A Mobile Quantum Payment Protocol Based on the Entanglement Coherence of Four-particle GHZ State

Xiaojun Wen[1], Yongzhi Chen[2], Wei Zhang[2], Zoe L. Jiang[3], Junbin Fang[4]

[1] School of Computer Engineering, Shenzhen Polytechnic, China
[2] School of Mechanical and Electrical Engineering, Shijiazhuang University, China
[3] School of Computer Science and Technology, Harbin Institute of Technology, Shenzhen, China
[4] Department of Optoelectronic Engineering, Jinan University, China
wxjun@szpt.edu.cn, yz.chen226@foxmail.com, zhang9wei@126.com, zoeljiang@hit.edu.cn, junbinfang@gmail.com

Abstract

This paper proposes a mobile quantum payment agreement based on the entanglement coherence of four-particle GHZ (Greenberger-Horne-Zeilinger) state. Taking the four-particle GHZ state as the quantum channel, achieving the overall process of mobile payment through the physical properties of quantum mechanics and adopting the quantum key distribution, this protocol overcomes the limitation of computational security that generally exists in the traditional mobile payment system, and possesses the unconditional security in cryptography.

Keywords: Quantum mobile payment, Four-particle GHZ State, Quantum blind signature

1 Introduction

Payment, as an important link in the modern financial system, plays a crucial role in the financial system. With the development of information technology, the payment method is no longer confined to traditional forms, such as cash payment and bank card payment, etc., in the era of e-commerce and big data. In recent years when the e-commerce develops rapidly, it’s a very important issue to choose a proper payment method. Since 1982 when Chaum proposed the concept of e-cash [1], many scientific researchers have begun to devote themselves to the study of e-cash system and proposed a lot of e-cash payment schemes [2-5]. Because compared with other payment methods, the e-payment is an ideal payment method.

Nowadays, the mobile payment has sprung up everywhere and become an important e-payment method that is most widely used by people. The mobile payment aims to pay off debts and discharge the debtor-creditor relationship by transferring the monetary value through mobile communication equipment and wireless communication technology. The mobile payment is mainly represented by the payment with mobile phone. The general operation mode is that users connect to the network through mobile terminals, such as mobile phone and computer, etc., or accomplish the information exchange through close information technology so as to transfer the cash from the paying party to the receiving party and achieve the goal of payment. Compared with the perfect traditional payment forms, such as cash payment and bank card payment, etc., the mobile payment, characterized by mobility, instantaneity and rapidity, is more convenient and cost-effective. Customers are uncontrolled to accomplish the payment through mobile terminals and network anywhere at any time. In the current market, the mainstream mobile payment platforms include Apple Pay, Alipay, WeChat Pay and “Quick Pass” UnionPay, etc., and the mobile payment has become a brand-new e-payment method closely related to our daily life.

In fact, the background support of mobile payment is the modern information and technology revolution and the emerging information technology that combines a new generation of electronic technology and information security technology with the internet, mobile communication network, mobile terminal and big data. However, the mobile payment, with simple payment procedures and simplex means of payment auditing and identity authentication, is short of dynamic and complete risk management system, so there are an endless number of internet frauds and telecom frauds in recent years, which shows that security is the greatest problem to impede the development of mobile payment. It should be pointed out that the existing e-payment system, including mobile payment system, is achieved based on the blind signature and group signature in the classical digital signature. The schemes of classical group signature and blind signature are mostly designed based on the computational complexity problems in the mathematical field, including the problems of factorization, discrete logarithm and quadratic residue,

