International Journal of Security and Its Applications
Vol. 10, No. 12 (2016), pp.97-110
http://dx.doi.org/10.14257/ijsia.2016.10.12.09

Semi-quantum Key Distribution Protocol Based on Bell States

Ting Wang [1,2], Dongning Zhao[3], Zhiwei Sun[4,*] and Weixin Xie[1]

[1]*ATR Key Laboratory of National Defense Technology, Shenzhen University, Shenzhen, China 518060*
[2]*School of Computer Science and Engineering, South China University of Technology, Guangzhou, China 510006*
[3]*College of Information Engineering, Shenzhen University, Shenzhen, China 518060*
[4]*School of Computer Engineering, Shenzhen Polytechnic, Shenzhen, China 518055*
wangt@szu.edu.cn, zhaodongning1979@gmail.com, sunzhiwei1986@gmail.com, wxxie@szu.edu.cn

Abstract

A quantum key distribution protocol with traditional Bob has been proposed recently by Boyer et al. using single-particle state. In this paper, a semi-quantum key distribution protocol is described, in which Einstein-Podolsky-Rosen (EPR) pairs of particles are utilized to generate a secret key in remote places. This extends the quantum key distribution protocol with traditional Bob where the single-qubit channel is replaced by the entangled EPR-pair channel. And quantum Alice is able to do any quantum operations, preparing quantum states and performing quantum measurement, but traditional Bob is not able to prepare and measure a particle in the computational basis, reflect the particles. Furthermore, entanglement states are used in our protocol. The analysis shows that our protocol is secure, which can avoid the beam splitter attack automatically, and the proposed protocol is more efficient than Boyer's scheme.

Keywords: *Quantum Key Distribution; Bell States; Quantum Cryptography*

1. Introduction

Cryptography is a technical science which studies the construction of cryptograph and the analysis of it, studies the objective law of the change of the cryptogram, which mainly studies how to transmit information secretly according to the stipulation of the communication parties. It is also a kind of important secret means to carry out the special transformation of information. Thus far, it is trusted that the only proven unconditionally secure crypto-system is the one-time-pad technique. To employ this technique, the two distant communicating parties must have a secure method to exchange a secret key each other when a message needs to be encrypted. However, it is a very difficult thing to exchange the secret key between the two parties before a communication because they can't use a public channel to send a secret key to the public. Fortunately Bennett-Brassard (BB84) [1] pointed out how to use the properties of quantum mechanics for the purpose of the cryptography, independently rediscovered by Ekert (E91) using entanglement states [2] a few years later, which was the beginning of quantum key distribution (QKD), and had been proven to be unconditionally secure [3] when both parties are quantum. So far, there are many quantum key distribution (QKD) schemes have already been put forward [4, 5, 6, 7, 8, 9].

The basic idea of quantum communication is proposed by Bennett *et al.*, in 1980s and 90s, and it mainly includes quantum key distribution (QKD) and quantum teleportation.

ISSN: 1738-9976 IJSIA

QKD can use quantum mechanics to make sure the communication is safe, which will enable two parties to produce a shared secret key that only they know at random, and it then can be used in encryption and decryption algorithms. QKD can realize the secure classic communication of the point to point way by one-time-pad, where the security has been strictly proved in mathematics, which is can't be done by the classic communication so far. Existing QKD technology can realize quantum key distribution in hundred kilometer scale, and it can also realize quantum key distribution network with the aid of optical switch technology. Taking the BB84 protocol as an example, which is also widely used at present, and the structure of its communication system can be described as Figure 1.

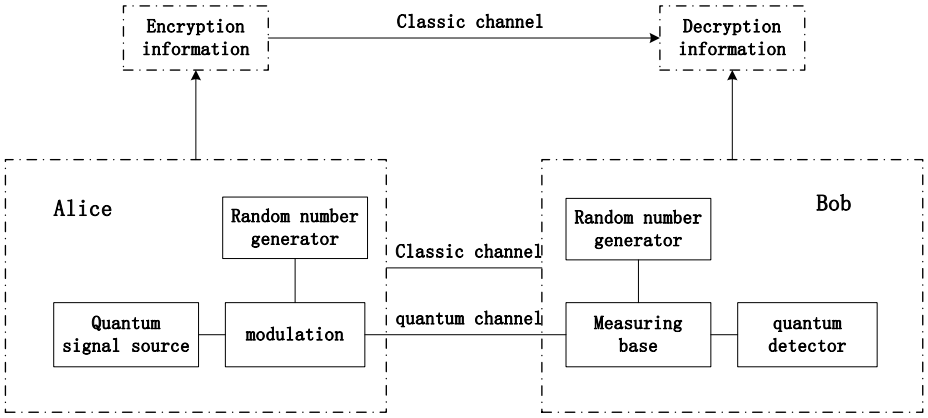

Figure 1. Structure of a Quantum Communication System

As can be seen from Figure 1, the above communication system establishes a point to point connection between two parties, generally named Alice and Bob, which hope to exchange secret keys. The connection can be constructed by the quantum public channel and classical public channel. Alice randomly generates a traditional bit stream and converts them into quantum states, and then sent them to the quantum channel. After receiving these quantum states of light, Bob can carry out some appropriate operations according to different situations, such as reflecting them, measuring and recording the results of the measurement and so on. The traditional public channel is mainly used to verify those correlations. If those correlations are large enough, it can be determined that the signal in the quantum channel is not being tapped by the third party basically.

