Computers, Materials & Continua CMC, vol.65, no.2, pp.1507-1517, 2020

Quantum Electronic Contract Scheme Based on Single Photon

Tian Cao[1], Yan Chang[1,*], Lili Yan[1], Shibin Zhang[1] and Qirun Wang[2]

Abstract: An electronic contract is a contract signed by electronic means, which is widely used in electronic commerce activities. In recent years, with the rapid development of quantum cryptography technology, the quantum electronic contract has been widely studied by researchers. Supported by the basic principles of quantum mechanics, a quantum electronic contract scheme based on the single photon is proposed in this paper. In this scheme, two copies of the same contract are signed by both parties involved, and then a copy of each contract is sent to a trusted third party. The trusted third party verifies the signatures of both parties and compares the signed copies to determine whether the contract is valid. Compared with the previous scheme, this scheme is based on the quantum electronic contract signed by the single photon. Because the single photon is easy to prepare and operate, this scheme is simple and easy to implement. At the same time, the scheme does not need to exchange signatures between the two parties, which reduces the complexity of communication. Nevertheless, it requires both parties and the third party to be honest and trustworthy.

Keywords: E-contract, quantum cryptography, single photon, trusted third party.

1 Introduction

Information security is a very important element in information transmission [Jonathan and Phyllis (2019)]. Currently, most of the research on information security is based on mathematical problems such as large number decomposition and discrete logarithm. However, with the rapid development of quantum technology, conventional information security protection methods have hidden dangers. As a result, many scholars study information protection technology [Wang, Gao, Liu et al. (2019)] based on quantum mechanics.

Quantum key distribution (QKD) is the ability of both parties to generate and share a random, secure key to encrypt and decrypt messages. In 1984, Bennett et al. [Bennett and Brassard (1984)] proposed the first quantum key distribution protocol-BB84 protocol. In 1992, Bennett et al. [Bennett and Wiesner (1992)] designed the B92 protocol based on non-orthogonal state by using quantum entanglement. In 1995, Goldenberg et al.

[1] College of Information Security Engineering, Chengdu University of Information Technology, Chengdu, 610225, China.

[2] School of Engineering and Technology, University of Hertfordshire, Hertford, UK.

[*] Corresponding Author: Yan Chang. Email: cyttkl@cuit.edu.cn.

Received: 17 February 2020; Accepted: 31 May 2020.

[Goldenberg and Vaidman (1995)] proposed a GV95 protocol based on orthogonal quantum states. In addition, there are many other key distribution protocols, such as entanglement exchange [Li and Liu (2018); Liu, Gao, Liu et al. (2019)], continuous variable quantum states [Liu and Min (2019)], decoy [Zhao and Shi (2019)] states and so on [Ge, Liu, Xia et al. (2019); Qu, Wu, Wang et al. (2017)].

Quantum secure direct communication (QSDC) is an information carrier of the communication and reception by the two parties in a quantum state. It transmits the confidential information directly through the quantum channel. In 2002, domestic scholars Long et al. [Long and Liu (2002)] proposed the first quantum secure direct communication scheme. Subsequently, more and more scholars began to make progress in this direction, put forwarding device-independent solutions [Zhou, Sheng and Long (2019)], anti-collective noise protocols [He and Ma (2019); Qu, Li, Xu et al. (2019)], etc. In addition, quantum secret sharing (QSS) has been adopted in their research, such as in Zhang et al. [Zhang, Shi, Hu et al. (2018); Cao and Ma (2019)] since Hillery et al. [Hillery, Buzek, Berthiaume et al. (1999)] proposed the first quantum secret sharing protocol based on the three-particle GHZ state in 1999. Until 2004, Lance et al. [Lance, Symul and Bowen (2004)] and others first called the quantum secret sharing of quantum information a quantum state sharing (QSTS) [Lance, Symul, Bowen et al. (2004)]. Subsequently, domestic and foreign scholars proposed to share arbitrary single qubits [Kang and Liao (2019)], multiple qubits [Su and Chen (2019)], and the quantum state sharing protocol based on Bell state [Gao, Wei and Wang (2019)].

