IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 13, 2018, accepted December 25, 2018, date of publication January 3, 2019, date of current version January 23, 2019.

Digital Object Identifier 10.1109/ACCESS.2018.2890166

Deterministic Quantum Secure Direct Communication Protocol Based on Omega State

LEILEI LI[1], JIAN LI[1], CHAOYANG LI[1], HENGJI LI[1], YUAN TIAN[1], YAN ZHENG[1], AND YUGUANG YANG[2]

[1]School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2]College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China

Corresponding author: Jian Li (buptlijian@126.com)

This work was supported by the National Natural Science Foundation of China under Grant U1636106, Grant 61472048, and Grant 61572053.

ABSTRACT A quantum secure direct communication (QSDC) protocol is presented. In the proposed protocol, the omega state is introduced to detect the eavesdropping during the quantum communication, eavesdropping behaviors will change the state of the omega state, and the sender Alice and the receiver Bob detect eavesdropping through the state measurement results. The relationship between the amount of information that the eavesdropper gets and the probability of being detected is also given. Compared with the original QSDC protocol based on the Bell state, when the same amount of information is obtained, the eavesdropper must face a higher detection probability in the proposed protocol, and the eavesdropper mostly can obtain 0.676 (bit) of information. The security analysis is also given, and the result indicates that the proposed protocol is more secure. A simulation based on the law of large number and the Monte Carlo method is also given, and the mean square error is introduced to describe the similarity between the simulation data and the theoretical value. The simulation result indicates that the proposed security in an ideal environment and the security analysis are correct, and the proposed protocol is more secure by sending more quantum particles in detecting eavesdropping.

INDEX TERMS Omega state, eavesdropping detection, security analysis, information entropy, simulation.

I. INTRODUCTION

How to distribute the key is a very important research in cryptography. The only key distribution protocol which has been proved the theoretical security by Shannon [1] is One-time pad(OTP) presented by Vernam [2] in 1926. However OTP needs to transmit a key which is equal to the cipher text, making it's difficult to apply. Today's widely used cryptography systems are usually based on the computational complexity [3]–[5], the eavesdropper cannot calculate the key in finite time, but their theoretical security have not been proved. In 1994, Shor [6] presented a quantum Las Vegas algorithm, indicating that the classical cryptography systems can be cracked in the future.

Different from the classical secure communication protocols' security are based on the complexity of computation, the quantum secure communication(QSC) protocols are based on the laws of physics, so QSC's security can be proved in theory. Quantum communication and quantum Cryptography mainly includes quantum key distribution (QKD) [7]–[9], quantum teleportation (QT) [10], [11], quantum secret sharing (QSS) [12], quantum secure direct communication (QSDC) [13]–[15], etc. In 1984, Bennett and Brassard [16] presented the first QKD protocol, which called the BB84 protocol. This protocol indicted that quantum qubits can replace classical bits in communication, the BB84 protocol and its improve protocols are still widely used in quantum communication [16]–[21].

Compared with QKD protocol, QSDC protocol can not tolerate the lack of the quantum information. In another word, QSDC protocol needs much more higher security requirement. In 2002, Long and Liu [22] present a QSDC protocol based on the Einstein-Podolsky-Rosen (EPR) pair [23]. He present an excellent idea of using quantum information blocks instead of quantum information bits, making QSDC is easily to applicate in theory. Before transmitting the secure message, one of communication parties can ensure the security of the quantum communication channel with the help of the quantum data block. Eavesdropping will cause the bit error in the data block. Same with the idea in [24] the block of entangled particles is divided into

two sequences: the checking(control) sequence(in control mode) is used to checking Eve's eavesdropping behavior and message-coding(message) sequence(in message mode) is used to transmit the secure message [23].

However, the original present protocol's [23] effect of detecting eavesdropping is low. A quantum secure direct communication protocol based on the quantum Omega state $|\Omega\rangle$ [25]–[27] and the idea presented in [22], [23], and [28] is presented to enhance the detection efficiency on Original present protocol which is based on EPR pairs and Bell states. Bob transmits the $|\Omega\rangle$ to Alice, and Alice takes a measurement to detect the eavesdropper Eve. To facilitate the expression, the protocol present in [23] is called ''OPP''(Original Present Protocol) in this paper and the proposed QSDC protocol based on Omega state in this paper is called ''SPP''(Second Present Protocol). The method of the entropy theory is introduced during the security analysis and it has been proved that if Eve wants to get more Information, she must face a large detection efficiency in SPP. In our secure analysis, Eve's eavesdropping can at most obtain about 0.676 information. The secure of SPP is also proved, the more qubits used in checking sequence, the more secure that SPP will be. Compared with OPP, SPP is more secure, but SPP faces the cost of sending more particles.