The development of QKD has mainly experienced four stages [10].

(1) Theoretical scientists proved the security theory of the ideal or semi practical QKD system based on the principle of quantum mechanics. The above security analysis is based on the simplified mathematical physics model of the physical device (light source, channel, detector, etc.) of the two parties. However, these models usually do not match the actual physical devices, or can't simulate the actual physical device used in the QKD system completely. Hence the unconditional security of QKD in theory does not guarantee the security of QKD system in practice.

(2) In order to improve the rate and increase the communication distance continuously, the experimental scientists improved the hardware technology of the quantum key distribution system in succession. At present, QKD has already walked out of the laboratory and being carried out a preliminary practical application, and there are at least three companies in the world are selling the commercial QKD system. For example, the Swiss election has used QKD to encrypt information since 2006, and South Africa's world cup also uses the QKD system to ensure information security in2010.

(3) Find security vulnerabilities in actual QKD system, and improve the software or hardware of the system to resist the actual security vulnerabilities. At present, the development of quantum key distribution is at this stage. How to check the shortcomings and fill the vulnerabilities of the actual security QKD system fully is one of the key research focuses in the current QKD field.

(4) When the security of actual QKD system passes repeated testing and proof, quantum key distribution will be practical for encryption and decryption. In addition, the network of QKD, the QKD from the ground to the satellite, as well as how to communicate the QKD with the traditional optical network communication are also the very concerned problems that hope to be solved. Once the issues described above are resolved, QKD technology will really go to the application.

Since Bennett and Brassard proposed the first QKD protocol BB84 protocol, QKD has become one of the most popular focuses in the quantum field, and also become the most easy to be applied in the quantum field, the most close to the actual technology. QKD depends on the physical characteristics of the quantum to ensure its theoretical security, but not to set any restrictions on the ability of Eve. However, most of the quantum key distribution protocols require that both the two sides have quantum capacity, but this often requires the use of tens of millions of quantum generating devices and operating equipment, which makes a lot of users feel afraid. So how to maximize the advantages of quantum cryptography, and how to reduce the cost, expand the application is becoming the primary task of the quantum research.

What will happen when one party (Alice) has a quantum capacity and the other (Bob) is only a traditional one? In this case, how do the two sides need to interact? Can they complete the key distribution? If they can, is the key distribution protocol secure?

Lately, several semi-quantum key distribution protocols (SQKD) [11–13] were proposed. For example, Boyer, Kenigsberg and Mor [11] introduced the idea of semi-quantum key distribution using four quantum states firstly, and for convenience we refer to the protocol as BKM2007. The literature [11] put forward two QKD protocols with the constraint that one party only has the traditional ability, and proved the robustness of their protocols against attacks, namely, any attempt by the third party to obtain information will inevitably lead to some errors, which makes the legitimate users can discover the attack behavior. Subsequently Zou and Qiu *et al.*, [13] has simplified the work of Boyer et al., namely, proposed a simplified version which only requires one quantum state, for convenience we refer to the protocol as ZQLWL2009. Zou *et al.*, mainly proposed several different SQKD schemes in which one party can send three, two and one quantum states respectively, and the analysis showed these protocols are also completely robust.

Compared with the classical protocol, in order to achieve a significant advantage, these protocols give an answer to how much “quantumness” a protocol is required to be. In these SQKD protocols, information passes through the quantum channel from Alice to the outside world, and then returns to Alice from the outside, where Bob can obtain a part of the channel information, no matter what time a qubit goes through the corresponding channel Bob can either choose to do nothing, or do one of the following two things: (1) Measuring the qubit in the computational basis $\{|1>, |0>\}$, the basis is also named “traditional” basis; (2) Reselecting a new qubit in the traditional basis and then send it. Bob is called traditional Bob If he is constrained to do only the processes (1) and (2), or do nothing and will not get any information of the quantum superposition of the computational basis states. If all the parties are traditional, Alice and Bob will use qubits to perform related operations in the traditional basis which would make the corresponding scheme be equivalent to an old-fashion traditional scheme, thus these operations themselves are considered to be traditional. So this kind of protocol is termed “QKD with traditional Bob” or “Semi-quantum key distribution (SQKD)”, and whose running environment can be described as Figure 2.