In traditional contract signing, both parties must sign the same copy of the contract at the same time to produce the commitment to the contract simultaneously. However, the signing of the contract in the network environment must be asynchronous, so the electronic contract came into being [Xiong (2018)]. However, the security of traditional electronic contracts is based on mathematical problems such as large number decomposition and discrete logarithm. With the development of quantum cryptography, quantum computing will pose a serious threat to the security of traditional electronic contracts. Therefore, the signing of electronic contracts based on new quantum cryptography technology has attracted people's attention.

In 2006, Y. H. Chou [Chou, Tsai, Ko et al. (2006)], a Taiwan scholar in China, first proposed the concept of quantum electronic contract signing, and designed the first two-party quantum electronic contract signing scheme based on the cryptography idea of quantum inadvertent transmission. In 2008, Czech scholar Bouda and others [Bouda, Mateus, Paunkovic et al. (2008)] proposed a simple two-party electronic contract signing scheme by using quantum anti-interference equipment. However, honest participants could not determine whether the other party also promised the contract in terms of fairness. In 2011, Portuguese scholar Paunkovic and others [Paunkovic, Bouda and Mateus (2011)] proposed an optimistic and fair electronic contract signing scheme by using non-orthogonal quantum states. Compared with the previous quantum electronic contract signing scheme, the safety of the scheme is guaranteed by the basic principles of quantum physics, and it has certain advantages in efficiency and experimental implementation. In 2019, Cai and others [Cai, Wang and Wang (2019)] proposed a fair and optimistic contract signing scheme based on quantum cryptography. In the same year,

scholars from the University of Lisbon proposed a quantum contract signing scheme based on entangled pairs [Yadav, Mateus, Paunkovic et al. (2019)].

This paper proposes a quantum photo-based contract scheme based on the single photon. In this scheme, the signing parties sign two copies of the same contract and send copies of their respective signed contracts to a third party. The third party verifies and compares the copies of the two signatures by means of the correlation of the Bell state particles, and checks whether the signing parties signed the same contract and whether they signed the contract without the impersonation. If the verification is passed, the third party determines that the parties to the contract have reached an agreement, then the contract is valid; otherwise the contract is invalid. Since the program reduces the number of steps between signing parties to exchange signatures, both parties to the contract and the third party must be honest and reliable. In addition, the operation of the third party enables the contract signing parties to communicate securely in the presence of Eve, and can detect and terminate the communication timely when Eve intervenes in the solution.

2 Quantum scheme of an electronic contract

This scheme includes two contract signers Alice, Bob and a trusted third party Charlie. Alice and Bob sign two copies of the same contract, and then they send their signed copies of the contract to Charlie, who checks whether the two signed copies are the same. This scheme includes three phases: initialization phase, signing phase and verification phase.

2.1 Initialization phase

(1) Charlie and Alice share their keys through QKD, $k_A = \{k_{A1}, k_{A2}, ..., k_{Ai}, ..., k_{A2n}\}$, $k_{Ai} = \{00,01,10,11\}$ and Charlie and Bob share their keys through QKD, $k_B = \{k_{B1}, k_{B2}, ..., k_{Bi}, ..., k_{B2n}\}$, $k_{Bi} = \{00,01,10,11\}$.

(2) Charlie prepares quantum sequences randomly as $S_A = \{A_1, A_2, ..., A_i, ..., A_n\}$ and $S_B = \{B_1, B_2, ..., B_i, ..., B_n\}$, $A_i, B_i \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$.

(3) Charlie performs corresponding unitary operations on S_A according to k_A (Tab. 1 for specific operation rules). The four unitary operations are expressed as Eqs. (1)-(4):

$$U_{00} = I = |0\rangle\langle 0| + |1\rangle\langle 1| \tag{1}$$

$$U_{01} = Z = |0\rangle\langle 0| - |1\rangle\langle 1| \tag{2}$$

$$U_{10} = X = |1\rangle\langle 0| + |0\rangle\langle 1| \tag{3}$$

$$U_{11} = Y = |1\rangle\langle 0| - |0\rangle\langle 1| \tag{4}$$

The sequence after the pass-through operation is recorded as S_A'. In order to detect the eavesdropping, Charlie inserts a decoy photon sequence into the sequence S_A' and declines the state of particles in a photon sequence randomly from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, sending S_A' to Alice. When Alice receives the sequence S_A', she informs Charlie that she has received the sequence. Then Charlie tells Alice the position and measurement base of the trapped photon.