A simulation based on the law of large number [29], [30] and Monte Carlo method [31]–[33] is also presented. The times of the eavesdropper Eve attempts to gain n bits without being detected $\hat{t}_n$ is simulated and the theoretical value t_n is also calculated. The mean square error(MSE) is introduced to describe the similarity between the simulation data $\hat{t}_n$ and the theoretical value t_n. With the given detecting probability $d = 0.5$ and the given probability that Alice and Bob change into control mode $c = 0.5$, when Eve tries to get $n = 10$ classical bits without being detected, the theoretical times of attempts is $t_{10} = 57.67$. After 1000 times of simulation, the simulation data $\hat{t}_{10}$ is approaching to the theoretical value t_{10}, and the value of MSE is approaching to 0. The simulation result indicates the SPP protocol is security in ideal environment and the security analysis in this paper is right.

II. QSDC PROTOCOL BASED ON THE OMEGA STATE

A. THE BELL STATE AND OMEGA STATE

The four Bell states can be written as:

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$$
$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \quad (1)$$

If takes a Bell measurement in two particles, the measurement result should be one of the four Bell state. If takes a B_z or B_x measurement on each particle, the measurement results should be always the same when it's $|\Phi^{\pm}\rangle$ and the result should be always different when it's $|\Psi^{\pm}\rangle$. When in message sequence, Bob takes a Bell measurement after he receives the travel qubit from Alice; In control sequence, both Alice and Bob takes the same B_z or B_x measurement on their holden qubit to detect the Eve's eavesdropping.

The Omega state [26] can be written as:

$$|\Omega\rangle = \frac{1}{\sqrt{2}}(|0\rangle|B_0\rangle|0\rangle + |1\rangle|B_1\rangle|1\rangle) \quad (2)$$

where $(|B_0\rangle, |B_1\rangle \in \{|\Psi^{\pm}\rangle, |\Phi^{\pm}\rangle\})$, in other words, there are total 16 Omega states can be generated through the Bell state and all of the Omega states can be used in detecting eavesdropping. In this paper, let's suppose $|B_0\rangle = |\Phi^{+}\rangle, |B_1\rangle = |\Phi^{-}\rangle$, the Eq. 2 can be rewritten:

$$\begin{aligned}|\Omega\rangle &= \frac{1}{\sqrt{2}}(|0\rangle|\Phi^{+}\rangle|0\rangle + |1\rangle|\Phi^{-}\rangle|1\rangle)\\ &= \frac{1}{2}(|0000\rangle + |0110\rangle + |1001\rangle - |1111\rangle)\\ &= \frac{1}{2}(|\Omega^{(0)}\rangle + |\Omega^{(1)}\rangle + |\Omega^{(2)}\rangle - |\Omega^{(3)}\rangle) \quad (3)\end{aligned}$$

Eq. 3 shows that the Omega state $|\Omega\rangle$ can be used in SPP to improved the effect of detecting eavesdropping.

B. THE BRIEF INTRODUCTION OF SPP PROTOCOL

The SPP protocol with $|\Omega\rangle$ can be described as the following steps:

1) Suppose Alice wants to transmit N(bit) classical bits to Bob, Bob prepares enough Bell states as the message sequence and enough $|\Omega\rangle$ states as the checking sequence C. If the probability of changing into control mode is c, Bob needs to prepares $cN/(1-c)$ $|\Omega\rangle$ states and N Bell states.
2) Just like OPP, Bob uses one particle of each Bell state to form the message qubits sequence A, which is used to transmit the secure message. Then Bob randomly inserts the checking sequence C into sequence A and stores their positions. Now, Bob has gotten his final travel data sequence block T, and the length of ($T = A \cup C$) is $N + 4cN/(1-c)$, where N is the length of the message qubits sequence A and $4cN/(1-c)$ is the length of the checking sequence C.
3) Bob transmits T to Alice, Alice gives a confirmation to Bob through a public channel after her receives transmits sequence T. Then Bob tells Alice the position of C, Alice extracts the checking qubits from T to get the message qubits sequence A and the checking sequence C.
4) Alice takes an Omega measurement on the checking sequence C, the measurement result should always be $|\Omega\rangle$ if there is no eavesdropping in ideal environment. Eve's eavesdropping will cause a bit error rate ber. If ber larger than the threshold, Alice and Bob think that the quantum communication is not safe, they will interrupt this communication and restart a new one. If ber less than threshold, Alice and Bob think the channel is safe and they will continue this communication.
5) Alice and Bob have confirmed the security of the quantum channel with this data block T, they will use the

message sequence A to transmit the security message like the OPP, Alice inserts new Omega state like step 2 and Bob detects eavesdropping with Omega state like step 4 again to make sure the security of the quantum channel.