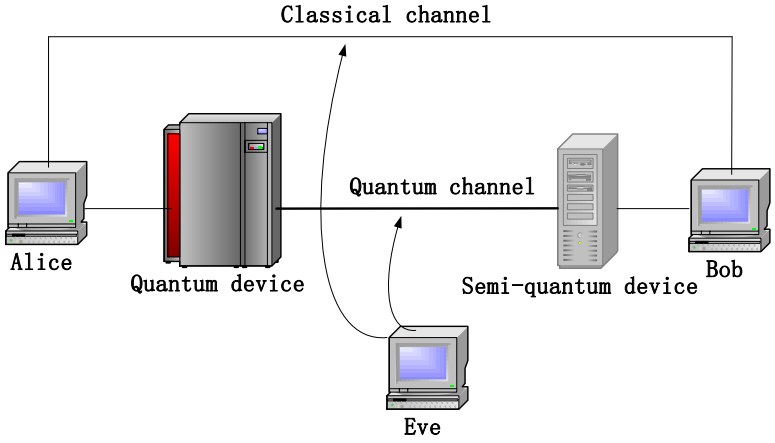

Figure 2. The Running Environment of a SQKD Protocol

It is proved that the SQKD protocols [11–13] is completely robust, which is the key step in the security analysis of their protocol. We say a protocol is robust if any attempt by the third party to obtain the information of the INFO string (prior to Alice and Bob performing the error correction code operation) will inevitably lead to some errors, which makes the legitimate users can discover the attack behavior. Especially, Boyer, Kenigsberg and Mor [11] divided the robustness into three kinds of cases: completely robust, partly robust, and completely nonrobust.

BKM2007 and ZQLWL2009 have the same drawbacks: the source of the photon is formed by the attenuated laser pulse, which contains more than two photons with a nonzero probability in practical, so this can cause the system be attacked by a beam splitter which has been discussed in the literature [14]. Using entangled photon pairs from parametric down-conversion, we are able to simulate a conditional single photon source [15] with a higher bit rate [16], while with a lower probability to produce multiple pairs of photons simultaneously. Therefore, the beam splitter attack can be automatically avoided, and the protocol is more efficient than BKM2007. On the other hand, because of the important study on the teleportation of the unknown quantum states [17], superdense quantum coding in communication [4] and QKD from Bell States [2]. At present, entangled states in multiple quantum systems have been widely considered as a very important resource in quantum communication and complex computation [18, 19], which has further stimulated the considerable interest of the quantum researchers on the SQKD protocol using Bell states.

The remainder of the paper is organized as follows. In Section 2, we put forward an efficient SQKD protocol using Bell state which exploits the properties of the entangled photon pairs generated by quantum generator with high security key. In Section 3, the security of proposed protocol is discussed completely. In Section 4, we make an efficiency comparison with the BKM2007 and ZQLWL2009 protocols in detail. Finally, Section 5 discusses and concludes the paper briefly.

2. Scheme for QKD with traditional Bob

In order to allow Alice and Bob to exchange a truly secret key while preventing a eavesdropper from learning something about the shared key in the presented protocol, two fundamental tools will be incorporated: error correction code and privacy amplification.

Error correction codes enable reliable delivery of traditional information over unreliable communication channels. In practice, communication channels are subject to various unavoidable noises, and thus errors may be introduced during transmission. Error correction codes provide a way of detecting and correcting errors. Since it was discovered

in the 1950s, the error correction code has become an important subject, and a variety of different traditional error correction protocols have been put forward [20]. In this paper, the code [21] introduced by Sipser is used, and it is able to correct a constant part of the error efficiently with constant information rate.

In 1988 Bennett, Brassard and Robert *et al.*, [22] firstly proposed privacy amplification, which can be used to transform a longer partly-secret string Z, where the adversary may have some information about the string, into a shorter and more confidential one K based on open discussion. An excellent and simple privacy amplification protocol is to compute the secret key K and consider the result as the output of a public selected two-universal hash function [23]. A class F of hash function from $\{0,1\}^n$ to $\{0,1\}^l$ can be called two-universal, if $\forall y, y^{'} \in \{0,1\}^n$ $(y \neq y^{'})$ and uniformly distributed f over F, we have

$$\Pr[f(y) = f(y^{'})] \leq \frac{1}{2^l}.$$

For example, suppose that F is a two-universal hash function from the definition domain Z to the value range $\{0,1\}^l$, and l represents the length of the secret key K. First of all, one participant chooses an instance of F at random, and then announces the instance to another participant publicly. Then, both participants obtain a high-security secret key $K = F$ (Z). This simple method has been shown that, even though the third party has partial traditional information on Z, it can also yield a secret key *K*, and it is asymptotically optimal about the secret key *K* [22, 24]. In the presented protocol, the above simple method will be used.

2.1. Security Requirements

To define the security of the scheme, we can refer to the security definition put forward by Boyer et al. in Ref. [11]. We generally say a scheme is secure (also known as complete robust), if nonzero information obtained by the third party on the quantum information string (prior to error correction code operation performed by Alice and Bob) will inevitably lead to some errors, which makes the legitimate users can discover the attack behavior through bits test. Here we prove that our protocol based on the Bell state is completely robust.

2.2. Semi-quantum Key Distribution Using Bell State

As one of the most important resources in the processing of quantum information, the application value of quantum entanglement in quantum secure communication mainly appears as two aspects: On the one hand the shared quantum key can be realized directly based on entanglement distribution. On the other hand, it mainly appears the basis of remote quantum communication based on quantum repeater. The traditional quantum entangled state is a linear superposition state of the two photon states. As the two photons can be located at different locations in space, entangled photons can form a non-traditional correlation with different regions, and this correlation can be used for secret Key sharing directly.

To propose our key distribution protocol, first of all we describe simply the four polarization entangled states:

1) $|\phi^{+}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$;

2) $|\phi^{-}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$;

3) $|\varphi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$;

4) $|\varphi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$.