Alice uses the measurement base published by Charlie to measure the trapped photon and publish the measurement results. Charlie analyzes the error rate. If the error rate is higher than the threshold, stop the process. Otherwise, proceed to the next stage.

Table 1: Unitary operation rules

The key $k_{Ai}(k_{Bi})$	Unitary operations
00	U_{00}
01	U_{01}
10	U_{10}
11	U_{11}

(4) Similarly, Charlie performs corresponding unitary operations on S_B according to k_B. The sequence after the pass-through operation is recorded as $S_B^{'}$. Also, eavesdropping detection is carried out. Charlie inserts a decoy photon sequence into sequence $S_B^{'}$ and declines the state of particles in a photon sequence randomly from $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$, sending $S_B^{'}$ to Bob. When Bob receives the sequence $S_B^{'}$, he informs Charlie that he has received the sequence. Then Charlie tells Bob the position and measurement base of the trapped photon. Bob uses the measurement base published by Charlie to measure the trapped photon and publish the measurement results. Charlie analyzes the error rate. If the error rate is higher than the threshold, stop the process. Otherwise, proceed to the next stage.

2.2 Signing phase

(1) Alice and Bob sign two copies of the same contract separately. They quantize and code $M_A=\{m_{A1},m_{A2},...,m_{Ai},...,m_{An}\}$ and $M_B=\{m_{B1},m_{B2},...,m_{Bi},...,m_{Bn}\}$, $m_{Ai},m_{Bi}\in(0,1)$, separately. The result is expressed as $P_A=\{p_{A1},p_{A2},...,p_{Ai},...,p_{An}\}$ and $P_B=\{p_{B1},p_{B2},...,p_{Bi},...,p_{Bn}\}$, where $p_{Ai},p_{Bi}\in(|0\rangle,|1\rangle)$. The coding rule is: if $m_{Ai}/m_{Bi}=0$, then $p_{Ai}/p_{Bi}=|0\rangle$; if $m_{Ai}/m_{Bi}=1$, then $p_{Ai}/p_{Bi}=|1\rangle$.

(2) Alice discards the decoy photon, measures $S_A^{'}$ with a Z basis, and records the measurement a $R_A=\{r_{A1},r_{A2},...,r_{Ai},...,r_{An}\}$, $r_{Ai}\in(|0\rangle,|1\rangle)$. Then Alice entangles R_A and P_A in Bell state according to priority. The steps are as follows:

Step ①: R_A first passes Hadamard Gate to transform into $R_A^{'}=\{r_{A1}^{'},r_{A2}^{'},...,r_{Ai}^{'},...,r_{An}^{'}\}$, $r_{Ai}^{'}\in(|+\rangle,|-\rangle)$. Hadamard Gate can be represented as:

$$H=\frac{1}{\sqrt{2}}[(|0\rangle+|1\rangle)\langle 0|+(|0\rangle-|1\rangle)\langle 1|] \tag{5}$$

Step ②: $R_A^{'}$ and P_A go through CNOT-Gate together, where $R_A^{'}$ is the control qubit and P_A is the target bit. If $r_{Ai}=|0\rangle$, then the state of p_{Ai} particle remains unchanged;

if $r_{Ai} = |1\rangle$, then the state of p_{Ai} particle changes contrary. Record the result as $\Theta_A = \{\Theta_{A1}, \Theta_{A2}, ..., \Theta_{Ai}, ..., \Theta_{An}\}$.

Table 2: The process and result of the Bell state entanglement operation on any two particles

(r_{Ai}, p_{Ai}) or (r_{Bi}, p_{Bi})	$r_{Ai}/r_{Bi} \otimes H$	$CNOT((r_{Ai}, p_{Ai}) or (r_{Bi}, p_{Bi}))$	Bell-based measurement
$\|0\rangle, \|0\rangle$	$H\|0\rangle = \frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	$\|\Phi^+\rangle$
$\|0\rangle, \|1\rangle$	$H\|0\rangle = \frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$\frac{1}{\sqrt{2}}(\|01\rangle + \|10\rangle)$	$\|\Psi^+\rangle$
$\|1\rangle, \|0\rangle$	$H\|1\rangle = \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$	$\|\Phi^-\rangle$
$\|1\rangle, \|1\rangle$	$H\|1\rangle = \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\frac{1}{\sqrt{2}}(\|01\rangle - \|10\rangle)$	$\|\Psi^-\rangle$

For example, if $r_{A1} = |1\rangle$, $p_{A1} = |0\rangle$, then perform a Bell state entanglement on $r_{A1}p_{A1} = |00\rangle$. First of all, r_{A1} passes Hadamard Gate to transform into $r'_{A1} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $r'_{A1}p_{A1} = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$, and then $r'_{A1}p_{A1}$ go through CNOT-Gate together; r'_{A1} is the control qubit and P_A is the target bit. Finally, $r_{A1}p_{A1} = |00\rangle$ converts to $\Theta_{A1} = |\Phi^+\rangle$.