6) Alice and Bob have successfully transmitted N(bit) classical bits, they repeat step 1) to step 6) until they finish transmitting the whole message.
7) The SPP protocol ends successfully.

Supposed the totally qubits cost is n_O in OPP and n_S in SPP, the extra cost of qubits in SPP Δ_q can be easily calculated:

$$\begin{aligned}\Delta_q &= n_S - n_O \\ &= (2N + \frac{4cN}{1-c}) - (2N + \frac{2cN}{1-c}) \\ &= \frac{2cN}{1-c}\end{aligned} \tag{4}$$

In next section, the security analysis of SPP will be given, and the comparison that SPP is more security via using more qubits in detecting eavesdropping is also discussed.

III. SECURITY ANALYSIS

Reference [34] has proved if the amount of information that the receiver Bob gets from the sender Alice $I(A, B)$ is larger than Eve's gain $I(A, E)$, the quantum commutation protocol is feasible. So the security of SPP can be proved with the information theory.

Suppose d is the probability that Eve takes an eavesdropping operation, according to [22]–[24] and [28]. The expression of the maximal amount of the information that Eve can get in OPP $I(d_{OPP})$ have been given, which is similar to cross entropy formula:

$$I(d_{OPP}) = -\left(d\log_2(d) + (1-d)\log_2(1-d)\right) \tag{5}$$

Eve doesn't know the position of sequence C, so she has to take the same eavesdropping operation on every qubits. Eve doesn't know any information about the qubits. Suppose the qubit that Eve measurement is $|0\rangle$ or $|1\rangle$ with the same probability $p = 1/2$. The effect of eavesdropping can be describe as the following Eq. 6:

$$E = \begin{pmatrix}\alpha & m \\ \beta & n\end{pmatrix} \tag{6}$$

where α, β, m, n is are normalization parameter that satisfy:

$$\begin{cases}|\alpha|^2 + |\beta|^2 = |m|^2 + |n|^2 = 1, \\ 0 \le \alpha, \beta, \quad m, n \le 1\end{cases} \tag{7}$$

In this matrix, the pure state $|0\rangle, |1\rangle$ will change into a mixed state, where:

$$\begin{cases}|E_{|0\rangle}\rangle = E|0\rangle = \alpha|0\rangle + \beta|1\rangle \\ |E_{|1\rangle}\rangle = E|1\rangle = m|0\rangle + n|1\rangle\end{cases} \tag{8}$$

Let's take $|\Omega^{(0)}\rangle = |0000\rangle$ into analysis, after Eve's eavesdropping, $|\Omega^{(0)}\rangle$ will change into a mix state as Eq. 9.

$$\begin{aligned}|\Omega^{(0)}\rangle_E &= E \otimes |\Omega^{(0)}\rangle \\ &= E \otimes |0000\rangle \\ &= |E_{|0\rangle}\rangle \otimes |E_{|0\rangle}\rangle \otimes |E_{|0\rangle}\rangle \otimes |E_{|0\rangle}\rangle\end{aligned} \tag{9}$$

Then, let's expand Eq. 9:

$$\begin{aligned}|\Omega^{(0)}\rangle_E = \alpha^4|0000\rangle + \alpha^2\beta^2|0110\rangle \\ +\alpha^2\beta^2|1001\rangle + \beta^4|1111\rangle + |\Omega^{(0)}\rangle_w\end{aligned} \tag{10}$$

where $|\Omega^{(0)}\rangle_w$ is the situation that Eve gets wrong result. From Eq.10, after Eve takes an eavesdropping operation, the probability that she still gets $|\Omega\rangle$ is:

$$p_{(|\Omega^{(0)}\rangle)} = |\alpha^4|^2 + |\alpha^2\beta^2|^2 + |\alpha^2\beta^2|^2 + |\beta^4|^2 \tag{11}$$

with the same idea, the rest of three state can be easily calculated:

$$\begin{aligned}p_{(|\Omega^{(1)}\rangle)} &= |\alpha^2m^2|^2 + |\alpha^2n^2|^2 + |m^2\beta^2|^2 + |\beta^2n^2|^2 \\ p_{(|\Omega^{(2)}\rangle)} &= |\alpha^2m^2|^2 + |m^2\beta^2|^2 + |\alpha^2n^2|^2 + |\beta^2n^2|^2 \\ p_{(|\Omega^{(3)}\rangle)} &= |m^4|^2 + |m^2n^2|^2 + |m^2n^2|^2 + |n^4|^2\end{aligned} \tag{12}$$