*Corresponding Author: Xiaojun Wen; E-mail: wxjun@szpt.edu.cn

DOI: 10.3966/160792642019102006016

etc. [6-9], but these schemes have not been proved to be unconditionally secure. Therefore, the e-payment system established based on the classical signatures cannot be proved to be unconditionally secure. With the unceasing enhancement of computing power and especially with the appearance of quantum computer, these algorithms or protocols will be unsafe any more, because they may be defeated by the quantum computer instantaneously. But the quantum signature can overcome the above-mentioned shortcomings of classical signatures. It's determined by the two basic characteristics of quantum key distribution, i.e. unconditional security and detectability of intercepting, so the e-payment system built based on the quantum signature is also of unconditional security. Therefore, people begin to turn their sights on the quantum cryptosystem based on the physical properties of quantum mechanics rather than on the computational complexity problems in the mathematical field and propose a series schemes of quantum group signature and quantum blind signature [10-19], based on which they establish some quantum payment systems [20] with unconditional security.

The first quantum cryptographic protocol with unconditional security in human history is the BB84 quantum key distribution (QKD) protocol proposed in 1984 [21], which has been proved to be unconditionally secure. Then, people successively put forward some quantum key distribution protocols based on quantum entangled states, which are widely used in practice and get more and more mature [22-23].

This paper distributes the key through quantum key distribution protocol, takes the four-particle GHZ state as the quantum channel, chooses the specific measurement direction to express sensitive messages and takes the quantum blind signature as the basis to build a mobile quantum payment system. Reference [20] mainly using quantum group blind signature to solve the traditional payment problem and improve security. Based on the rapid development of third-party mobile payment, this paper designs a quantum mobile payment protocol. Compared with reference [20], a new application scenario of quantum payment is introduced in this paper, and the group signature is removed, so this protocol is more concise under the premise of unchanged security. However, it should be noted that our protocol is established in absence of noise and of imperfections in detecting.

2 Basic Principles

2.1 Entanglement Coherence of Four-particle GHZ State

Set the four photons, A, B, C and D, at the GHZ state

$$|\psi\rangle_{\mathrm{ABCD}} = \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)_{\mathrm{ABCD}} \qquad \textbf{(1)}$$

Alice, Bob, Charlie and Diana possess photon A, B, C and D respectively. Define the eigen state of measurement basis $\mathrm{B_x}$ as

$$|+x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),\ |-x\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \qquad \textbf{(2)}$$

If Alice, Bob, Charlie and Diana adopt basis $\mathrm{B_x}$ to measure their own particle, the measurement results of A, B, C and D have quantum coherence. It can be known from equation (2) that

$$|0\rangle = \frac{1}{\sqrt{2}}(|+x\rangle + |-x\rangle),\ |1\rangle = \frac{1}{\sqrt{2}}(|+x\rangle - |-x\rangle) \qquad \textbf{(3)}$$

Substituting equation (3) into equation (1), the state of particle GHZ can be expressed as:

$$|\psi\rangle_{\mathrm{ABCD}} = \frac{1}{\sqrt{2}}[\prod_j (|+x\rangle_j + |-x\rangle_j) + \prod_j (|+x\rangle_j - |-x\rangle_j)] \qquad \textbf{(4)}$$

j belongs to the set {Alice, Bob, Charlie and Diana} and the right side of the equation is 8 superposition items for the state of the four particles along the *x* direction. Thereinto, 2 items are full--*x* state $|-x\rangle\ |-x\rangle\ |-x\rangle\ |-x\rangle$ and full-+*x* state $|+x\rangle\ |+x\rangle\ |+x\rangle\ |+x\rangle$ and the remaining 6 phases are the permutation and combination of any two of the four particles as -*x*:

$$(|-x\rangle\ |-x\rangle\ |+x\rangle\ |+x\rangle + |+x\rangle\ |-x\rangle\ |-x\rangle\ |+x\rangle + |-x\rangle\ |+x\rangle\ |-x\rangle\ |+x\rangle + |+x\rangle\ |-x\rangle\ |+x\rangle\ |-x\rangle + |-x\rangle\ |+x\rangle\ |+x\rangle\ |-x\rangle + |+x\rangle\ |+x\rangle\ |-x\rangle\ |-x\rangle)$$