(3) Alice performs the unitary operation on the first particle of Θ_A according to k_A (Table 1 for specific operation rules), records the result as Θ_A', and sends Θ_A' to Charlie with Alice's signature on the copy of the contract M_A.

(4) Similarly, Bob does the same steps as Alice. Bob discards the decoy photon, measures S'_B with a Z basis, records the measurement as $R_B = \{r_{B1}, r_{B2}, ..., r_{Bi}, ..., r_{Bn}\}$, and then entangles R_B and P_B in Bell state according to priority. And then Bob performs the unitary operation on the first particle of Θ_B according to k_B, records the result as Θ_B', sends Θ_B' to Charlie with Bob's signature on the copy of the contract M_B.

2.3 Verification phase

(1) After Charlie received the signature sent by Alice, he measures Θ_A' with Bell base and records the result as $R(\Theta_A')$. From the relationship between particle results of each process in Tab. 3, Charlie can deduce the result of M_A according to S_A, unitary operation and $R(\Theta_A')$.

Table 3: Results of particles in each process

A_i/B_i	Unitary operation	$A_i^{'}/B_i^{'}$	r_{Ai}/r_{Bi}	M_{Ai}/M_{Bi}	p_{Ai}/p_{Bi}	Θ_{Ai}/Θ_{Bi}	$R(\Theta_{Ai}^{'})/R(\Theta_{Bi}^{'})$
$\|0\rangle$	U_{00}	$\|0\rangle$	$\|0\rangle$	0	$\|0\rangle$	$\|\Phi^+\rangle$	$\|\Phi^+\rangle$
				1	$\|1\rangle$	$\|\Psi^+\rangle$	$\|\Psi^+\rangle$
	U_{01}	$\|0\rangle$	$\|0\rangle$	0	$\|0\rangle$	$\|\Phi^+\rangle$	$\|\Phi^-\rangle$
				1	$\|1\rangle$	$\|\Psi^+\rangle$	$\|\Psi^-\rangle$
	U_{10}	$\|1\rangle$	$\|1\rangle$	0	$\|0\rangle$	$\|\Phi^-\rangle$	$\|\Psi^-\rangle$
				1	$\|1\rangle$	$\|\Psi^-\rangle$	$\|\Phi^-\rangle$
	U_{11}	$\|1\rangle$	$\|1\rangle$	0	$\|0\rangle$	$\|\Phi^-\rangle$	$\|\Psi^+\rangle$
				1	$\|1\rangle$	$\|\Psi^-\rangle$	$\|\Phi^+\rangle$
$\|1\rangle$	U_{00}	$\|1\rangle$	$\|1\rangle$	0	$\|0\rangle$	$\|\Phi^-\rangle$	$\|\Phi^-\rangle$
				1	$\|1\rangle$	$\|\Psi^-\rangle$	$\|\Psi^-\rangle$
	U_{01}	$\|1\rangle$	$\|1\rangle$	0	$\|0\rangle$	$\|\Phi^-\rangle$	$\|\Phi^+\rangle$
				1	$\|1\rangle$	$\|\Psi^-\rangle$	$\|\Psi^+\rangle$
	U_{10}	$\|0\rangle$	$\|0\rangle$	0	$\|0\rangle$	$\|\Phi^+\rangle$	$\|\Psi^+\rangle$
				1	$\|1\rangle$	$\|\Psi^+\rangle$	$\|\Phi^+\rangle$
	U_{11}	$\|0\rangle$	$\|0\rangle$	0	$\|0\rangle$	$\|\Phi^+\rangle$	$\|\Psi^-\rangle$
				1	$\|1\rangle$	$\|\Psi^+\rangle$	$\|\Phi^-\rangle$
$\|+\rangle$	U_{00}	$\|+\rangle$	$\|0\rangle$	0	$\|0\rangle$	$\|\Phi^+\rangle$	$\|\Phi^+\rangle$
				1	$\|1\rangle$	$\|\Psi^+\rangle$	$\|\Psi^+\rangle$
			$\|1\rangle$	0	$\|0\rangle$	$\|\Phi^-\rangle$	$\|\Phi^-\rangle$
				1	$\|1\rangle$	$\|\Psi^-\rangle$	$\|\Psi^-\rangle$
	U_{01}	$\|-\rangle$	$\|0\rangle$	0	$\|0\rangle$	$\|\Phi^+\rangle$	$\|\Phi^-\rangle$
				1	$\|1\rangle$	$\|\Psi^+\rangle$	$\|\Psi^-\rangle$
			$\|1\rangle$	0	$\|0\rangle$	$\|\Phi^-\rangle$	$\|\Phi^+\rangle$
				1	$\|1\rangle$	$\|\Psi^-\rangle$	$\|\Psi^+\rangle$
	U_{10}	$\|+\rangle$	$\|0\rangle$	0	$\|0\rangle$	$\|\Phi^+\rangle$	$\|\Psi^-\rangle$
				1	$\|1\rangle$	$\|\Psi^+\rangle$	$\|\Phi^+\rangle$
			$\|1\rangle$	0	$\|0\rangle$	$\|\Phi^-\rangle$	$\|\Psi^-\rangle$
				1	$\|1\rangle$	$\|\Psi^-\rangle$	$\|\Phi^-\rangle$
	U_{11}	$\|-\rangle$	$\|0\rangle$	0	$\|0\rangle$	$\|\Phi^+\rangle$	$\|\Psi^-\rangle$
				1	$\|1\rangle$	$\|\Psi^+\rangle$	$\|\Phi^-\rangle$
			$\|1\rangle$	0	$\|0\rangle$	$\|\Phi^-\rangle$	$\|\Psi^+\rangle$
				1	$\|1\rangle$	$\|\Psi^-\rangle$	$\|\Phi^+\rangle$

