IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 3, 2019, accepted August 19, 2019, date of publication August 23, 2019, date of current version September 9, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2937101

One Step Quantum Key Distribution Protocol Based on the Hyperentangled Bell State

YANYAN HOU[1,3], JIAN LI[2,3], HENGJI LI[3], CHAO-YANG LI[3], YUGUANG YANG[4], NA WANG[3], AND ZHENGYAN ZHOU[3]

[1]College of Information Science and Engineering, Zaozhuang University, Zaozhuang 277160, China
[2]Center for Quantum Information Research, Zaozhuang University, Zaozhuang 277160, China
[3]Beijing University of Posts and Telecommunications, School of Computer Science, Beijing 100876, China
[4]School of Computer Science, Beijing University of Technology, Beijing 100124, China

Corresponding author: Yanyan Hou (hyy@uzz.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant U1636106, in part by the Natural Science Foundation of Beijing under Grant 4182006, and in part by the China Postdoctoral Science Foundation under Grant 2019M650020.

ABSTRACT Considering the security and efficiency of quantum communication system, one step quantum key distribution protocol based on hyperentangled Bell state is proposed. Every 6 classical bits are divided into a group, which are encoded by single particle and hyperentangled Bell state, the sender Alice sends them to receiver Bob, Bob randomly selects the position of hyperentangled Bell state to measure and detects the existence of eavesdropper Eve by comparing measurement results in his hand and transmitted by Alice. Quantum key distribution protocol based on grouping is proposed to solve the storage problem of quantum information and improve the maneuverability, a security analysis is calculated under the intercept-measure-resend attack which introduce at least an error rate of 46.875%, if Eve wants to get all the information, the probability of detection eavesdropping under the entanglement-measure attack is 93.75%, so it proves that proposed protocol does not need to store the quantum state and asymptotically secure under intercept-measure-resend attack and entanglement-measure attack.

INDEX TERMS Entanglement-measure attack, hyperentangled bell state, intercept-measure-resend attack, quantum key distribution, single particle.

I. INTRODUCTION

With the development of information technology, traditional cryptographic security based on the conjectured difficulty of computing functions is challenged enormously. Quantum cryptography different from traditional cryptography, based on the theory of quantum physics, can provide a new way for ensuring communication safety, more and more researchers have focused on quantum communication research. Quantum communication includes quantum key distribution (QKD), quantum secure direct communication (QSDC), quantum secret sharing (QSS) et al. QKD protocol provides a way to obtain unconditional security key based on Heisenberg uncertainty principle and quantum non-cloning theorem, it allows two remote authorized parties to share a secret key by quantum channel and transmit information by classical channel, so it is widely used in practical applications, QSDC protocol is designed for providing directional information communication only by quantum channel.

In 1984, Bennett and Brassard proposed the first QKD protocol BB84 [1]. Many researchers began to research QKD protocol since BB84 is proposed, Ekert proposed E91 protocol [2], Bennett proposed E92 protocol [3]. SARG04 protocol is regarded as an improved BB84 protocol, which can well resist particle beam separation attack [4]. In recent years, quantum secure direct communication (QSDC) was put forward and studied by many researchers, Bostrm and Felbinger [5] presented a famous QSDC protocol called original ping pong protocol (OPP) in 2002, which greatly promoted the development of quantum secure direct communication. In QSDC protocol, secret information instead of secret key is transmitted by quantum channel, the security requirements are more stricter than QKD protocol, researchers have found much vulnerability with ping pong protocol [6]–[19]. Compared with QSDC protocol, QKD protocol only transmits key information by quantum channel with lower security

The associate editor coordinating the review of this article and approving it for publication was Bora Onat.

requirements, some new QKD protocols were proposed, such as [20]–[33]. Hyperentangled state, the entanglement of particles in several degrees of freedom, has attracted much attention due to enhance the channel capacity in quantum communication [34]–[47]. However, little attention has been devoted to quantum storage time in most protocols, short storage time of quantum state is an important problem in quantum communication field, at present, the world record of quantum state storage time is only 3 ms at Heifei National Laboratory for Physical Sciences of Microscale and Department of Modern Physics. QKD protocol which need to store quantum states has some limitations on operability, considering the storage time of quantum state, a new quantum key distribution protocol based on grouping is proposed, which does not need to store quantum states. In our paper, hyperentangled Bell states are used to encode information for increasing the efficiency of eavesdropping detection, for simplicity, we call the proposed QKD protocol as HQKD and analyze the security of the protocol.

II. NEW QUANTUM KEY DISTRIBUTION PROTOCOL

A. HYPERENTANGLED STATE

In quantum key distribution protocol, entanglement state, a unique phenomenon in quantum physics, is important in quantum information communication and can be used to transmit information. 4 Bell states for two particles are as follows.

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{1}$$

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{2}$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{3}$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{4}$$

The Bell state is just the entanglement of particles in one degree of freedom, the hyperentangled state is the entanglement of quantum system in multiple degrees of freedom, which has attracted many researchers's attention for its wide applications in quantum communication. Hyperentangled Bell state is a quantum state that two particles are entangled simultaneously in 2 independent degrees of freedom. QKD protocol has been demonstrated by hyperentangled Bell states, which only requires two particles entangled in both spatial (path) and polarization degrees of freedom.If one particle of hyperentangled Bell state is measured, the hyperentangled Bell state will collapse and the state of remaining particle can be determined, so a hyperentangled Bell state can transmit 4 classical binary bits, it can be expressed as follows.

$$|\theta\rangle_{sp}^{ab} = |\varsigma\rangle_s^{ab} \otimes |\varepsilon\rangle_p^{ab} \tag{5}$$

The Bell states of polarization degree of freedom $|\varepsilon\rangle_p$ can be written as follows.

$$|\Phi^{\pm}\rangle_p^{ab} = \frac{1}{\sqrt{2}}(|HH\rangle^{ab} \pm |VV\rangle^{ab}) \tag{6}$$

$$|\Psi^{\pm}\rangle_p^{ab} = \frac{1}{\sqrt{2}}(|HV\rangle^{ab} \pm |VH\rangle^{ab}) \tag{7}$$

The Bell states of spatial degree of freedom $|\varsigma\rangle_s$ can be written as follows.

$$|\Phi^{\pm}\rangle_s^{ab} = \frac{1}{\sqrt{2}}(|H'H'\rangle^{ab} \pm |V'V'\rangle^{ab}) \tag{8}$$

$$|\Psi^{\pm}\rangle_s^{ab} = \frac{1}{\sqrt{2}}(|H'V'\rangle^{ab} \pm |V'H'\rangle^{ab}) \tag{9}$$

In equation (6), (7), (8) and (9), a and b are two hyperentangled particles, p is polarization degree of freedom, s is spatial degree of freedom, $|H\rangle$ is polarization horizontal state, $|V\rangle$ is polarization vertical state,$|H'\rangle$ and $|V'\rangle$ denote two orthogonal spatial states.

