightarrow b}' + M$, she cannot obtain any secret information as he/she does not know the basis of the initial preparing photons and legitimate dialogue parties’ operations. He/she only can randomly select a basis to measure the photons. In this case, even if Eve only wants to disturb the transmission (i.e., denial of service attack) without considering of being discovered, he/she can’t get any useful information about the messages.

As we know that, the PNS technology in the steps 2, 4 and 6 will make the receivers (Alice and Bob) in our protocol have the ability to distinguish whether each quantum signal in the sequence is a single-photon one or a multi-photon one before they perform any operations on the photons in the sequence. For this end, they can store the quantum signals, after Alice (Bob) has published the positions of the checking photons, Bob (Alice) randomly chooses a subset of the checking photons and then splits each of them to two signals with a PNS, Bob (Alice) measures each signal in the basis $\{|0\rangle,|1\rangle\}$ or in the basis $\{|+\rangle,|\bar{-}\rangle\}$. If the signal is a multi-photon, each measurement will have an outcome.

To make sure that the protocol is secure against to invisible photon eavesdropping attack, we have added filters in each receiver’s laboratory in the protocol. All the senders’ photon pulses should pass through receiver’s filter first. Only wavelengths close to the operating wavelength can be let in. Thus, Eve’s invisible photons can be filtered out by the filter.

In the following, we show that how the protocol can overcome the information leakage problem. Without loss of generality, we suppose that the initial states of the single photons in the sequence $M$ are $|0\rangle$ or $|\bar{-}\rangle$, in other words, the classical bits that Alice wants to transmit to Bob are 01, if Bob’s secret message bits are 10, Bob will apply operation $I$ on the first photon and apply operation $i\sigma$ on the second photon. It is obviously that the states of these two photons in the sequence $M$ will be changed to $|0\rangle$ or $|\bar{+}\rangle$. The photons’ initial basis and Bob’s operations are unknown to Eve. Hence, Eve only can guess the preparing photons’ initial states, the probability that he can succeed in guessing is 1/4. There are two photons in the sequence $M$, each photon is randomly chosen from the set $\{|0\rangle,|1\rangle,|+\rangle,|\bar{-}\rangle\}$, it corresponds to
\[ \sum p_i p_j \log_2 \left( \frac{1}{p_i p_j} \right) = -16 \times \log_2 \left( \frac{1}{16} \right) = 4 \text{ bits}, \]
which is just the biggest uncertainty [38]. So the information leakage problem does not exist.

IV. DISCUSSION

Compared with the previous protocols, such as the NBA protocol [23], MAN protocol [24], XIA protocol [26] and GAO protocols [31], in which the EPR pairs act as quantum channel and the Bell measurement is needed, the proposed scheme in this paper does not require EPR source and Bell measurement, which, in the long run, this will provide many advantages. To realize this scheme, one only needs single photon source and quantum state storage devices, which are all principally available at present. For instance, single photon can be produced in experiments [39, 40], and quantum information storage can be realized through electromagnetic induced transparency [41, 42]. So the present protocol is experimentally feasible within current technologies.

Although JI protocol [25] and YANG protocol [27] are proposed based on single photons, the transmitted information was partly leaked out, any eavesdropper can elicit some information about the secrets from the public announcements of the legal users. This situation contradicts with the main aim of quantum cryptography. We point out that the eavesdropping checking strategy in JI protocol [25] is not advisable, the recipient selects N-1 batches of photons from the N batches and then measures these photons with a randomly choosing basis, it needs N quantum photons to transmit one classical bit, which greatly reduces the efficiency of the protocol.

In fact, our scheme is a variant of YANG protocol [27], we know that one party has to publish the relationship of the classical information in order to make sure that the other party can recover the message in YANG protocol [27], which makes the correlation relationship of the classical information expose to the potential attacker. To solve this problem, we first plan to adopt “one time pad” model [43] for as the communication initiator Alice has got Bob’s message, she can use this message as the secret key to encrypt her message and then transmit the cipher-text to Bob, who can decrypt the cipher-text accurately. However, According to Cabello’s definition of efficiency [44]

\[ \eta = \frac{b_i}{q_i + h_i} \]

where \( b_i, q_i, h_i \) are the secret bits exchanged, the quantum bits used and the classical bits used respectively. The theoretic efficiency only can approach to 50\%, which is a low value. The adoption of “one time pad” model will introduce another problem, that is, the secret key used here is Bob’s secret message, it is not a real random number, so the unconditionally security can’t be guaranteed.

In SHI protocol [32], the only quantum dialogue protocol can overcome the information leakage problem based on single photons as far as we know, it needs 2N photons to transform N bits classical information. In our protocol, it only needs N single photons to transform N bits classical information, except those photons used for eavesdropping check, all the photons can be used for transmitting secret messages. The theoretic efficiency of our protocol can approach to 66.7\%, which is very high for quantum dialogue protocol.

V. CONCLUSION

In summary, we have put forward an efficient quantum dialogue protocol using single photons. The protocol overcomes the information leakage problem existed in most previous quantum dialogue protocols and has a high efficiency for qubits. The protocol is secure against denial of service attack, the delay-photon Trojan horse attack and invisible photon eavesdropping attack. As only single photons are used, the protocol is feasible within current technologies.

REFERENCES

[20] X. H. Li, F. G. Deng, and H. Y. Zhou, “Improving the security of