$\|-\rangle$	U_{00}	$\|-\rangle$	$\|0\rangle$	0	$\|0\rangle$	$\|\Phi^+\rangle$	$\|\Phi^-\rangle$
				1	$\|1\rangle$	$\|\Psi^+\rangle$	$\|\Psi^-\rangle$
			$\|1\rangle$	0	$\|0\rangle$	$\|\Phi^-\rangle$	$\|\Phi^+\rangle$
				1	$\|1\rangle$	$\|\Psi^-\rangle$	$\|\Psi^+\rangle$
	U_{01}	$\|+\rangle$	$\|0\rangle$	0	$\|0\rangle$	$\|\Phi^+\rangle$	$\|\Phi^-\rangle$
				1	$\|1\rangle$	$\|\Psi^+\rangle$	$\|\Psi^-\rangle$
			$\|1\rangle$	0	$\|0\rangle$	$\|\Phi^-\rangle$	$\|\Phi^+\rangle$
				1	$\|1\rangle$	$\|\Psi^-\rangle$	$\|\Psi^+\rangle$
	U_{10}	$\|-\rangle$	$\|0\rangle$	0	$\|0\rangle$	$\|\Phi^-\rangle$	$\|\Psi^-\rangle$
				1	$\|1\rangle$	$\|\Psi^+\rangle$	$\|\Phi^+\rangle$
			$\|1\rangle$	0	$\|0\rangle$	$\|\Phi^-\rangle$	$\|\Psi^-\rangle$
				1	$\|1\rangle$	$\|\Psi^-\rangle$	$\|\Phi^-\rangle$
	U_{11}	$\|+\rangle$	$\|0\rangle$	0	$\|0\rangle$	$\|\Phi^+\rangle$	$\|\Psi^-\rangle$
				1	$\|1\rangle$	$\|\Psi^+\rangle$	$\|\Phi^-\rangle$
			$\|1\rangle$	0	$\|0\rangle$	$\|\Phi^-\rangle$	$\|\Psi^-\rangle$
				1	$\|1\rangle$	$\|\Psi^-\rangle$	$\|\Phi^+\rangle$

(2) Similarly, After Charlie receives the signature sent by Bob, he measures Θ_B' with Bell base and records the result as $R(\Theta_B')$. From the relationship between particle results of each process in Tab. 3, Charlie can deduce the result of M_B according to S_B, unitary operation and $R(\Theta_B')$.