B. THE HQKD PROTOCOL

One of difficult problems is that quantum storage time is too short in quantum communication process, ping pong protocol takes two steps for transmitting information and need to store information for receivers, BB84 protocol only takes one step to transmit information and not need to store quantum states. Similar to BB84 protocol, information is transmitted by choosing different measurement bases, the HQKD transmits information by choosing different position of hyperentangled states, it also takes one step to transmit information and not need to store quantum states. Classical binary information is grouped into 6 bits and one hyperentangled Bell state and single particle are prepared for every group, then Alice transmits each group particles (three particles) to Bob at the same time by quantum channels. After receiving these particles, Bob does not store the group particles and immediately chooses the position of hyperentangled Bell state for measurement, if Bob chooses the right position, he will get the right information. Detailed protocol is described as 6 steps.

(1) Alice transmits an orderly binary sequence to Bob, she divides every 6 binary bits into a group and prepares one hyperentangled Bell state and single particle for encoding each group binary information.

(2) Alice extracts a group information and numbers them (1, 2, 3, 4, 5, 6) in turn, she divides this group into three smaller groups (1, 2), (3, 4), (5, 6) which are called A, B, C in turn. If Alice chooses two smaller groups A and B encoded by hyperentangled Bell state, the remaining smaller group C is encoded by single particle in spatial and polarization degree of freedom, position (A, B) is used to record the position information of hyperentangled Bell state. If Alice chooses smaller groups A and C encoded by hyperentangled Bell state, position (A, C) is used to record the position information, just as it shown in Figure 1. Each Hyperentangled Bell state represents 4 classical binary bits (two smaller groups) respectively.

$$0000 \rightarrow |\Phi^+\rangle_p \otimes |\Phi^+\rangle_s, \quad 0001 \rightarrow |\Phi^+\rangle_p \otimes |\Phi^-\rangle_s,$$
$$0010 \rightarrow |\Phi^+\rangle_p \otimes |\Psi^+\rangle_s, \quad 0011 \rightarrow |\Phi^+\rangle_p \otimes |\Psi^-\rangle_s,$$
$$0100 \rightarrow |\Phi^-\rangle_p \otimes |\Phi^+\rangle_s, \quad 0101 \rightarrow |\Phi^-\rangle_p \otimes |\Phi^-\rangle_s,$$
$$0110 \rightarrow |\Phi^-\rangle_p \otimes |\Psi^+\rangle_s, \quad 0111 \rightarrow |\Phi^-\rangle_p \otimes |\Psi^-\rangle_s,$$

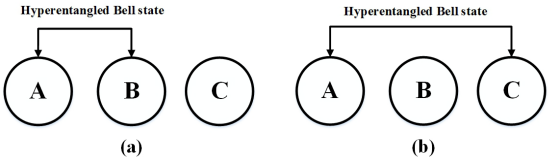


FIGURE 1. The hyperentangled state of two types of location.

$$
\begin{aligned}
&1000 \rightarrow |\Psi^+\rangle_p \otimes |\Phi^+\rangle_s, \quad 1001 \rightarrow |\Psi^+\rangle_p \otimes |\Phi^-\rangle_s,\\
&1010 \rightarrow |\Psi^+\rangle_p \otimes |\Psi^+\rangle_s, \quad 1011 \rightarrow |\Psi^+\rangle_p \otimes |\Psi^-\rangle_s,\\
&1100 \rightarrow |\Psi^-\rangle_p \otimes |\Phi^+\rangle_s, \quad 1101 \rightarrow |\Psi^-\rangle_p \otimes |\Phi^-\rangle_s,\\
&1110 \rightarrow |\Psi^-\rangle_p \otimes |\Psi^+\rangle_s, \quad 1111 \rightarrow |\Psi^-\rangle_p \otimes |\Psi^-\rangle_s \qquad (10)
\end{aligned}
$$

Single partcile in spatial and polarization degree of freedom represents 2 classical binary bits respectively.

$$
\begin{aligned}
&00 \rightarrow |0\rangle_p \otimes |0\rangle_s, \quad 01 \rightarrow |0\rangle_p \otimes |1\rangle_s,\\
&10 \rightarrow |1\rangle_p \otimes |0\rangle_s, \quad 11 \rightarrow |1\rangle_p \otimes |1\rangle_s \qquad (11)
\end{aligned}
$$

Alice records the position information and sends every group quantum information to Bob by quantum channel at the same time. If information of all groups are taken out, go to step (5), otherwise go to (3).

(3) When Bob has received the qubits from Alice, Bob randomly chooses position (A,B) or position (A,C) to measure hyperentangled Bell state and does B_z measurement on remaining single particle.

(4) After Bob completed quantum measurement, Alice tells Bob the position information of hyperentangled Bell state by classical channel. If the position information chosen by Bob is not right, the key generated by the current group will be discarded. Otherwise, Bob decodes the key information and adds them into the whole raw key, then goes to step (2) to start the next group.

(5) In order to detect Eavesdropper Eve, Bob randomly extracts some hyperentangled Bell state particles from the whole raw key as decoy particles, Alice tells Bob the original information of the decoy particles, Bob compares measurement results in his hand with the transmitted by Alice. According to [48], without eavesdroppers the error rate ε will be lower than the specified threshold 11%, quantum channel is considered to be secure and the generated key information is credible, otherwise, the generated key information is unreliable and the communication process ends.

(6) After quantum channels have been proved secure, Alice and Bob perform the correction and privacy amplification for the remaining particles, the final key is got.