Which are created directly using the parametric down-conversion by the method described in Ref. [13]. $|\phi^\pm\rangle$ and $|\varphi^\pm\rangle$ are also known as Bell or EPR state. The concrete steps of the SQKD protocol using Bell state are described as follows.

(1) Quantum Alice and traditional Bob let the Bell state $|\phi^\pm\rangle$ and $|\varphi^\pm\rangle$ stand for a bit traditional information '0' and '1' separately.

(2) Alice randomly selects a set of ordered $N = 4n(1+\delta)$ EPR pairs on quantum state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, where n represents the required length of the INFO string, $\delta > 0$ represents a fixed parameter, and then Alice transforms the ordered EPR pairs to two partner-photon sequences $[P_1(H), P_2(H), \cdots, P_N(H)]$ and $[P_1(T), P_2(T), \cdots, P_N(T)]$, where $P_i(H)$ and $P_i(T)$ are two interconnected photons in the ith $(i = 1, \cdots, n)$ EPR pairs. We call $[P_1(H), P_2(H), \cdots, P_N(H)]$ the home sequence or simply the H-sequence, and the other sequence is called travel sequence or the T-sequence for short.

(3) For each qubit in the H-sequence, Alice randomly selects whether to apply the Pauli operation $X = |0\rangle\langle 1| + |1\rangle\langle 0|$ or to do nothing. We notice that by performing the Pauli operation *X*, it transforms the state $|\phi^+\rangle$ into $|\varphi^+\rangle$. Then she stores the H-sequence and returns it to traditional Bob using a quantum channel.

(4) After receiving a qubit, Bob can choose either to reflect it at random (we name the operation as "CTRL") or to measure the qubit in the computational basis $\{|1>, |0>\}$, the basis is also named "traditional" basis and then send it again with the original state (we name the operation as "to SIFT it"). He records the results of the measurement which is completely secret to any other person. Qubits are sent one after another, i.e., only when Alice receives the previous qubit, she sends a qubit, and Bob resends a qubit at once when he receives it.

(5) Alice uses an *N*-qubit recorder to save all the photons back from Bob. Then she announces it through a public traditional channel.

(6) After hearing from Alice, Bob declares which qubits he chose will be performed the operation CTRL, and it is hoped that for approximately *N/2* qubits of T-sequence, Bob will choose to reflect them at random. We refer to these qubits as T_{CTRL}, and the corresponding qubits in the H-sequence is called H_{CTRL}. We refer to the qubits Bob chose to perform the operation SIFT as T_{SIFT}, and the correlated partner-photon is H_{SIFT}. If the number of the T_{SIFT} bits is no more than 2n, they will exit the protocol, but this appears as a very small probability.

(7) Alice checks the error rate of the T_{CTRL} in the following way. She makes Bell measurement on the CTRL qubit (qubit in the T_{CTRL}) and corresponding home qubit (qubit in the H-sequence), and compares the measurement result with the corresponding initial EPR state. If they are unequal, some errors may happen. If the error rate on the T_{CTRL} is higher than a predetermined threshold P_{CTRL}, Alice exits the protocol, otherwise proceed to the next step.

(8) Alice measures particles of H_{SIFT} and particles of T_{SIFT} in the computational basis, and chooses randomly *n* H_{SIFT} to be TEST qubits, then announces the positions of the

TEST qubits. Bob announces the results of his measurement (of T_{SIFT}) corresponding to the TEST qubits. Alice makes a careful analysis of these results of the measurements. If they are indeed perfectly correlated, Alice and Bob can certain that the protocol has not been attacked by the third party. Otherwise they quit the protocol immediately.

(9) Alice announces the measurement results of the remaining H_{SIFT}. Bob obtains the raw key by comparing the measurement results of H_{SIFT} and T_{SIFT}, which is shown clearly in Table 1. Where IS denotes Initial state, MR_H denotes Measurement result of H_{SIFT}, MR_T denotes Measurement result of T_{SIFT} and, RK denotes Raw key. For instance, if the measuring result of H_{SIFT} is '0', and the corresponding result on that of T_{SIFT} is also '0' which is only known by Bob, then Bob can deduce the initial state is $|\phi^+\rangle$. And therefore, they can share a secret raw key '0'. Both of them choose the first *n* raw key to be acted as information string.

Table 1. Relations of the Initial State, Measurement Results and Raw Key

IS	MR_H	MR_T	*RK*
$\|\phi^+\rangle$	0	0	0
$\|\varphi^+\rangle$	0	1	1
$\|\phi^+\rangle$	1	1	0
$\|\varphi^+\rangle$	1	0	1

(10) At last, Alice publishes error correcting code that can be used to modify the errors on the information string, and privacy amplification which can be used to generate a much shorter and highly secret key from the information string by transformation. They both use their information to extract the last *l*-bit secret key from the *n*-bit information string. For example, Alice selects a hash function *F* at random, which is from the definition domain $\{0,1\}^n$ to the value range $\{0,1\}^l$, and she publishes *F* to Bob. Then both of them can calculate the final secret key *k* through applying *F* to the information string, *i.e.*, $K = F(INFOstring)$.