The coherence of Alice, Bob, Charlie and Diana's measurement results is shown in Table 1. It can be known from Table 1 that:

Table 1. Entanglement Coherence of Four-particle GHZ State under Basis B_x

Alice	Bob	Charlie	Diana	Remarks
$\|-x\rangle$	$\|-x\rangle$	$\|-x\rangle$	$\|-x\rangle$	*I*
$\|+x\rangle$	$\|+x\rangle$	$\|+x\rangle$	$\|+x\rangle$	*I*
$\|-x\rangle$	$\|-x\rangle$	$\|+x\rangle$	$\|+x\rangle$	*Z*
$\|+x\rangle$	$\|-x\rangle$	$\|-x\rangle$	$\|+x\rangle$	*I*
$\|-x\rangle$	$\|+x\rangle$	$\|-x\rangle$	$\|+x\rangle$	*Z*
$\|+x\rangle$	$\|-x\rangle$	$\|+x\rangle$	$\|-x\rangle$	*Z*
$\|-x\rangle$	$\|+x\rangle$	$\|+x\rangle$	$\|-x\rangle$	*I*
$\|+x\rangle$	$\|+x\rangle$	$\|-x\rangle$	$\|-x\rangle$	*Z*

(1) An even number of -*x* states can be obtained by measuring each one-particle state through basis B_x.

This means if all the four people measure their own particle along the *x* direction, the measurement result of Alice can be determined by combining the results of Bob, Charlie and Diana. If the number of -*x* calculated simply by them is the even number, the measurement result of Alice is +*x*, and if it is odd, the result is -*x*. The result of A cannot be determined unless the other three people combine their messages.

(2) Meanwhile, it can be seen if the measurement results of Bob and Charlie are the same, the measurement results of Diana and Alice must be the same, as shown in the row with mark I in the remark column of Table 1. Conversely, if the measurement results of Bob and Charlie are converse, the measurement results of Diana and Alice must be converse, as shown in the row with mark Z in the remark column of Table 1.

This is the entanglement coherence rule of four-particle GHZ state.

1.2 Phase Transformation of the Quantum State Through Quantum Gate Z

Quantum gate *Z* is the *z* component $\hat{\sigma}_z$ of Pauli matrix, expressed as the matrix form:

$$Z = \hat{\sigma}_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \textbf{(5)}$$

The function of gate *Z* is to achieve the phase transformation of quantum bit, namely, changing the direction of basis $|1\rangle$. If the gate *Z* acts on the quantum state $|\psi\rangle = a|0\rangle + b|1\rangle$, the result will be $Z|\psi\rangle = a|0\rangle$ - $b|1\rangle$, namely, rotating π/2 around basis $|1\rangle$ in the clockwise direction. If the gate *Z* acts on the quantum state $|+x\rangle$ or $|-x\rangle$, the result will be:

$$Z|+x\rangle = Z\left[1/\sqrt{2}(|0\rangle + |1\rangle)\right] = |-x\rangle \quad \textbf{(6)}$$

$$Z|-x\rangle = Z\left[1/\sqrt{2}(|0\rangle - |1\rangle)\right] = |+x\rangle \quad \textbf{(7)}$$

3 Protocol Description

The scenario setting and protocol description are as follows:

It is assumed that customer Alice wants to buy something from merchant Diana by means of e-payment through the mobile terminal Charlie and their deposit banks are Bob. Alice sends a shopping message *M* (including the payment amount message M_1 and the detailed goods message M_2, of which message M_2 should be blind due to privacy protection) to merchant Diana and asks bank Bob to pay at the same time. Bank Bob and mobile terminal Charlie will sign the shopping message after receiving the request for authorization. Thereinto, they carry on the blind signature to M_2, meanwhile deduct the amount M_1 from Alice's account, then deposit M_1 into the merchant's account. At last, Diana delivers the goods to Alice after confirming that the signature of mobile terminal Charlie is effective. In this way, the transaction is finished.

The quantum payment protocol model is as shown in Figure 1.