Table 1 is an example of the process that one group information (010001) was encoded and sent to Bob. Before information was transmitted, Alice and Bob confirm the relationship between hyperentangled Bell states and 4 bit information based on equation 10, the relationship between single particle and 2 bit information based on equation 11. As shown in Table 1, Alice needs to transmit (010001) to Bob, she divides this group information into three smaller groups A, B and C, smaller group A is (01), smaller group B is (00), smaller grouper C is (01). Assuming Alice chooses smaller groups A and C encoded by hyperentangled Bell state, smaller group B encoded by single particle. The information of (A,C) is (0101), which is encoded as $|\Phi^-\rangle_p^{AC} \otimes |\Phi^-\rangle_s^{AC}$ based on equation 10; the information of smaller group B is encoded as $|0\rangle_p^B \otimes |0\rangle_s^B$ based on equation 11. Information is transmitted to Bob by quantum channel, assuming Bob chooses the same position as Alice to measure, he will get hyperentangled Bell state $|\Phi^-\rangle_p^{AC} \otimes |\Phi^-\rangle_s^{AC}$ and single particle state $|0\rangle_p^B \otimes |0\rangle_s^B$. When Alice tells Bob the position of hyperentangled Bell state, Bob will get the right group information (010001) based on equation 10 and equation 11.

TABLE 1. The example of the process that one group (010001) is transmitted to Bob.

Number of classical bits	1	2	3	4	5	6
Binary bits that Alice prepares	0	1	0	0	0	1
Group divided by Alice	A		B		C	
Hyperentangled Bell state and single particle sent by Alice	$\|\Phi^-\rangle_p^{AC} \otimes \|\Phi^-\rangle_s^{AC}$		$\|0\rangle_p^B \otimes \|0\rangle_s^B$		$\|\Phi^-\rangle_p^{AC} \otimes \|\Phi^-\rangle_s^{AC}$	
Measurement position made by Bob	(A,C)		B		(A,C)	
Measurement result got by Bob	$\|\Phi^-\rangle_p^{AC} \otimes \|\Phi^-\rangle_s^{AC}$		$\|0\rangle_p^B \otimes \|0\rangle_s^B$		$\|\Phi^-\rangle_p^{AC} \otimes \|\Phi^-\rangle_s^{AC}$	
Measurement position made by Bob	right		right		right	
Share secret key by Alice and Bob	0	1	0	0	0	1
Is the key correct or not	√	√	√	√	√	√

III. PROTOCOL SECURITY ANALYSIS

A. THE INTERCEPT-MEASURE-RESEND ATTACK

Security analysis is very important for QKD protocol, the theoretical security is based on the law of quantum mechanics. For quantum key communication process, there are many types of attacks, including coherent attack and incoherent attack. Intercept-measure-resend (IR) attack is a common incoherent attack, security analysis under IR attack is analyzed now.

Alice sends quantum information to Bob, but Eve does not know the position of hyperentangled Bell state, he randomly chooses the position (A, B) or position (A, C) to measure and resends them to Bob, which would cause bit error. If Bob measures hyperentangled Bell state with the same position as Alice sends and there is no eavesdroppers, they can get the right key, the bit error rate is 0.

If Bob chooses the wrong position to measure, Alice and Bob will find measurement positions different by Alice and Bob's comparison process, the result will be discarded whether Eve eavesdrops or not.

TABLE 2. The example of the process that Eve eavesdrops (right position).

Number of classical bits	1	2	3	4	5	6
Binary bits that Alice prepares	0	1	0	0	0	1
Group divided by Alice	A		B		C	
Hyperentangled Bell state and single particle sent by Alice	$\|\Phi^-\rangle_p^{AC} \otimes \|\Phi^-\rangle_s^{AC}$		$\|0\rangle_p^B \otimes \|0\rangle_s^B$		$\|\Phi^-\rangle_p^{AC} \otimes \|\Phi^-\rangle_s^{AC}$	
Measurement position made by Eve	(A, C)		B		(A, C)	
Measurement result got by Eve	$\|\Phi^-\rangle_p^{AC} \otimes \|\Phi^-\rangle_s^{AC}$		$\|0\rangle_p^B \otimes \|0\rangle_s^B$		$\|\Phi^-\rangle_p^{AC} \otimes \|\Phi^-\rangle_s^{AC}$	
Measurement position made by Bob	(A, C)		B		(A, C)	
Measurement result got by Bob	$\|\Phi^-\rangle_p^{AC} \otimes \|\Phi^-\rangle_s^{AC}$		$\|0\rangle_p^B \otimes \|0\rangle_s^B$		$\|\Phi^-\rangle_p^{AC} \otimes \|\Phi^-\rangle_s^{AC}$	
Public discussion of states	0	1	0	0	0	1
Is the key correct or not	√	√	√	√	√	√

TABLE 3. The example of the process that Eve eavesdrops (wrong position with wrong result).

Number of classical bits	1	2	3	4	5	6
Binary bits that Alice prepares	0	1	0	0	0	1
Group divided by Alice	A		B		C	
Hyperentangled Bell state and single particle sent by Alice	$\|\Phi^-\rangle_p^{AC} \otimes \|\Phi^-\rangle_s^{AC}$		$\|0\rangle_p^B \otimes \|0\rangle_s^B$		$\|\Phi^-\rangle_p^{AC} \otimes \|\Phi^-\rangle_s^{AC}$	
Measurement position made by Eve	(A, B)		(A, B)		C	
Measurement result got by Eve	$\|\Phi^+\rangle_p^{AB} \otimes \|\Phi^+\rangle_s^{AB}$		$\|\Phi^+\rangle_p^{AB} \otimes \|\Phi^+\rangle_s^{AB}$		$\|0\rangle_p^C \otimes \|0\rangle_s^C$	
Measurement position made by Bob	(A, C)		B		(A, C)	
Measurement result got by Bob	$\|\Phi^+\rangle_p^{AC} \otimes \|\Phi^-\rangle_s^{AC}$		$\|0\rangle_p^B \otimes \|0\rangle_s^B$		$\|\Phi^+\rangle_p^{AC} \otimes \|\Phi^-\rangle_s^{AC}$	
Public discussion of states	0	0	0	0	0	1
Is the key correct or not	×	×	×	×	×	×

If Eve takes IR attacks during the communication process, because Eve does not know the position of hyperentangled Bell state, he will randomly choose position to measure that will cause bit error, assuming Alice chooses the position of hyperentangled Bell state (A, C), the analysis is as follow.