According to the symmetry and Eq. 3, the probability that Eve still gets $|\Omega\rangle$ state $p_{|\Omega\rangle}$ can be easy calculate:

$$p_{|\Omega\rangle} = \left(\frac{1}{2}\right)^2 \sum_{i=0}^{3} p_{(\Omega^{(i)})} \tag{13}$$

Eq. 13 shows the probability that Eve gets the same Omega state as Alice, so the probability that Eve's eavesdropping being detected in SPP can be gotten:

$$d_{SPP} \ge 1 - p_{|\Omega\rangle} \tag{14}$$

Suppose $|\alpha|^2 = a$, $|m|^2 = t$, so the amount of information that Eve gets I_0 when Bob sends 0 and I_1 when Bob sends 1 can be calculated:

$$\begin{cases}I_0 = H(a) = -\left(a\log_2(a) + (1-a)\log_2(1-a)\right) \\ I_1 = H(t) = -\left(t\log_2(t) + (1-t)\log_2(1-t)\right)\end{cases} \tag{15}$$

If Bob sends 0 or 1 with the same probability, according to the symmetry of α and m, when $a = t$ Eve can get most information:

$$I = \frac{1}{2}I_0 + \frac{1}{2}I_1 = H(a) \tag{16}$$

When $a = t$ Eve can get most information with the minimal probability of being detected.

$$d_{SPP} = 1 - p_{|\Omega\rangle} = -4a^4 + 8a^3 - 8a^2 + 4a \tag{17}$$

Eq. 17 is a quartic equation of a, and its solutions have been given by Ferrari. Based the idea of kernel method in the theory of Support Vector Machine (SVM), and suppose $a = k(d)$ which satisfy Eq. 17:

$$4(k(d))^4 - 8(k(d))^3 + 8(k(d))^2 - 4(k(d)) + d = 0 \tag{18}$$

With different value of $d \in (0, 0.5)$, the solution of $a = k(d)$ can be given through MATLAB or Python with the Newton method.

According to the Eq. 18, the amount of information that Eve gets in SPP is:

$$I(d_{SPP}) = H(k(d)) \tag{19}$$

According to the Eq. 5 and 14, the different amount of information in two detection strategies with the same detecting probability $d \in (0, 0.5)$ [24], [28] can be given. The relationship of the information I that Eve can gets in OPP and SPP with the same detecting probability $d \in (0, 0.5)$ is shown in Fig. 1.

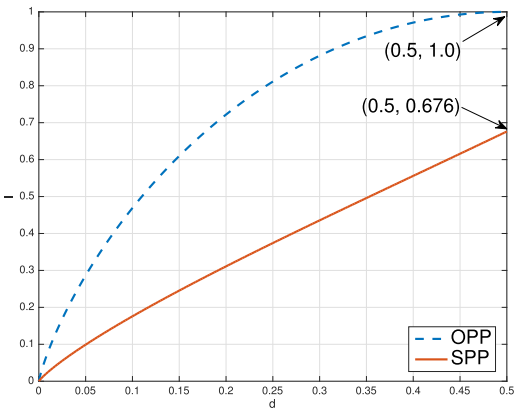


FIGURE 1. The relationship between the information that Eve gets *I* and the detecting probability *d*.

From Fig. 1, it can be concluded that the information that Eve gets in SPP is always less than OPP when $d \in (0, 0.5)$. The maximum amount of information that Eve gets is 0.676 in SPP while 1 in OPP. So it has been proved that the present improved detection strategy SPP has the better detection efficiency than OPP. However, according to the Eq. 4, SPP needs to send more $2cN/(1-c)$ qubits, in another words, SPP improves its detection efficiency via spending more qubits in detecting eavesdropping.

Now, let's analysis the security of the present SPP protocol with the theory of information. Suppose Alice and Bob have the probability of $c \in [0, 1]$ to choose the control sequence and every qubit which carry 1 information in message sequence, the average amount of information that qubit carry in SPP is $(1 - c)$. Assume that each communication is independent, and c_i means Alice and Bob sends i qubits in control sequence before send 1 message qubit, the probability that Eve gets 1 message transfer successfully without being detected s_1 can be described as:

$$\begin{aligned} s_1 &= \sum_{i=0}^{\infty} P(c_i|c) = \sum_{i=0}^{\infty} c^i (1-d)^i (1-c) \\ &\to \frac{1-c}{1-c(1-d)} \end{aligned} \tag{20}$$

When Eve successfully gets $I(d_{SPP})$ information transfer in 1 message qubit without being detected, the amount of probability is $(s_1)^{1/I(d_{SPP})}$, and $1/I(d_{SPP})$ is the expected times that Eve detects the communication. If Eve wants to gets $nI(d_{SPP})$ information from n message qubits, the successfully probability can be described as:

$$s_n = (s_1)^{n/I(d_{SPP})} = \left(\frac{1-c}{1-c(1-d)}\right)^{n/H(k(d)))} \tag{21}$$