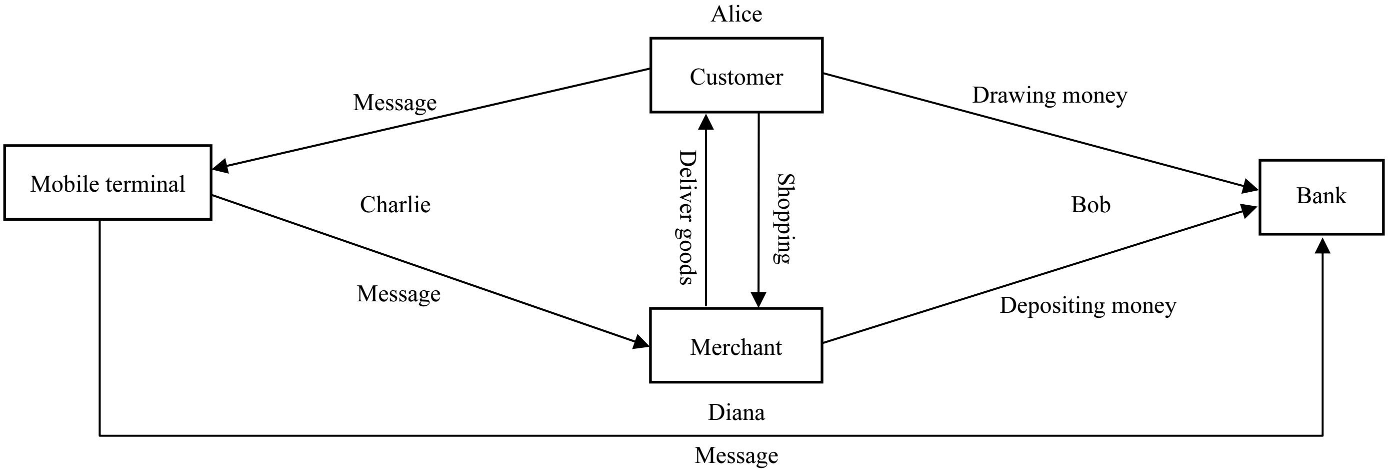

Figure 1. Quantum payment protocol model based on the entanglement coherence of four-particle GHZ State

3.1 System Initialization

3.1.1 Step 1: quantum key distribution

The shared keys of all trading parties are shown as follows:

K_{AB}, K'_{AB}: the shared key of Alice and bank Bob;

K_{AC}, K'_{AC}: the shared key of Alice and mobile terminal Charlie;

K_{AD}: the shared key of Alice and merchant Diana;

K_{BD}: the shared key of bank Bob and merchant Diana;

K_{CD}: the shared key of merchant Diana and mobile terminal Charlie.

The distribution of these keys can be accomplished through the famous BB84 protocol or B92 protocol [18-19], or other mature protocols in practical application [20-21].

3.1.2 Step 2: establishment of the quantum channel of GHZ state

Bank Bob prepares n sets of four-particle entanglement of the GHZ state as shown in equation (1). Bob keeps particle B from each set of entangled particles for itself, sends particle A to its customer Alice, sends particle C to mobile terminal Charlie and sends particle D to merchant Diana. The particles distribution of a set of four-particle GHZ is as shown in Figure 2.

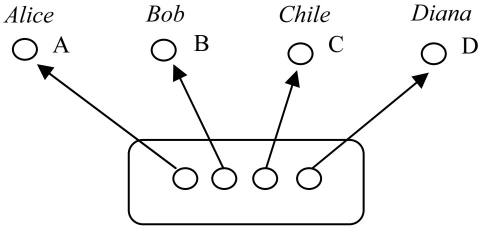

Figure 2. The particles distribution of a set of four-particle GHZ

3.1.3 Step 3: Alice carries out the message segmentation and transformation and tells all the parties to begin the transaction

Alice divides the shopping message M (the classical binary sequence) into two parts: M_1 and M_2. M_1 includes the payment amount and the information about the deposit bank Bob of merchant Diana and M_2 is the detailed billing information about the goods purchased by customer Alice, of which M_2 should be blind due to privacy protection. Alice informs bank Bob to withdraw the amount, and transfer the amount M_1 drawn by bank Bob from its own account into the account of Diana in bank Bob. Alice tells Diana to start the transaction through the public channel.