(1)If Eve chooses position (A, C) to measure and resends the result to Bob, the probability is 50%. When Bob receives particles, if Bob chooses the same position (A, C) to measure, Bob will get the same result as Alice sent, they will not find the existence of Eve. Table 2 shows this process of transmitting one group information (010001).

(2) If Eve chooses position (A, B) to measure and resends the result to Bob, the probability is 50%, the hyperentangled Bell state position chosen by Bob is inconsistent with Alice's choice, it will destroy the original hyperentangled Bell state of A and C particles. According to Heisenberg uncertainty principle, A and B particles will randomly collapse into one of hyperentangled Bell state, C particle will randomly collapse into one of single particle state. For example, if Alice sends (010001) binary sequence to Bob, smaller group A is (01), smaller group B is (00), smaller group C is (01), according to equation(8) and (9), Alice encodes A and C as $|\Phi^-\rangle_p^{AC} \otimes |\Phi^-\rangle_s^{AC}$,$B$ as $|0\rangle_p^B \otimes |0\rangle_s^B$, if Eve chooses position (A, B) to measure, the measurement result is so.

$$\begin{aligned} m_e = & \frac{1}{\sqrt{2}}((|\Phi^+\rangle_p^{AB} + |\Phi^-\rangle_p^{AB})|0\rangle_p^C \\ & - (|\Psi^+\rangle_p^{AB} + |\Psi^-\rangle_p^{AB})|1\rangle_p^C) \\ \otimes & \frac{1}{\sqrt{2}}((|\Phi^+\rangle_s^{AB} + |\Phi^-\rangle_s^{AB})|0\rangle_s^C \\ & - (|\Psi^+\rangle_s^{AB} + |\Psi^-\rangle_s^{AB})|1\rangle_s^C) \end{aligned} \tag{12}$$

Eve can obtain 16 different measurement results with the same probability of 1/16, subsequently, Eve resends the measurement result to Bob. If Eve's measurement result is $\frac{1}{\sqrt{2}}((|\Phi^+\rangle_p^{AB})|0\rangle_p^C) \otimes \frac{1}{\sqrt{2}}((|\Phi^+\rangle_s^{AB}|0\rangle_s^C)$, he resends the result to Bob, supposing Bob chooses hyperentangled Bell state position (A, C) to measure, Bob will get a random result as follow.

$$\begin{aligned} m_c = & \frac{1}{\sqrt{2}}((|\Phi^+\rangle_p^{AC} + |\Phi^-\rangle_p^{AC})|0\rangle_p^B \\ & - (|\Psi^+\rangle_p^{AC} + |\Psi^-\rangle_p^{AC})|1\rangle_p^B) \\ \otimes & \frac{1}{\sqrt{2}}((|\Phi^+\rangle_s^{AC} + |\Phi^-\rangle_s^{AC})|0\rangle_s^B \\ & - (|\Psi^+\rangle_s^{AC} + |\Psi^-\rangle_s^{AC})|1\rangle_s^B) \end{aligned} \tag{13}$$

From the equantion (13), Bob may get the right state $\frac{1}{\sqrt{2}}((|\Phi^-\rangle_p^{AC})|0\rangle_p^B) \otimes \frac{1}{\sqrt{2}}((|\Phi^-\rangle_s^{AC}|0\rangle_s^B)$ with 1/16 probability, then he get the right result (010001); Bob may get wrong state with 15/16 probability, the result may be one of the following case {(000000), (000001), (000110), (000111), (010000), (010110) (010111), (101000), (101001), (101110), (101111), (111000), (111001), (111110), (111111} and in these cases eavesdropper Eve will be detected by comparison between Alice and Bob. Table 3 shows an example that Alice transmits (010001) to Bob, Eve chooses wrong position to eavesdrop and gets wrong result, Table 4 shows an example that Alice transmits (010001) to Bob, Eve chooses wrong position to eavesdrop and gets right result.

If Eve's measurement result is one of the remaining 15 cases, the analysis process is similar to the above analysis, in each case, Eve will be detected with 15/16 probability.

TABLE 4. The example of the process that Eve eavesdrops (wrong position with right result)

Number of classical bits	1	2	3	4	5	6
Binary bits that Alice prepares	0	1	0	0	0	1
Group divided by Alice	A		B		C	
Hyperentangled Bell state and single particle sent by Alice	$\|\Phi^-\rangle_p^{AC} \otimes \|\Phi^-\rangle_s^{AC}$		$\|0\rangle_p^B \otimes \|0\rangle_s^B$		$\|\Phi^-\rangle_p^{AC} \otimes \|\Phi^-\rangle_s^{AC}$	
Measurement position made by Eve	(A, B)		(A, B)		C	
Measurement result got by Eve	$\|\Phi^+\rangle_p^{AB} \otimes \|\Phi^+\rangle_s^{AB}$		$\|\Phi^+\rangle_p^{AB} \otimes \|\Phi^+\rangle_s^{AB}$		$\|0\rangle_p^C \otimes \|0\rangle_s^C$	
Measurement position made by Bob	(A, C)		B		(A, C)	
Measurement result got by Bob	$\|\Phi^-\rangle_p^{AC} \otimes \|\Phi^-\rangle_s^{AC}$		$\|0\rangle_p^B \otimes \|0\rangle_s^B$		$\|\Phi^-\rangle_p^{AC} \otimes \|\Phi^-\rangle_s^{AC}$	
Public discussion of states	0	1	0	0	0	1
Is the key correct or not	√	√	√	√	√	√

In HQKD protocol, Bob and Eve measure hyperentangled Bell states independently. Eve chooses the right position of hyperentangled Bell state with 1/2 probability, in this case, he can get the correct result without being detected by Bob and Alice; Eve chooses the wrong position of hyperentangled Bell state with 1/2 probability, he will get a random result, in this case, Bob gets the correct result with 1/16 probability and the wrong result with 15/16 probability. Therefore, when there is eavesdropper Eve, the probability of getting wrong key is $\zeta = 15/32 = 46.875\%$.