3. Security Analysis

Quantum key distribution can make use of the principle of quantum mechanics to realize the unconditional security between the two sides of the communication, in which unauthorized third party can't eavesdropping on the key transmission. Even though the third party controls infinite computing power and storage capacity, this technology is also unconditionally secure. At present, single photon QKD protocol, entangled photon pair QKD protocol and continuous variable QKD protocol etc. have been proved to be unconditionally secure under the assumption of ideal light source, channel and detection model. But the unconditional security of these protocols requires three preconditions: (1) Experimental equipment (including single photon source, measurement devices, *etc.*) must be ideal, and can be trusted; (2) The third party can't get any information from the Bob or Alice labs; (3) The classical communication channel is available for authentication.

Now, let we analyze the security of the proposed protocol. Firstly, when Alice sends T-sequence to Bob, an eavesdropper Eve who wants to get the information of the initial states, can intercept the particle and then resend a false particle instead the original particle according to his measurement results. Because the state of particle about T-sequence is

$$\rho_{T_i} = Tr_{H_i}(\rho_{H_iT_i}) = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \frac{I}{2} \quad (1)$$

where $i = 1, \cdots, N$. The state of the particle is not dependent on the initial entangled state, and all the measurements result carried out by the third party will not have the information of the initial state, which prevents Eve from knowing the secret key. On the other hand, we show that if the third party sends a false information to Bob, for instance, this false information is in the state $|\varphi_E\rangle = d|1\rangle + c|0\rangle$, where $|c|^2 + |d|^2 = 1$, she will be detected by eavesdropping check. As if Bob chooses to reflect it, the state of the home particle and the false information is

$$\rho_{HE} = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) \otimes (c^* d|1\rangle\langle 0| + cd^*|0\rangle\langle 1| + c^2|0\rangle\langle 0| + d^2|1\rangle\langle 1|) \quad (2)$$

When Alice and Bob make eavesdrop checking, Alice makes a Bell measuring for the home particle and false information, and she will have the same probability to get any one of the four Bell states with the equal probability, namely that is 1/4. So the error rate caused by the third party is $\frac{3}{4}$.

Furthermore, the most common attack from Eve is usually represented by a unitary operator U_E, whose main role is to make the EPR particles and Eve auxiliary system entanglement. By the subsequent measurement of the auxiliary system, Eve can get the information of EPR system. The most general global state before Bob decides whether to SIFT or CTRL is of the form

$$|\Phi\rangle = |00\rangle_{HT}|A\rangle_E + |01\rangle_{HT}|B\rangle_E + |10\rangle_{HT}|C\rangle_E + |11\rangle_{HT}|D\rangle_E \quad (3)$$

where $|A\rangle, |B\rangle, |C\rangle$ and $|D\rangle$ are the selections of Eve for her system states, in which she doesn't have to make up her mind how to measure the corresponding particle states until both of them have been published.

Suppose the initial state Alice preparing is $|\phi^+\rangle$. Eve applies the unitary operation U_E to the qubit sent to Alice from Bob. If Bob chooses to measure, record the result and send it again, the global state before Eve's application U_E is $|00\rangle_{HT}|A\rangle_E + |11\rangle_{HT}|D\rangle_E$. Once Eve has applied U_E, it must be such that $U_E|00\rangle_{HT}|A\rangle_E = |00\rangle_{HT}|E_0\rangle_E$, or Eve's attack can be detectable, and similarly, $U_E|11\rangle_{HT}|D\rangle_E = |11\rangle_{HT}|E_1\rangle_E$. Because of the linear features of quantum mechanics, if Bob chooses to reflect it (CTRL), then the final quantum state must be must be $U_E|\Phi\rangle = |00\rangle_{HT}|E_0\rangle_E + |11\rangle_{HT}|E_1\rangle_E$. As $U_E|\Phi\rangle = |\phi^+\rangle_{HT}(|E_0\rangle_E + |E_1\rangle_E) + |\phi^-\rangle_{HT}(|E_0\rangle_E - |E_1\rangle_E)$ and $|\phi^-\rangle_{HT}$ have probability 0 of being measured by Alice, $|E_0\rangle_E = |E_1\rangle_E$ must hold.

Similarly, if the initial state is $|\varphi^+\rangle$, Eve applies the unitary operation U_E to the qubit sent to Alice from Bob. If Bob chooses to measure, record the result and send it again, the global state before Eve's application U_E is $|01\rangle_{HT}|B\rangle_E + |10\rangle_{HT}|C\rangle_E$, Once Eve has applied U_E, it must be such that $U_E|01\rangle_{HT}|B\rangle_E = |10\rangle_{HT}|E_0\rangle_E$, or Eve's attack can be detectable, and similarly, $U_E|10\rangle_{HT}|C\rangle_E = |10\rangle_{HT}|E_0\rangle_E$. Because of the linear features of quantum mechanics, if Bob chooses to reflect it (CTRL), then the final quantum state must be must be $U_E|\Phi\rangle = |10\rangle_{HT}|E_0\rangle_E + |01\rangle_{HT}|E_1\rangle_E$. As $U_E|\Phi\rangle = |\varphi^+\rangle_{HT}(|E_1\rangle_E + |E_0\rangle_E) + |\varphi^-\rangle_{HT}(|E_1\rangle_E - |E_0\rangle_E)$ and $|\phi^-\rangle_{HT}$ have probability 0 of being measured by Alice, $|E_0\rangle_E = |E_1\rangle_E$ must hold.