Suppose Alice and Bob have the probability of $c = 0.5$ to choose control mode, Eq. 21 describes the relationship in the amount of information that Eve gets $n \in [0, 50]$, the probability $d \in (0, 0.5)$ that Eve takes an eavesdropping operation. and the probability $s \in [0, 1]$ that Eve successfully gets the information without being detected. Fig. 2 shows the relationship between n (the number of qubits used in detecting eavesdropping), s (the probability that Eve successfully gets the message sequence without being detected) and d (the probability that Eve successfully gets the $I(d_{SPP})$ message information) with $c = 0.5$ (the probability of changing into control mode). To observe the change s in different number of qubits n conveniently, given d a fixed value that $d \in \{0.01, 0.05, 0.5\}$, so the Fig. 2 can be reduced from three dimensions to two dimensions, just as Fig. 3 shows:

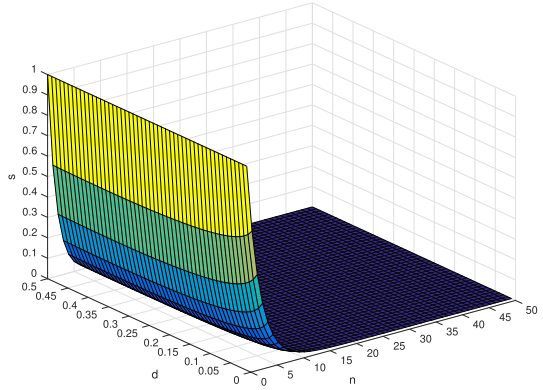


FIGURE 2. The relationship between *n*, *d* and *s*, with the increase of *n* from 0 to 50 and *d* from 0 to 0.5, *s* rapidly drops to 0. Indicating SPP is asymptotic safety.

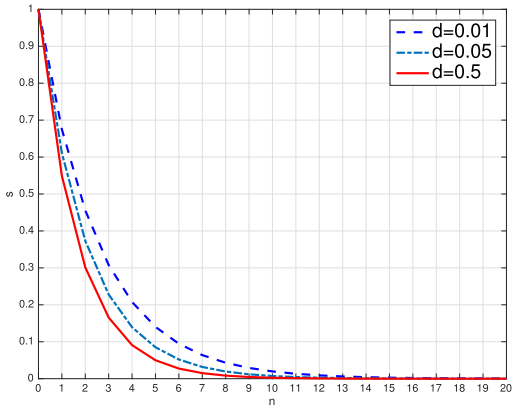


FIGURE 3. The relationship between *n* and *s* with a fixed value *d*.

TABLE 1. Simulation result of $\hat{t}_n$ and MSE with $n = 10$ and repeat algorithm 1 once.

value/times	10	50	100	200	300	500	750	1000
$\hat{t}_{10}$	87.33	55.49	59.98	55.21	60.18	57.48	57.07	56.64
MSE	880.2	10.34	5.357	6.023	6.344	0.035	0.352	1.060

When $d \in (0, 0.5)$ and $n \in [0, 50]$, with the increase of n, the value of s drops rapidly and $\lim_{n\to\infty} s = 0$. Suppose n is a fixed value, with the same n, the larger value of d, the larger gradient of s. In another word, the larger probability d that Eve tries to eavesdrop the information, the larger probability that Eve's eavesdropping behavior being detected. In our analysis, Eve can only gets part of the message without being detected, but she gets these information randomly, she doesn't know which part of information she has gotten, means what Eve's gets is useless.

In a word, the security of SPP with $d \in (0, 0.5)$ has been proved, and SPP can improved its detection effect via using more qubits in control sequence. After Alice and Bob confirm the security of the quantum channel, they can transmit information in message sequence just like OPP. SPP can not only detect the eavesdropping behavior in control sequence, but also transmit information in message sequence. So the SPP protocol has been proved to be secure as a QSDC protocol.

IV. SIMULATION BASED ON THE MONTE CARLO METHOD

The law of large number can be described as the following equation:

$$\lim_{n\to\infty} P\left\{\left|\frac{1}{n}\sum_{k=1}^{n} x_k - \frac{1}{n}\sum_{k=1}^{n} E_{x_k}\right| < \epsilon\right\} = 1 \tag{22}$$

where ϵ is small enough and always satisfied $\epsilon > 0$. Eq. 22 indicates if the count of simulation times n is big enough, the mean value of simulation data(x_k) will always approach to its theoretical value(E_{x_k}). Based the idea of the law of large number, the simulation with Monte Carlo method can be designed. After enough times of simulation, the simulation data $\hat{t}$ should approach to the theoretical value t, and the MSE between $\hat{t}$ and t should small enough.