If Alice and Bob compare m groups information, they would detect eavesdropper Eve with the probability of $P_d = 1 - (1/2 + 1/2 \times 1/16)^m$, in order to get the probability of $1 - 10^{-9}$, they need to compare 33 groups information, which is less than 72 groups information in BB84 protocol.

According to [38], [39], $I(A, B)$ is the mutual information between Alice and Bob, $I(A, E)$ is the mutual information between Alice and Eve, $I(A, B)$ should be greater than $I(A, E)$ based on the security requirement of quantum channel, if the bit error rate of quantum channel is larger than 11%, eavesdropper Eve will be detected. In order to avoid being detected, Eve should eavesdrop with a certain probability r, the overall error rate should satisfy $\zeta_d = \zeta \times r < 0.11$, we can get the value of r which should be less than 0.235 and satisfy the following equation.

$$I_1 = -(r * \frac{15}{32}) \log_2(r * \frac{15}{32}) \tag{14}$$

$$I_0 = -(1 - r * \frac{15}{32}) \log_2(1 - r * \frac{15}{32}) \tag{15}$$

If $0 < r < 0.235$, according to [40], the following equation should satisfy $\bigtriangleup = 1 - 2 \times (I_0 + I_1) > 0$, if $r \geq 0.235$, Alice and Bob will find eavesdropper Eve, they will discard this communication and restart a new one.

B. THE ENTANGLEMENT-MEASURE ATTACK

Now we analyze another type of attack named entanglement-measure attack. In order to reduce the probability of being detected, Eve attacks only B and C particles. Assume A and C particles are hyperentangled Bell state $|\Phi^+\rangle_{ps}^{AC} = |\Phi^+\rangle_p^{AC} \otimes |\Phi^+\rangle_s^{AC}$, B is single particle state $|0\rangle_p^B \otimes |0\rangle_s^B$, $|H\rangle$, $|V\rangle$, $|H'\rangle$ and $|V'\rangle$ are written as $|1\rangle_p$, $|0\rangle_p$, $|1\rangle_s$ and $|0\rangle_s$, $|\Phi^+\rangle_{ps}^{AC}$ can be written as.

$$\begin{aligned}|\Phi\rangle_{ps}^{AC} = \frac{1}{2}(&|00\rangle_p^{AC}|00\rangle_s^{AC} + |00\rangle_p^{AC}|11\rangle_s^{AC} \\ &+ |11\rangle_p^{AC}|00\rangle_s^{AC} + |11\rangle_p^{AC}|11\rangle_s^{AC})\end{aligned} \tag{16}$$

After Eve's attack $\widehat{E}$, the state $|0\rangle_p$ and $|1\rangle_p$ become.

$$\begin{aligned}|\varphi_0\rangle_p &= \widehat{E}|0x\rangle_p = \alpha|0x_0\rangle_p + \beta|1x_1\rangle_p, \\ |\varphi_1\rangle_p &= \widehat{E}|1y\rangle_p = m|0y_0\rangle_p + n|1y_1\rangle_p,\end{aligned} \tag{17}$$

The state $|0\rangle_s$ and $|1\rangle_s$ become.

$$\begin{aligned}|\varphi_0'\rangle_s &= \widehat{E}|0x'\rangle_s = \alpha'|0x_0'\rangle_s + \beta'|1x_1'\rangle_s, \\ |\varphi_1'\rangle_s &= \widehat{E}|1y'\rangle_s = m'|0y_0'\rangle_s + n'|1y_1'\rangle_s,\end{aligned} \tag{18}$$

$|x_0\rangle_p$, $|x_1\rangle_p$, $|y_0\rangle_p$, $|y_1\rangle_p$, $|x_0'\rangle_s$, $|x_1'\rangle_s$, $|y_0'\rangle_s$ and $|y_1'\rangle_s$ are the pure ancillary states determined by Eve, and satisfy.

$$\begin{aligned}|\alpha|^2 + |\beta|^2 = 1, \quad |\alpha'|^2 + |\beta'|^2 = 1, \\ |m|^2 + |n|^2 = 1, \quad |m'|^2 + |n'|^2 = 1\end{aligned} \tag{19}$$

After being attacked by Eve, A and C particles can be written as.

$$\begin{aligned}&\frac{1}{\sqrt{2}}(\alpha|00x_0\rangle_p + \beta|10x_1\rangle_p + m|01y_0\rangle_p + n|11y_1\rangle_p) \\ &\otimes \frac{1}{\sqrt{2}}(\alpha'|00x_0'\rangle_s + \beta'|10x_1'\rangle_s + m'|01y_0'\rangle_s + n'|11y_1'\rangle_s)\end{aligned} \tag{20}$$

After being attacked by Eve, B particle satisfies can be written as.

$$(\alpha|0x_0\rangle_p + \beta|1x_1\rangle_p) \otimes (\alpha'|0x_0'\rangle_s + \beta'|1x_1'\rangle_s) \tag{21}$$

So the lower bound of the detection probability d_l is:

$$\begin{aligned}d_l &= 1 - p(|\Phi^+\rangle_p^{AC})p(|\Phi^+\rangle_s^{AC})p(|0\rangle_p^B)p(|0\rangle_s^B) \\ &= 1 - \frac{1}{4}((\alpha\alpha')^2 + (n\alpha')^2 + (nn')^2 + (\alpha' n)^2)(\alpha\alpha')^2\end{aligned} \tag{22}$$

Suppose $|\alpha|^2 = a$, $|\beta|^2 = b$, $|m|^2 = s$, $|n|^2 = t$, $|\alpha'|^2 = a'$, $|\beta'|^2 = b'$, $|m'|^2 = s'$, $|n'|^2 = t'$, a, b, s, t, a', b', s' and t' are positive real numbers, $a + b = s + t = a' + b' = s' + t' = 1$, so d_l can be written as.

$$d_l = 1 - \frac{1}{4}(aa' + tt' + at' + ta')aa' \tag{23}$$

Considering the same probability of sending $|0\rangle$ and $|1\rangle$ in the general system, we set $a = a' = t = t'$, after simple mathematical calculation, we can get a.

$$a = (1 - d_l)^{1/4} \tag{24}$$

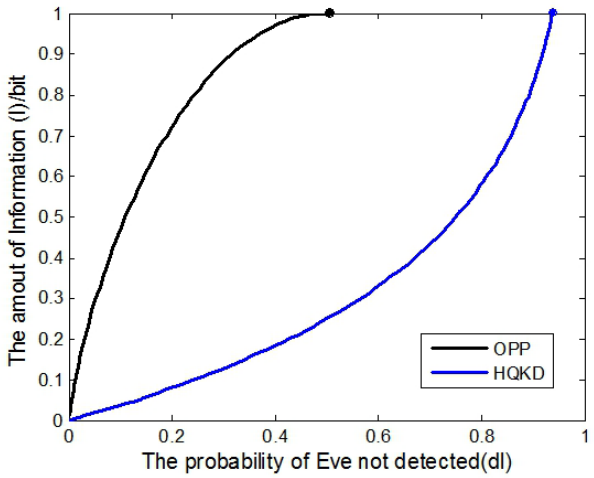


FIGURE 2. The relationship between d_l and I.