If the original state is $|\phi^+\rangle_{HT}$, the final state must be $U_E|\Phi\rangle = |\phi^+\rangle_{HT}|E_0\rangle_E$. If the original state is $|\varphi^+\rangle_{HT}$, the final state must be $U_E|\Phi\rangle = |\varphi^+\rangle_{HT}|E_0\rangle_E$. Hence only those particles that are not associated with EPR particles in the Eve system can pass the check of legitimate users, so that Eve can't get any information from her subsequent measurements on it.

In the imperfect quantum channel, the protocol is sensitive to the noise, and some errors may happen on the INFO string. The situation can be handled by the relevant error correction techniques (such as error correcting code). In the final step of the protocol, Alice returns an overview of the characteristics of the error correction code and the corresponding information string to Bob, the supplemental information make Bob can restore the true information string from its noisy version by standard methods. On the other hand, if Eve uses the same basis as Bob to measure the SIFT qubits, she will gain a certain amount of information of the INFO string without being detected. So to reduce Eve's partial information about the INFO string, the privacy amplification technique is needed. Using the above mentioned privacy amplification method from the two-universal hash function, both of them can exchange a highly secret key, that is to say, privacy amplification can transform the partially secure INFO string to a highly secure key by announcing a two-universal random function from $\{0,1\}^n$ to $\{0,1\}^l$ using the public communication channel.

However, there are some hidden safety problems in the actual QKD system, which will result in the following two results: (1) The existing theoretical security analysis can't be applied to the actual QKD system directly, the security of the actual QKD system can't be proved, and its security code rate can't be accurately estimated; (2) The third party can use the security vulnerabilities that has not been included in the analysis of theoretical security in the actual physical device to steal information, and it's hard to be found. In short, the majority of QKD experimental devices are not ideal in the experiment, and these non ideal experimental devices may result in the information leakage of the side channel etc. On the basis of this, the secret information can be obtained by the third party who can't be detected by the legal communication party. Therefore, how to resist the side channel attacks based on experimental devices has become the top priority of the security analysis of QKD protocol.

4. Efficiency Analysis

A SQKD scheme based on Bell state is put forward in this paper, and the security of this scheme is guaranteed by a special technique, namely, the technique of generating the entangled photon pairs from parametric down-conversion. The scheme also involves entanglement swapping, which can improve the efficiency of QKD scheme. Overall, the scheme has the following characteristics.

(1) The efficiency of the key distribution is improved. The efficiency of the previous QKD protocol distribution is relatively low. For example, in the BB84 protocol, the probability of the communication between the two parties using the same basis is 1/2, that is, up to only 1/2 of the particles can be used to get the key. In the EPR protocol, the probability of the two parties using the same basis is only 2/9, and the rest of the particles are used in the Bell theory to detect whether exist the eavesdropping on the quantum information is.

(2) It uses the properties of quantum physics to solve the problem of the security and efficiency of the protocol. The protocol does not use the classical cryptography method to check the identity of the communication or the messages of the transfer. Instead, the techniques of entanglement state, error correction and privacy amplification are fully

utilized, where the entanglement state of particles are used to distribute the secret key, and the latter two are used to ensure the security of information.

(3) It reduces the requirements for the channel and the device. The proposed protocol reduces the equipment cost of quantum communication system, further plays the advantage of quantum cryptography. So that it is more close to the practical application and the related techniques are also much easier to be achieved.

Our protocol is efficient in that it uses all Bell states to distribute the key except those, approximately half of the Bell states, chosen for checking eavesdropping. This is different from the BKM2007 where only $\frac{3}{4}$ of the particles are used as keys. We now study the efficiency of the protocol. Here we consider the efficiency definition introduced by Cabello in Ref. [25],

$$\eta = \frac{b_s}{q_t + b_t} \tag{4}$$

where b_s represents the length of the corresponding information string, q_t represents the number of the quantum bits transmitted over a quantum channel, and b_t represents the number of the bits transmitted over the classical channel. From analysis it is easy to know that the efficiency of the proposed protocol (approximate $\frac{1}{8}$) is more efficient than that of the BKM2007 protocol (about $\frac{1}{16}$) and not lower than that of the ZQLWL2009 protocol (about $\frac{1}{8}$), which is shown in Table 2.

From the perspective of theoretical research, the proposed protocol has made a new and interesting development for the idea of Boyer et al.'s protocol based on Bell state, and gives an efficient and secure protocol; But from the point of view of practical application it may be difficult to realize because constructing a reliable quantum memory in the experimental quantum physics is still a main research goal [26–28], and current technology allowing storage time is still limited. In the future, we would like to explore the problems when implementing semi-quantum key distribution in the practical scenario. In conclusion, the entanglement of multiple quantum systems has been recognized as a very useful resource for quantum communication and fast computation, which motivates the considerable interest of more quantum cryptography researchers in the study of semi-quantum key distribution protocols based on the Baer state using Bell states, and this kind of protocol can avoid the beam splitter attack automatically. Furthermore, it has also been shown to be secure for a general attack. The efficiency analysis shows that the proposed protocol is more efficient than the BKM2007 protocol. Although it is as efficient as ZQLWL2009, only single-particle states is used in ZQLW2009.