Suppose $d = 0.5$ and $c = 0.5$, The value of $a = k(d) = 0.822$ can be calculated with Newton method. So the value of α, β, m, n can be also gotten. The probability of getting n bit without being detected can be described:

$$\begin{aligned} s_1 &= \sum_{i=0} c^i(1-d)^i(1-c) = \sum_{i=0}(\frac{1}{2})^{2i+1} \\ s_n &= (s_1)^n \end{aligned} \tag{23}$$

Suppose the theoretical times t_n of Eve tries before successfully getting n bits can be calculated:

$$t_n = \frac{1}{s_n} = (s_1)^{-n} \tag{24}$$

When calculated the value of $a = 0.822$, the distribution of the Omega state after eavesdropping by Eve can be calculated and the Omega state can be encode into $2^4 = 16$ classical bits during the simulation with the one-hot encoding.

Suppose the simulation data $\hat{t}$ means the mean number of the attempt count in T times simulation and the theoretical value t is calculated from Eq. 24. To describe the similarity between the simulation data $\hat{t}$ and the theoretical value t, the mean square error(MSE) is introduced:

$$MSE = \frac{1}{T}\sum_{i=1}^{T}(\hat{t}_n^i - t_n^i)^2 \tag{25}$$

The algorithm of the simulation can be described as algorithm 1. The algorithmic complexity of algorithm 1 is $O(tT) \to O(n^2)$. After repeating enough times of algorithm 1, we can conclude the less of the MSE, the more similarity of $\hat{t}$ and t, The Table 1 shows one of the simulation results of $\hat{t}_n$ and the MSE when $n = 10$, the Fig. 4 shows the change rule of MSE when $n = 10$ and simulation times $T \in [1, 300]$. From Eq. 24, the theoretical value when $n = 10$ is $t_{10} = 57.67$. From Table 1, after 1000 times of simulation on

Algorithm 1 The Algorithm of the Simulation Based on the Monte Carlo Method

Input: The simulation times T and the number of classical bits that Eve tries to detected n.

Output: The mean value of $\hat{t}_n$.

function MonteCarloSimulation(T, n)
  Initialize the theoretical value t_n from Eq. 24;
  Initialize current simulation data $\hat{t}_n = 0$;
  Initialize current count $c = 1$;
  for $c \le T$ **do**
    Initialize current gotten bits $n' = 0$;
    while $n' < n$ **do**
      Initialize current count $t = 1$;
      Take an Omega detecting, if Eve has been detected, $d_e = 1$, else $d_e = 0$;
      if $d_e == 1$ **then**
        $t \leftarrow t + 1$;
        continue;
      else
        $n' \leftarrow n' + 1$;
      end if
    end while
    $\hat{t}_n^c \leftarrow t$;
    $\hat{t}_n \leftarrow \frac{\hat{t}_n \times c + \hat{t}_n^c}{c+1}$;
    $c \leftarrow c + 1$;
  end for
  return the mean value of $\hat{t}_n$;
end function

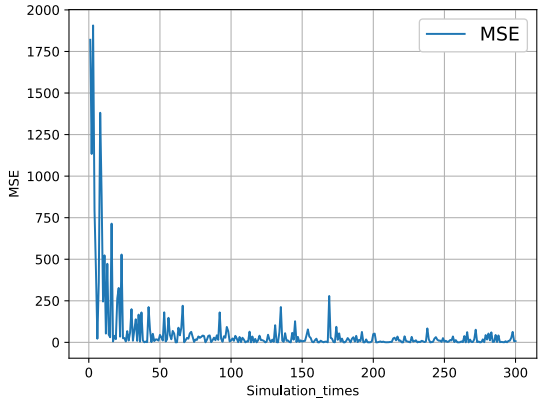


FIGURE 4. The simulation result of the MSE.

algorithm 1, the simulation data $\hat{t}_{10}$ is approached to the theoretical value t_{10}. From Table 1 and Fig. 4, the value of MSE declines rapidly and approach to 0. In a word, the change of MSE indicates that the simulation data $\hat{t}_{10}$ is approaching to the theoretical value t_{10}. The simulation result also shows the SPP protocol is a security protocol when $d = 0.5$ and $c = 0.5$, and our security analysis is right.

V. CONCLUSION

The security of SPP has been proved in this paper, the larger probability that Eve takes an eavesdropping operation, the less successful probability that Eve gets the information without being detected. The more qubits used in detecting eavesdropping, the larger probability to detect the eavesdropping. A comparison about the information Eve gets in OPP and SPP is also given, with the same probability d that Eve takes eavesdropping operation, the amount of information that Eve gets in SPP is less than Eve's gain in OPP.