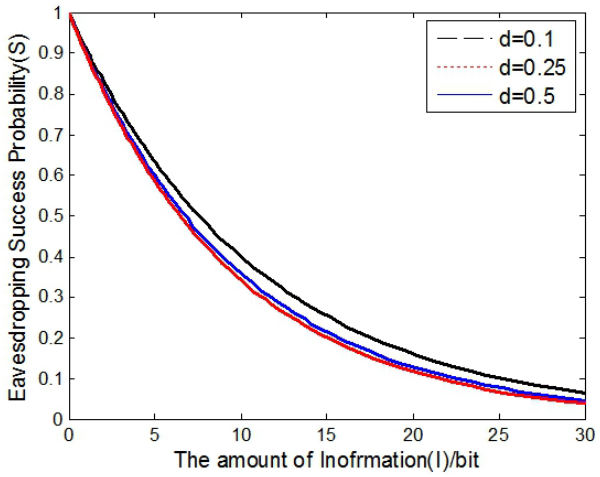


FIGURE 3. Eavesdropping success probability as a function of the maximal eavesdropped information, plotted for different detection probabilities.

The relationship between the maximal amount of the information I and detection probability d_l is as follows.

$$\begin{aligned} I &= -a\log_2 a - (1-a)\log_2(1-a) \\ &= H(a) = H((1-d_l)^{1/4}) \end{aligned} \tag{25}$$

From the Figure 2, we can see that if Eve wants to get all the information, the detection probability is 0.9375, Eve will face greater eavesdropping detection probability than OPP protocol.

Assuming the probability of Bob choosing one group particles as decoy particles is c, when Alice chooses the first group as message particles, the amount of information eavesdropped by Eve is $1-c$, when Bob chooses the first group as decoy particles but the second group as message particles, the amount of information eavesdropped by Eve is $c(1-d)(1-c)$. Similarly, the amount of information that eavesdropped by Eve can be got in each case. If Eve is not detected, the probability of successful eavesdropping is as follows.

$$\begin{aligned} s(c,d) &= (1-c)+c(1-d)(1-c)+c^2(1-d)^2(1-c)+\ldots \\ &= (1-c)/[1-c(1-d)] \end{aligned} \tag{26}$$

After n successful eavesdropping, Eve can get $6nI(d)$ bits classical information, this probability is s^n, the probability for successful eavesdropping $I = 6nI(d)$ bit information is as follows.

$$s(I,c,d) = ((1-c)/(1-c(1-d)))^{I/6I(d)} \tag{27}$$

For Eve chooses wrong position with 50% probability, so $c = 0.5$, we can get eavesdropping success probability s as a function of the information I. Figure 2 shows eavesdropping success probability as a function of the maximal eavesdropped information for different detection probabilities d.

In Figure 3, When is $I \to \infty$ $s \to 0$ got, Eve only gets part of right information but does not even know which part is it, so the HQKD protocol can be thought as asymptotically secure. If desired, the security can arbitrarily be improved by increasing the control parameter c at the cost of decreasing information transmission rate.

IV. CONCLUSION

In this paper, a new quantum key distribution protocol HQKD is proposed and the security of this protocol is analyzed for intercept-measure-resend (IR) attack and entanglement-measure attack. HQKD protocol doesn't need to store the quantum states and improves the maneuverability, the position of hyperentangled Bell state is used to encode information and detect eavesdroppers.Compared with [44], 6 bits classical information can be encoded by a hyperentangled Bell state and single particle, this protocol is with higher information transmission efficiency.Compared with OPP protocol, the HQKD protocol is with higher eavesdropping detection efficiency 93.75% when Eve wants to get all the information. The protocol needs to fabricate and measure single particle, which can be implemented by using single photon source, single photon detectors and linear optical devices, this protocol also needs to fabricate and measure hyperentangled Bell states, which has been experimentally realized [48], [49], but based on the existing technical conditions, there are some difficulties in realizing to mix hyperentangled Bell states and single particle, quantum experiments have developed rapidly in recent years and the research of mixing hyperentangled Bell states and single particle will be research focus, we believe that the problem will be solved with the advancement of technology.

REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public-key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst. Signal Process.*, Washington, DC, USA, 1984, pp. 175–179.

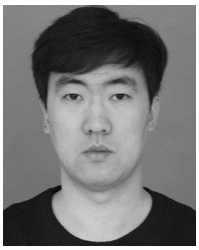
[2] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett*, vol. 67, no. 2, pp. 661–663, 1991.