Table 2. Efficiency of BKM2007, ZQLWL2009 and our Protocol

	q_t	b_s	b_t	Efficiency
BKM2007	$8n$	n	$8n$	$\frac{1}{16}$
ZQLWL2009	$4n$	n	$4n$	$\frac{1}{8}$
Our protocol	$4n$	n	$4n$	$\frac{1}{8}$

With regard to the specific implementation, our protocol requires Bell state analysis. On the one hand, although the Bell measurement has not been solved in a general sense, but it has been implemented on certain techniques. In fact, entanglement swapping has already been implemented. So with the rapid development of quantum cryptography, our protocol is expected to be implemented under the current technical conditions.

5. Conclusion and Expectation

Based on the important works on quantum secret key distribution [2], quantum teleportationc[17] and superdense coding [4], we put forward a SQKD scheme by using Bell states, in which the EPR pairs of particles can be used to generate a secret key in remote locations, and it extends the QKD protocol with traditional Bob where the single-qubit channel is replaced by the entangled EPR-pair channel. The robustness of the proposed scheme is discussed. We also have compared with Boyer's protocol and Zou's protocol in the Efficiency Analysis part of the paper, and given the security analysis according to the Boyer's robust definition in section. Using the entangled photon pairs as generated by parametric down-conversion, the beam splitter attack can be automatically avoided. From this point of view, the security of our scheme is stronger than that without Bell states. At the same time, we also present the comparison with other similar protocols in efficiency analysis, analysis shows that the proposed distribution protocol is efficient than BKM2007 scheme; although it is as efficient as ZQLWL2009, ZQLWL2009 is subject to the beam splitter attack. The presented protocol with Bell state can avoid the beam splitter attack automatically.

The physical realization of the existing quantum secret communication is mostly based on the weak coherent light of the single photon level and the communication of entangled optical. The main hardware technologies include the weak coherent light source, entangled light source, transmission and detection, and the software aspect also includes the techniques of the final code extraction (coding). The main index to estimate a system's advancement is the ability to generate the secure final code. The final secure code per second generated from a system is proportional to the system repetition rate and per pulse rate. In addition to the error code rate and loss rate, the bit rate of each pulse is determined by the refinement and coding technology. At present, the error rate can be reduced from many aspects, such as improving the quality of light source coding, channel transmission, as well as synchronous detection, detector efficiency, etc.

So far, the security of classical secure communication has not been proved by mathematics. However, we can realize the secure communication of strict mathematical proof by using the quantum mechanism. Although the key distribution distance reported by the existing system with weak coherent state as the source is not secure, but we still have other ways to solve the problem. The existing technology has been able to achieve the absolute security of quantum cryptography system, such as the decoy state method and the distribution method of entanglement pair, etc. In the future, the development of the ideal single photon source or entanglement source technology will greatly improve the efficiency and the practical performance of the quantum cryptography system. With the method of the quantum entanglement, the quantum relay technology based on refinement, transformation and storage will eventually realize the secure arbitrarily remote quantum communication and communication network.

Acknowledgments

This work is supported by the National Science Foundation of Guangdong Province (2015A030310172), the Science and Technology Innovation Projects of Shenzhen (ZDSYS20140430164957660, JCYJ20150324141711562, JCYJ20150324141711665, JCYJ20150324140036830, GJHZ20160226202520268).