The simulation which simulates the times of attempts that Eve tries to get n classical bits information without being detected is also given, and the mean square error(MSE) is introduce to describe the similarity between the simulation data and the theoretical value. With the given d,c and n, the simulation data $\hat{t}_n$ is approaching to the theoretical value t_n, and the value of MSE is approaching to 0. The result of simulation data and the value of MSE indicate that the SPP protocol is security and the security analysis is correct.

SPP uses the Omega state in control sequence to generate check sequence which is used to detect eavesdropping, and it uses Bell states in message sequence to generate message-code sequence which is used to transmit the secret message just like OPP. The Omega state can be prepared from Bell states, so the idea of detecting eavesdropping in SPP is very suitable for the OPP.

SPP doesn't need to introduce extra device into OPP, and SPP doesn't change the message-code sequence, so SPP can still get a good efficiency in transmitting message. In another word, SPP's message sequence is the same as OPP, making its easy to applicate.

However, compare with OPP, SPP needs to send more $2cN/(1-c)$ qubits to detect the eavesdropping. Means SPP gets more secure via sending more qubits than OPP.

In summary, a deterministic quantum secure direct communication protocol based on Omega state $|\Omega\rangle$ has been presented. The Omega state is used in control sequence to detecting the eavesdropping, and the Bell states are used in message sequence to transmit the secret message just like the original present protocol based on EPR pairs and Bell state [23]. Eve will face a larger probability of being detected when she wants to get the same amount of information in SPP than OPP. In another word, with the same probability of being detected, Eve can only gets at most 0.676 information in SPP rather than 1 information in OPP. In our security analysis, Eve can get part of information randomly without being detected, but she doesn't know which part of information she gets, so what Eve gets is useless. However, SPP needs to send more $2cN/(1-c)$ qubits than OPP, means that SPP gets more secure via sending more qubits used in detecting eavesdropping.

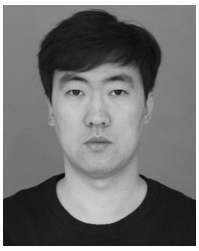
REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[2] G. S. Vernam, "Cipher printing telegraph systems," *J. AIEE*, vol. 45, no. 6, p. 572, Jun. 1926.
[3] T. T. Cormen, C. E. Leiserson, and R. L. Rivest, "Introduction to algorithms," *Resonance*, vol. 1, no. 9, pp. 14–24, 2003.
[4] R. Howard, "Data encryption standard," *Comput. Secur.*, vol. 6, no. 3, pp. 195–196, 1977.
[5] U.S. Department of Commerce, "Advanced encryption standard," in *Proc. Nat. Comput. Conf.*, 1997, pp. 83–87.
[6] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, Nov. 1994, pp. 124–134.
[7] A. El Allati, M. El Baz, and Y. Hassouni, "Quantum key distribution via tripartite coherent states," *Quantum Inf. Process.*, vol. 10, no. 5, pp. 589–602, 2011.
[8] X.-Y. Zhou, C.-H. Zhang, C.-M. Zhang, and Q. Wang, "Obtaining better performance in the measurement-device-independent quantum key distribution with heralded single-photon sources," *Phys. Rev. A, Gen. Phys.*, vol. 96, no. 5, p. 052337, 2017.
[9] H. K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *Science*, vol. 283, no. 5410, pp. 2050–2056, 1999.
[10] R. Valivarthi *et al.*, "Quantum teleportation across a metropolitan fibre network," *Nature Photon.*, vol. 10, pp. 676–680, Sep. 2016.
[11] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, "Experimental quantum teleportation," *Nature*, vol. 390, pp. 575–579, Dec. 1997.
[12] Y. Jiang, S. Zhang, F. Yang, Y. Chang, and H. Zhang, "Quantum secret sharing protocol and its modeling checking," *Laser Optoelectron. Progr.*, vol. 54, no. 12, p. 122704, 2017.
[13] Y.-G. Yang, Y.-W. Teng, H.-P. Chai, and Q.-Y. Wen, "Revisiting the security of secure direct communication based on ping-pong protocol[Quantum Inf. Process. 8, 347 (2009)]," *Quantum Inf. Process.*, vol. 10, no. 3, pp. 317–323, 2011.
[14] T. Hwang, Y. P. Luo, C. W. Yang, and T. H. Lin, "Quantum authencryption: One-step authenticated quantum secure direct communications for off-line communicants," *Quantum Inf. Process.*, vol. 13, no. 4, pp. 925–933, 2014.
[15] C.-W. Yang and T. Hwang, "Improved QSDC protocol over a collective-dephasing noise channel," *Int. J. Theor. Phys.*, vol. 51, no. 12, pp. 3941–3950, 2012.
[16] C. H. Bennett and G. Brassard, "An update on quantum cryptography," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 196. 1984, pp. 475–480.
[17] P. Sibson *et al.*, "Chip-based quantum key distribution," *Nature Commun.*, vol. 8, p. 13984, Feb. 2017.