[3] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Phys. Rev. Lett*, vol. 68, no. 5, p. 557, 1992.
[4] V. Scarani, N. Gisin, and S. Popescu, "Proposal for energy-time entanglement of quasiparticles in a solid-state device," *Phys. Rev. Lett*, vol. 92, no. 16, 2004, Art. no. 167901.
[5] K. Boström and T. Felbinger, "Deterministic secure direct communication using entanglement," *Phys. Rev. Lett.*, vol. 89, Oct. 2002, Art. no. 187902.
[6] A. Wójcik, "Eavesdropping on the 'ping-pong' quantum communication protocol," *Phys. Rev. Lett*, vol. 90, no. 15, 2003, Art. no. 157901.
[7] D. Fu-Guo, L. Xi-Han, L. Chun-Yan, Z. Ping, and Z. Hong-Yu, "Eavesdropping on the 'ping-pong' quantum communication protocol freely in a noise channel," *Chin. Phys. Lett*, vol. 16, no. 2, pp. 277–281, 2005.
[8] Q.-Y. Cai, "The 'ping-pong' protocol can be attacked without eavesdropping," *Phys. Rev. Lett*, vol. 91, no. 10, 2003, Art. no. 109801.
[9] F.-G. Deng and G. L. Long, "Secure direct communication with a quantum one-time pad," *Phys. Rev. A, Gen. Phys.*, vol. 69, May 2004, Art. no. 052319.
[10] D. Jiang, Y. Chen, X. Gu, L. Xie, and L. Chen, "Deterministic secure quantum communication using a single d-level system," *Sci. Rep.*, vol. 7, Mar. 2017, Art. no. 44934.
[11] A. G. de Araújo Holanda Guerra, F. F. S. Rios, and R. V. Ramos, "Quantum secure direct communication of digital and analog signals using continuum coherent states," *Quantum Inf. Process.*, vol. 15, no. 11, pp. 4747–4758, 2016.
[12] C. Wang, F. G. Deng, Y. S. Li, X. S. Liu, and G. L. Long, "Quantum secure direct communication with high-dimension quantum superdense coding," *Phys. Rev. A, Gen. Phys.*, vol. 71, no. 4, 2005, Art. no. 044305.
[13] J. Li, D. Song, R. Li, and X. Lu, "A quantum secure direct communication protocol based on four-qubit cluster state," *Secur. Commun. Netw.*, vol. 8, no. 1, pp. 36–42, 2015.
[14] W. Li, J. Chen, X. Wang, and C. Li, "Quantum secure direct communication achieved by using multi-entanglement," *Int. J. Theor. Phys.*, vol. 54, no. 1, pp. 100–105, 2015.
[15] J. Li, Z. Pan, F. Sun, Y. Chen, Z. Wang, and Z. Shi, "Quantum secure direct communication based on dense coding and detecting eavesdropping with four-particle genuine entangled state," *Entropy*, vol. 17, no. 10, pp. 6743–6752, 2015.
[16] J. Cai, Z. Pan, T.-J. Wang, S. Wang, and C. Wang, "High-capacity quantum secure direct communication using hyper-entanglement of photonic qubits," *Int. J. Quantum Inf.*, vol. 14, no. 8, 2016, Art. no. 1650043.
[17] M. Nanvakenari and M. Houshmand, "An efficient controlled quantum secure direct communication and authentication by using four particle cluster states," *Int. J. Quantum Inf.*, vol. 15, no. 1, 2017, Art. no. 1750002.
[18] X.-L. Zhao, J.-L. Li, P.-H. Niu, H.-Y. Ma, and D. Ruan, "Two-step quantum secure direct communication scheme with frequency coding," *Chin. Phys. B*, vol. 26, no. 3, 2017, Art. no. 030302.
[19] Z. Zhang, Z. Man, and Y. Li, "Improving Wójcik's eavesdropping attack on the ping-pong protocol," *Phys. Lett. A*, vol. 333, nos. 1–2, pp. 46–50, 2004.
[20] W.-Y. Hwang, H.-Y. Su, and J. Bae, "Improved measurement-device-independent quantum key distribution with uncharacterized qubits," *Phys. Rev. A, Gen. Phys.*, vol. 95, no. 6, 2017, Art. no. 062313.
[21] L. A. Lizama-Pérez, J. M. López, and E. De Carlos López, "Quantum key distribution in the presence of the intercept-resend with faked states attack," *Entropy*, vol. 19, no. 1, p. 4, 2016.
[22] H. Lai, M.-X. Luo, C. Zhan, J. Pieprzyk, and M. A. Orgun, "An improved coding method of quantum key distribution protocols based on Fibonacci-valued OAM entangled states," *Phys. Lett. A*, vol. 381, no. 35, pp. 2922–2926, 2017.
[23] D. Pastorello, "A quantum key distribution scheme based on tripartite entanglement and violation of CHSH inequality," *Int. J. Quantum Inf.*, vol. 15, no. 5, 2017, Art. no. 1750040.
[24] Y. Wang, W.-S. Bao, H.-Z. Bao, C. Zhou, M.-S. Jiang, and H.-W. Li, "High-dimensional quantum key distribution with the entangled single-photon-added coherent state," *Phys. Lett. A*, vol. 381, no. 16, pp. 1393–1397, 2017.
[25] C.-L. Xie, Y. Guo, Y.-J. Wang, D. Huang, and L. Zhang, "Security simulation of continuous-variable quantum key distribution over air-to-water channel using Monte Carlo method," *Chin. Phys. Lett.*, vol. 35, no. 9, 2018, Art. no. 090302.
[26] H. Liu, W. Qu, T. Dou, J. Wang, Y. Zhang, and H. Ma, "Passive round-robin differential-quadrature-phase-shift quantum key distribution scheme with untrusted detectors," *Chin. Phys. B*, vol. 27, no. 10, 2018, Art. no. 020303.
[27] C.-M. Zhang, J.-R. Zhu, and Q. Wang, "Practical reference-frame-independent measurement-device-independent quantum key distribution systems against the worst relative rotation of reference frames," *Commun. Theor. Phys*, vol. 70, no. 4, pp. 379–383, 2018.
[28] H. Zhang, Y. Mao, D. Huang, Y. Guo, X. Wu, and L. Zhang, "Finite-size analysis of eight-state continuous-variable quantum key distribution with the linear optics cloning machine," *Chin. Phys. B*, vol. 27, no. 9, 2018, Art. no. 090307.
[29] W. Liu, J. Peng, P. Huang, S. Wang, T. Wang, and G. Zeng, "Continuous-variable quantum key distribution based on continuous random basis choice," *Chin. Phys. B*, vol. 27, no. 7, 2018, Art. no. 070305.
[30] X. Wang, Y. Zhang, and S. Yu, "High speed error correction for continuous-variable quantum key distribution with multi-edge type LDPC code," *Sci. Rep.*, vol. 8, no. 1, 2018, Art. no. 10543.
[31] W. Zhang, D. Qiu, and P. Mateus, "Security of a single-state semi-quantum key distribution protocol," *Quantum Inf. Process.*, vol. 17, no. 6, p. 135, 2018.
[32] Z. Zhang, R. Shi, G. Zeng, and Y. Guo, "Coherent attacking continuous-variable quantum key distribution with entanglement in the middle," *Quantum Inf. Process.*, vol. 17, no. 6, p. 133, 2018.
[33] B. Qi and C. C. W. Lim, "Noise analysis of simultaneous quantum key distribution and classical communication scheme using a true local oscillator," *Phys. Rev. Appl.*, vol. 9, no. 5, 2018, Art. no. 054008.
[34] G. Bin, H. Yu-Gai, F. Xia, and Z. Cheng-Yi, "A two-step quantum secure direct communication protocol with hyperentanglement," *Chin. Phys*, vol. 20, no. 10, pp. 66–70, 2011.
[35] T. C. Wei, J. T. Barreiro, and P. G. Kwiat, "Hyperentangled Bell-state analysis," *Phys. Rev. A, Gen. Phys.*, vol. 75, no. 6, 2012, Art. no. 060305.
[36] C. Wang, L. Xiao, W.-Y. Wang, G.-Y. Zhang, and G. L. Long, "Quantum key distribution using polarization and frequency hyperentangled photons," *J. Opt. Soc. Amer. B, Opt. Phys.*, vol. 26, no. 11, pp. 2072–2076, 2009.
[37] G. Bin, H. Yu-Gai, F. Xia, and C. Yu-Lin, "Bidirectional quantum secure direct communication network protocol with hyperentanglement," *Commun. Theor. Phys.*, vol. 56, no. 10, pp. 659–663, 2011.
[38] W. Tie-Jun, L. Tao, D. Fang-Fang, and D. Fu-Guo, "High-capacity quantum secure direct communication based on quantum hyperdense coding with hyperentanglement," *Chin. Phys. Lett*, vol. 28, no. 4, 2011, Art. no. 040305.
[39] S. Jin, G. Yan-Xiao, X. Ping, Z. Shi-Ning, and Z. You-Bang, "Quantum secure direct communication by using three-dimensional hyperentanglement," *Commun. Theor. Phys.*, vol. 56, no. 5, pp. 831–836, 2011.
[40] T.-J. Wang, L.-L. Liu, R. Zhang, C. Cao, and C. Wang, "One-step hyperentanglement purification and hyperdistillation with linear optics," *Opt. Express*, vol. 23, no. 7, pp. 9284–9294, 2015.
[41] F. Wu, G. Yang, H. Wang, J. Xiong, F. Alzahrani, A. Hobiny, and F. Deng, "High-capacity quantum secure direct communication with two-photon six-qubit hyperentangled states," *Sci. China Phys., Mech. Astron.*, vol. 60, no. 12, 2017, Art. no. 120313.
[42] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, no. 2, pp. 441–444, 2000.
[43] V. Scarani and N. Gisin, "Quantum communication between N partners and Bell's inequalities," *Phys. Rev. Lett*, vol. 87, Aug. 2001, Art. no. 117901.
[44] J. Li, N. Li, L.-L. Li, and T. Wang, "One step quantum key distribution based on EPR entanglement," *Sci. Rep.*, vol. 6, Jun. 2016, Art. no. 28767.
[45] A. Cabello, "Bipartite bell inequalities for hyperentangled states," *Phys. Rev. Lett*, vol. 97, no. 14, 2006, Art. no. 140406.
[46] Y.-B. Sheng, F.-G. Deng, and G. L. Long, "Complete hyperentangled-Bell-state analysis for quantum communication," *Phys. Rev. A, Gen. Phys.*, vol. 82, no. 3, 2011, Art. no. 032318.
[47] L. Xu and Z.-W. Zhao, "High-capacity quantum private comparison protocol with two-photon hyperentangled Bell states in multiple-degree of freedom," *Eur. Phys. J. D*, vol. 73, no. 3, p. 58, 2019.
[48] Z.-B. Chen, J.-W. Pan, Y.-D. Zhang, Č. Brukner, and A. Zeilinger, "All-versus-nothing violation of local realism for two entangled photons," *Phys. Rev. Lett*, vol. 90, no. 16, 2003, Art. no. 160408.
[49] T. Yang, Q. Zhang, J. Zhang, J. Yin, Z. Zhao, M. Zukowski, Z.-B. Chen, and J.-W. Pan, "All-versus-nothing violation of local realism by two-photon, four-dimensional entanglement," *Phys. Rev. Lett*, vol. 95, no. 24, 2005, Art. no. 240406.