(3) Charlie judges whether M_A and M_B are the same. If they are the same, the contract will take effect. Otherwise, the contract will not take effect. This scheme is illustrated in Fig. 1.

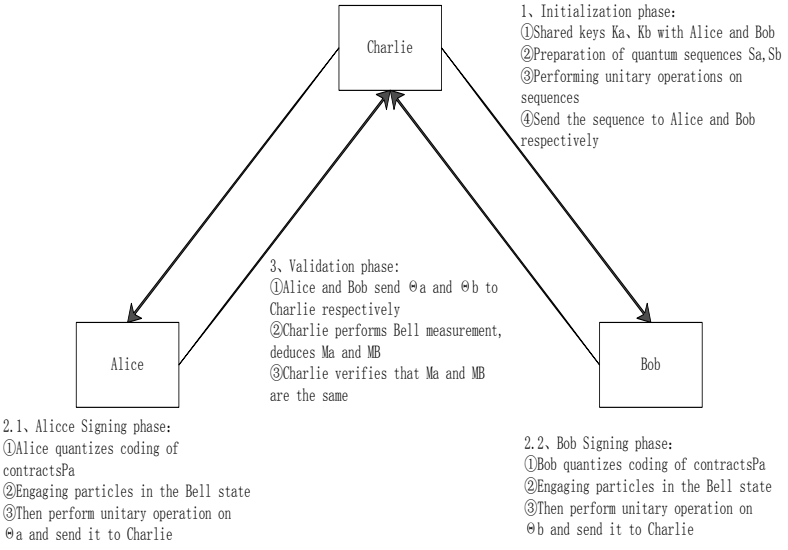

Figure 1: Simple process diagram of the quantum contract scheme based on the single photon

3 Security analysis

3.1 Non-repudiation of signature contracts

In the initial stage, Charlie randomly generates quantum sequences S_A and S_B, and sends them to Alice and Bob respectively through the unitary operation. Alice and Bob carry out the z-based measurement on the quantum sequences S_A' and S_B' received respectively, And then they entangle the Bell state with the particle sequence encoded by the contract copy in order, perform the unitary operation after getting Θ_A and Θ_B. Alice and Bob send Θ_A' and Θ_A' to Charlie. At this point, Charlie makes Bell-based measurements of Θ_A' and Θ_A' according to S_A and S_B. The results of the unitary operation and Bell-based measurement can verify whether Alice and Bob have repudiation behavior.

3.2 Impossibility of signing contract

Eve arbitrarily spoofs Alice and Bob. Suppose he pretends to be Alice and carries out a Z-based measurement after receiving S_A' sent by Charlie. The measurement result is recorded as R_{E_A}. He prepares the corresponding Bell state according to the measurement results. If $R_{E_A}=|0\rangle$, then he randomly prepares $|\Phi^+\rangle$ or $|\Phi^-\rangle$; if $R_{E_A}=|1\rangle$, then he randomly prepares $|\Psi^+\rangle$ or $|\Psi^-\rangle$. Afterward, Eve sends a series of Bell state particles that he has prepared to Charlie. Because Eve doesn't know the shared key k_A and the content of the contract M, he may be discovered by Charlie during the verification phase. The probability that he can spoof successfully is $\frac{3}{128}$. In the case where the quantum bit n of the contract M is sufficiently large and the shared key k_A with the number of 2n is sufficiently long, the probability that the Eve is falsely found is $1-\left(\frac{3}{128}\right)^n$, which is close to 1. Hence, this quantum electronic contract has no impersonation.