References

[1] C, H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing", In Int. Conf. on Computers, Systems and Signal Processing, India, Bangalore, December, **(1984)**, pp. 175-179.
[2] A.K. Ekert, "Quantum cryptography based on bell's theorem", Physical review letters, vol. 67, no. 6, **(1991)**, pp. 661-663.
[3] P.W. Shor and J. Preskill, "Simple proof of security of the bb84 quantum key distribution protocol", Physical review letters, vol. 85, no. 2, **(2000)**, pp. 441-446.
[4] C.H. Bennett and S.J. Wiesner, "Communication via one-and two-particle operators on einstein-podolsky-rosen states", Physical review letters, vol. 69, no. 20, **(1992)**, pp. 2881-2884.
[5] C.H. Bennett, "Quantum cryptography using any two nonorthogonal states", Physical Review Letters, vol. 68, no. 21, **(1992)**, pp. 3121-3124.
[6] L. Goldenberg and L. Vaidman, "Quantum cryptography based on orthogonal states", Physical Review Letters, vol. 75, no.7, **(1995)**, pp. 1239-1250.
[7] M. Koashi and N. Imoto, "Quantum cryptography based on split transmission of one-bit information in two steps", Physical review letters, vol. 79, no. 12, **(1997)**, pp. 2383-2386.
[8] N.L. Piparo and M. Razavi, "Long-distance trust-free quantum key distribution", IEEE Journal of Selected Topics in Quantum Electronics, vol. 21, no. 3, **(2014)**, pp. 1-8.
[9] D. B. Soh, C. Brif, P.J. Coles, N. Lutkenhaus, R.M. Camacho, J. Urayama and M. Sarovar, "Self-referenced continuous-variable quantum key distribution protocol", Physical Review X, vol. 5, no. 4, **(2015)**, pp. 041010.
[10] V. Scarani, H. Bechmann-Pasquinucci, J. Cerf N, et al. "The Security of Practical Quantum Key Distribution", Rev. Mod. Phys. vol. 81, no.3, **(2009)**, pp. 1301-1350.
[11] M. Boyer, D. Kenigsberg and T. Mor, "Quantum key distribution with classical bob", Physical Review A, vol. 99, **(2007)**, pp. 140501.
[12] M. Boyer, R. Gelles, D. Kenigsberg and T. Mor, "Semiquantum key distribution", Physical Review A, vol. 79, no.3, **(2009)**, pp. 032341.
[13] X. Zou, D. Qiu, L. Li, L. Wu and L. Li, "Semiquantum-key distribution using less than four quantum states", Physical Review A, vol. 79, no. 5, **(2009)**, pp. 052312.
[14] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, "Experimental quantum cryptography", Journal of cryptology, vol. 5, no.1, **(1992)**, pp. 3-28.
[15] P.G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A.V. Sergienko and Y. Shih, "New high-intensity source of polarization-entangled photon pairs", Physical Review Letters, vol. 75, no. 24, **(1995)**, pp. 4337-4341.
[16] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter and A. Zeilinger, "Quantum cryptography with entangled photons", Physical Review Letters, vol. 84, no. 20, **(2000)**, pp. 4729-4732.
[17] C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres and W.K. Wootters, "Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels", Physical review letters, vol. 70, no. 13, **(1993)**, pp. 1895-1899.
[18] C.A. Fuchs, "Nonorthogonal quantum states maximize classical information capacity", Physical Review Letters, vol. 79, no. 6, **(1997)**, pp. 1162-1165.
[19] D. Gottesman and I.L. Chuang, "Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations", Nature, vol. 402, no. 6760, **(1999)**, pp. 390-393.
[20] W.C. Huffman and V. Pless, "Fundamentals of Error-correcting Codes", Cambridge university press, New York, **(2003)**.
[21] M. Sipser and D.A. Spielman, "Expander codes", IEEE Transactions on Information Theory, vol. 42, no. 6, **(1996)**, pp. 1710-1722.
[22] C.H. Bennett, G. Brassard and J. Robert, "Privacy amplification by public discussion", SIAM journal on Computing, vol. 17, no. 2, **(1988)**, pp. 210-229.
[23] J. CARTER, "Universal classes of hash functions", Journal of Computer and System Sciences, vol. 18, **(1979)**, pp. 143-154.
[24] C.H. Bennett, G. Brassard, C. Crepeau and U.M. Maurer, "Generalized privacy amplification. Information Theory", IEEE Transactions on Information Theory, vol. 41, no. 6, **(1995)**, pp. 1915-1923.
[25] A. Cabello, "Quantum key distribution in the holevo limit", Physical Review Letters, vol. 85, no. 26, **(2000)**, pp. 5635-5638.
[26] B. Julsgaard, J. Sherson, J.I. Cirac, J. Fiurasek and E.S. Polzik, "Experimental demonstration of quantum memory for light", Nature, vol. 432, no. 7016, **(2004)**, pp. 482-486.
[27] J. Appel, E. Figueroa, D. Korystov, M. Lobino and A. Lvovsky, "Quantum memory for squeezed light", Physical review letters, vol. 100, no.9, **(2008)**, PP. 093602.
[28] C. Schaffner, "Simple protocols for oblivious transfer and secure identification in the noisy-quantum-storage model", Physical Review A, vol. 82, no.3, **(2010)**, pp. 032308.

Authors

Ting Wang, he received his B.S. degree in applied mathematics from Qufu Normal University in 2003, received his M.S. degree from Wuhan University, Wuhan, China, in 2006, and received his Ph.D. degree from Shenzhen University, Shenzhen, China, in 2014. He is currently a postdoctoral researcher in ATR Key Laboratory of National Defense Technology, College of Information Engineering, Shenzhen University. His research interests include public key cryptography and information security.

Dongning Zhao, she received her B.S. and M.S. in communication engineering from Nanjing Institute of Communication Engineering, Nanjing, China, in 2001 and 2004, respectively, received her Ph.D. degrees in signal and information processing from Shenzhen University, Shenzhen, China, in 2015. She is currently a postdoctoral researcher in College of Information Engineering, Shenzhen University. Her research interests include multimedia security, information hiding and digital watermark.

Zhiwei Sun, he received his B.S. degree in the science of information computation from Shandong Technology and Business University in 2008, received his M.S. and Ph.D. degrees in computer software and theory from Sun Yat-sen University, Guangzhou, China, in 2014. He is currently working as a teacher in School of Computer Engineering, Shenzhen Polytechnic. His research interests include quantum computing and quantum key agreement protocol, etc.

Weixin Xie, he received his B.S. from Xi'an Military Telecommunication Engineering Institute, Xi'an, China, in 1965. From 1981 to 1983, he was a visiting scholar with University of Pennsylvania, Philadelphia, USA. And from 1989 to 1990, he was a visiting professor with University of Pennsylvania, Philadelphia, USA. He is currently a professor with ATR National Defense Technology Key Laboratory, College of Information Engineering, Shenzhen University. He has published more than 100 papers in the journals. His research interests include intelligent information processing and sensor network, etc.