YANYAN HOU received the M.S. degree in signal and information processing from Shandong University, in 2007. She is currently pursuing the Ph.D. degree with the Beijing University of Posts and Telecommunications, Beijing, China. She is currently an Associate Professor with the College of Information Science and Engineering, Zaozhuang University, Zaozhuang, China. She has authored more than 20 articles. Her research interests include quantum communication and quantum cryptography.

JIAN LI received the Ph.D. degree from the Beijing Institute of Technology, in 2005. He is currently a Professor with the School of Computer, Beijing University of Posts and Telecommunications, Beijing, China. His research interests include information security and quantum cryptography.

HENGJI LI received the M.S. degree from the China University of Petroleum, Beijing, China, in 2017. He is currently pursuing the Ph.D. degree with the Beijing University of Posts and Telecommunications. His research interests include information security and quantum walks.



CHAO-YANG LI received the M.S. degree from the Zhenzhou University of Light Industry, Zhenzhou, Henan, China, in 2017. He is currently pursuing the Ph.D. degree with the Beijing University of Posts and Telecommunications. His research interests include information security, cryptography, and blockchain.

YUGUANG YANG received the Ph.D. degree from the Beijing University of Posts and Telecommunications, in 2006. She is currently a Professor with the School of Computer, Beijing University of Technology, Beijing, China. Her research interests include cryptography and information security.

NA WANG received the Ph.D. degree from the School of Mathematical Sciences, Xiamen University, in 2018. She is currently a Postdoctoral Fellow with the School of Computer Science, Beijing University of Posts and Telecommunications. Her research interests include cryptography, message sharing, and information security issues in distributed and cloud systems.

ZHENGYAN ZHOU received the B.E. degree from Huazhong Agricultural University, Wuhan, Hubei. She is currently pursuing the M.S. degree with the Beijing University of Posts and Telecommunications. Her research interests include quantum cryptography and quantum security communication.