3.3 Interception/measurement/retransmission attack

In this attack, Eve wants to get the content of the contract. So he intercepts S_A' and S_B' sent by Charlie to Alice and Bob and measures them with Z-base. The measurement result is recorded as R_{E_A} and R_{E_B}. He sends the corresponding particles to Alice and Bob according to R_{E_A} and R_{E_B}. When Eve sends Charlie Θ_A' and Θ_B' to Alice and Bob, he intercepts Θ_A' and Θ_B' and measures them with Bell. The measurement result is recorded as $R_{\Theta E_A}$ and $R_{\Theta E_B}$. Then he infers the contract M according to R_{E_A}, R_{E_B} and $R_{\Theta E_A}$, $R_{\Theta E_B}$. Since Charlie sends S_A and S_B, the corresponding operations are performed on the particles based on the keys k_A and k_B shared by Alice and Bob. Alice and Bob also send them to Charlie after the operation of Θ_A' and Θ_B'. But Eve doesn't know the shared keys k_A and k_B, so he doesn't know which kind of operation is done on the particle. The probability that he guesses the contract content correctly is $\frac{1}{8}$. If the quantum bit n of the contract is large enough, then the probability of his guess is $1-\left(\frac{1}{8}\right)^n$,

which is close to 1; therefore, the program can resist interception/measurement/ retransmission attacks.

3.4 Eavesdropping detection

In the quantum channel, if there is a man-in-the-middle attack, then in the initial stage, Charlie sends a sequence S with a deceptive photon to Alice and Bob. If the channel is not safe, the eavesdropper must perform the particle before Alice and Bob receive the particle measured. At this time, Charlie does not announce the location and state of detecting the photon. The eavesdropper does not know the location and state of the photon, so he cannot choose the correct base to decoy the photon. According to the quantum immeasurable theorem, the state of the particle changes after being measured. Then, after Alice and Bob's measurement of the temptation of photons, Charlie will find that the state of the nuzzle photons inserted is different. Then, the eavesdroppers will be discovered. As a result, they will give up the newsletter.

4 Summary

A single photon-based quantum electron contract scheme is proposed in this paper. A trusted third party can verify and compare whether the two signing parties sign the same contract by means of the relevance of the Bell state, that is, whether the parties signing the contract have reached an agreement; at the same time, it guarantees the non-repudiation and impersonation of the signed contract. This solution reduces the steps of exchanging signatures between contract-signing parties and reduces communication complexity. At the same time, this scheme is to operate on the single photon, which is easy to operate and easy to implement. In the presence of Eve, it is possible to communicate securely, and when Eve intervenes in the solution, the scheme can detect and terminate the communication in time to ensure security.

Funding Statement: This work is supported by NSFC (Grant Nos. 61572086, 61402058), Sichuan Science and Technology Program (Grant Nos. 2017JY0168, 2018TJPT0012, 2018GZ0232, 2018CC0060, 2017GFW0119, 2017GZ0006, 2016GFW0127), the National Key Research and Development Program (No. 2017YFB0802302), Sichuan innovation team of quantum security communication (No. 17TD0009), and Sichuan academic and technical leaders training funding support projects (No. 2016120080102643).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

Bennett, C. H.; Brassard, G. (1984): Quantum cryptography: public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computer, System and Signal Processing*, Bangalore, India, pp. 175-179.

Bennett, C. H.; Wiesner, S. J. (1992): Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states. *Physical Review Letters*, vol. 69, no. 20, pp. 2881-2884.

Bouda, J.; Mateus, P.; Paunkovic, N.; Rasga, J. (2008): On the power of quantum tamper-proof devices. *International Journal of Quantum Information*, vol. 6, no. 2, pp. 281-302.

Cai, X. Q.; Wang, X. X.; Wang, T. Y. (2019): Fair and optimistic contract signing based on quantum cryptography. *International Journal of Theoretical Physics*, vol. 58, no. 11, pp. 3677-3683.

Cao, H.; Ma, W. P.; Lü, L. D.; He, Y. Y.; Liu, G. (2019): Multi-party quantum privacy comparison of size based on d-level GHZ states. *Quantum Information Processing*, vol. 18, no. 9, pp. 1-14.

Chou, Y. H.; Tsai, I. M.; Ko, C. M.; Kuo, S. Y.; Chen, I. Y. (2006): Quantum oblivious transfer and fair digital transactions. *IEEE Pacific Rim International Symposium on Dependable Computing*, vol. 1, pp. 121-128.

Gao, G.; Wei, C. C.; Wang, D. (2019): Cryptanalysis and improvement of dynamic quantum secret sharing protocol based on two-particle transform of Bell states. *Quantum Information Processing*, vol. 18, no. 6, pp. 1-9.

Ge, C. P.; Liu, Z.; Xia, J. Y.; Fang, L. M. (2019): Revocable identity-based broadcast proxy re-encryption for data sharing in clouds. *IEEE Transactions on Dependable and Secure Computing*, pp. 1.