[18] H.-L. Yin *et al.*, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Phys. Rev. Lett.*, vol. 117, no. 19, p. 190501, 2016.
[19] S. K. Liao *et al.*, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, 2017.
[20] J. Li, N. Li, L.-L. Li, and T. Wang, "One step quantum key distribution based on EPR entanglement," *Sci. Rep.*, vol. 6, p. 28767, Jun. 2016.
[21] J. Li, Y.-G. Yang, X.-B. Chen, Y.-H. Zhou, and W.-M. Shi, "Practical quantum private database queries based on passive round-robin differential phase-shift quantum key distribution," *Sci. Rep.*, vol. 6, p. 31738, Aug. 2016.
[22] G. L. Long and X. S. Liu, "Theoretically efficient high-capacity quantum-key-distribution scheme," *Phys. Rev. A, Gen. Phys.*, vol. 65, no. 3, p. 032302, 2002.
[23] F.-G. Deng, G. L. Long, and X.-S. Liu, "Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block," *Phys. Rev. A, Gen. Phys.*, vol. 68, no. 4, pp. 113–114, 2003.
[24] K. Boström and T. Felbinger, "Deterministic secure direct communication using entanglement," *Phys. Rev. Lett.*, vol. 89, p. 187902, Oct. 2002.
[25] Y. F. Yang and Y. E. Zhi-Qing, "Scheme of quantum dialogue based on four-particle omega state and security of intercept-resend attack," (in Chinese), *Acta Photon. Sinica*, vol. 42, no. 10, pp. 1256–1260, 2013.
[26] B. Pradhan, P. Agrawal, and A. K. Pati. (May 2007). "Teleportation and superdense coding with Genuine quadripartite entangled states." [Online]. Available: https://arxiv.org/abs/0705.1917
[27] D. Bru, M. Lewenstein, A. Sen, U. Sen, G. M. D'Ariano, and C. Macchiavello, "Dense coding with multipartite quantum states," *Int. J. Quantum Inf.*, vol. 4, no. 3, pp. 415–428, 2006.
[28] F. Gao, F. Guo, Q. Wen, and F. Zhu, "Efficiency comparison of different detection strategies in ping-pong protocol," (in Chinese)," *Sci. China Press*, vol. 2, no. 39, pp. 161–166, 2009.
[29] G. Boger, "Spreadsheet simulation of the law of large numbers," *Math. Comput. Edu.*, vol. 39, no. 3, pp. 175–182, 2005.
[30] P. Revesz, "The laws of large numbers," *Technometrics*, vol. 11, no. 3, p. 625, 1968.
[31] K. Ohno, K. Esfarjani, and Y. Kawazoe, *Monte Carlo Methods*. Berlin, Germany: Springer, 1999, pp. 195–270.
[32] L. E. C. Robalino, G. F. G. Fernández, E. Gallego, K. A. Guzmán-García, and H. R. Vega-Carrillo, "Study by Monte Carlo methods of an explosives detection system made up with a D-D neutron generator and NaI(Tl) gamma detectors," *Appl. Radiat. Isot.*, vol.141, pp. 167–175, Nov. 2018.
[33] T. Goda, D. Murakami, K. Tanaka, and K. Sato, "Decision-theoretic sensitivity analysis for reservoir development under uncertainty using multilevel quasi-Monte Carlo methods," *Comput. Geosci.*, vol. 22, no. 4, pp. 1009–1020, 2018.
[34] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.

LEILEI LI received the B.E. degree from the Beijing University of Posts and Telecommunications, Beijing, China, in 2015, where he is currently pursuing the Ph.D. degree. His research interests include quantum information security, cryptography, and machine learning.

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.



CHAOYANG LI received the M.S. degree from the Zhengzhou University of Light Industry, Zhengzhou, 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.

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.

YUAN TIAN received the M.S. degree from Shaanxi Normal University, Xi'an, Shanxi, China, in 2018. He is currently pursuing the Ph.D. degree with the Beijing University of Posts and Telecommunications. His research interests include information security, privacy preserving, and blockchain.

YAN ZHENG received the Ph.D. degree from Jilin University, in 2003. She is currently an Associate Professor with the School of Computer, Beijing University of Posts and Telecommunications, Beijing, China. Her research interests include quantum information and data mining.

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.