Goldenberg, L.; Vaidman, L. (1995): Quantum cryptography based on orthogonal states. *Physical Review Letters*, vol. 75, no. 7, pp. 1239-1243.

He, Y. F.; Ma, W. P. (2019): Multiparty quantum secure direct communication immune to collective noise. *Quantum Information Processing*, vol. 18, no. 1, pp.1-11.

Hillery, M.; Buzek, V.; Berthiaume, A. (1999): Quantum secret sharing. *Physical Review A*, vol. 59, no. 3, pp. 1829-1834.

Jonathan, M. S.; Illari, P. (2019): Building general knowledge of mechanisms in information security. *Philosophy & Technology*, vol. 32, no. 4. pp. 627-659.

Kang, Y.; Liao, Q.; Geng, J.; Guo, Y. (2019): Continuous variable quantum secret sharing with Chinese remainder theorem. *International Journal of Theoretical Physics*, vol. 58, no. 12, pp. 3986-3997.

Lance, A. M.; Symul, T.; Bowen, W. P.; Sanders, B. C.; Lam, P. K. (2004): Tripartite quantum state sharing. *Physical Review Letters*, vol. 92, no. 17, 177903.

Li, D. F.; Liu, M. Z. (2018): Quantum entanglement death problem depict in two atomic systems. *International Journal of Theoretical Physics*, vol. 57, no. 5, pp. 1265-1271.

Liu, W. J.; Gao, P. P.; Liu, Z. H.; Chen, H. W.; Zhang, M. J. et al. (2019): A quantum-based database query scheme for privacy preservation in cloud environment. *Security and Communication Networks*, pp. 1-14.

Liu, Z. M.; Min, Q. Y.; Zhou, L. (2019): Generating postselected quantum state from fock state using ancillary squeezed-vacuum state and continuous-variable postselection. *International Journal of Theoretical Physics*, vol. 59, no. 2, pp. 361-373.

Long, G. L.; Liu, X. S. (2002): Theoretically effically high-capacity quantum-key-distribution scheme. *Physical Review A*, vol. 65, no. 3.

Paunkovic, N.; Bouda, J.; Mateus, P. (2011): Fair and optimistic quantum contract signing. *Physical Review A*, vol. 84, no. 6, 062331.

Qu, Z. G.; Wu, S. Y.; Wang, M. M.; Sun, L.; Wang, X. J. (2017): Effect of quantum noise on deterministic remote state preparation of an arbitrary two-particle state via various quantum entangled channels, *Quantum Information Processing*, vol. 16, no. 306, pp. 1-25.

Qu, Z. G.; Li, Z. Y.; Xu, G.; Wu, S. Y.; Wang, X. J. (2019): Quantum image steganography protocol based on quantum image expansion and grover search algorithm. *IEEE Access*, vol. 7, pp. 50849-50857.

Su, C. F.; Chen, C. Y. (2019): Information hiding method based on quantum image by using Bell states. *Quantum Information Processing*, vol. 19, no. 25, pp. 4709-4712.

Wang, J.; Gao, Y.; Liu, W.; Wu, W. B.; Lim, S. J. (2019): An asynchronous clustering and mobile data gathering schema based on timer mechanism in wireless sensor networks, *Computers, Materials & Continua*, vol. 58, no. 3, pp. 711-725.

Xiong, C. Y. (2018): E-contract application in cloud service based on network environment. *Electronic World*, no. 22, pp. 50-52.

Yadav, P.; Mateus, P.; Paunković, N.; Souto, A. (2019): Quantum contract signing with entangled pairs. *Quantum Information*, vol. 21, no. 9, pp. 821.

Zhao, W.; Shi, R. H.; Feng, Y. Y.; Huang, D. (2019): Unidimensional continuous-variable quantum key distribution with discrete modulation. *Physics Letters A*. vol. 384, no. 2.

Zhang, W. Y.; Shih, F. Y.; Hu, S. B.; Jian, M. W. (2018): A visual secret sharing scheme based on improved local binary pattern. *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 32, no. 6.

Zhou, L.; Sheng, Y. B.; Long, G. L. (2019): Device-independent quantum secure direct communication against collective attacks. *Science Bulletin*, vol. 65, no. 1, pp. 12-20.