3.2 Alice Makes Message M2 Blind

Set M_2, the detailed billing information about the goods purchased by customer Alice, as $M_2=\{m(i),i=0,1,2,\cdots,n\}$, which is a binary classical bit string. Alice can obtain the blind message M_2' by encrypting M_2 through K_{AD}, the shared key of Alice and merchant Diana,

$$M_2'=E_{K_{\text{AD}}}(M_2)=\{m'(i),i=1,2,\cdots,n\} \quad \textbf{(8)}$$

3.3 Alice Notices Bank Bob and Mobile Terminal Charlie and Initiates the Shopping

Alice initiates the shopping and encrypts the payment amount message M_1 and the blind message M_2' through the shared key K_{AB}, K'_{AB} and the shared key K_{AC}, K'_{AC} respectively, and then sends the messages to bank Bob and mobile terminal Charlie.

3.4 Alice Authorizes Bob and Charlie

Step 1. Alice, based on the sensitive message M_2= $\{m(i),i=0,1,2,\cdots,n\}$, measures the particle A sequence possessed by her through basis B_x and selects the specific measurement direction of $+x$ direction or $-x$ direction according to the rules shown in the equation below:

$$\begin{cases} m(i)=0, & +x \\ m(i)=1, & -x \end{cases} \quad \textbf{(9)}$$

The selection of specific measurement direction refers to quantum random collapse. In the case of measurement under basis B_x, the measurement result will collapse into state $|+x\rangle$ (or state $|-x\rangle$) at the probability of 50%, which is called by us that the specific measurement direction that has been selected is $+x$ direction (or $-x$ direction). In this way, we select the particle that has collapsed into state $|+x\rangle$ in the particle A sequence when $m(i)$=0 , and select the particle that has collapsed into state $|-x\rangle$ in the particle A sequence when $m(i)$=1. For example, if i=1, $m(1)$=0, Alice selected the a set of four-particle GHZ whose particle A's quantum state is $|+x\rangle$ as the first set four-particle GHZ.

We record the sequence number of these selected particles in the particle A sequence and notice the other three parties that have participated in the protocol through the classical communication mode. We discard the unselected particles and the four-particle GHZ entanglement, in which the unselected particles exist. The speed of message transfer will not surpass the speed of light, because we choose the classical communication mode to notice the other three parties.

Step 2. Alice authorizes Bob and Charlie to implement the blind signature of M_2

Alice notices Bob and Charlie and asks them to measure the particle B and C sequences under basis B_x respectively. After measurement, Charlie reports the measurement result to bank Bob. Alice authorizes Bob to compare the measurement results of particle B and C sequences, as recorded as 1 bit classical message $\text{m}_{\text{BC}}(i)$ according to the equation below

$$\left.\begin{matrix} |+x\rangle_B|+x\rangle_C \\ |-x\rangle_B|-x\rangle_C \end{matrix}\right\}\rightarrow m_{BC}(i)=0$$
$$\left.\begin{matrix} |+x\rangle_B|-x\rangle_C \\ |-x\rangle_B|+x\rangle_C \end{matrix}\right\}\rightarrow m_{BC}(i)=1 \quad \textbf{(10)}$$

Bob encrypts the comparison result $M_{BC}=\{m_{BC}(i)\}$ through K_{BD} and then sends it to Diana as the blind signature of Alice's shopping list M_2.

3.5 Merchant Diana Verifies the Signature

Step 1. Merchant Diana receives the blind signature $\mathrm{M_{BC}}$ that has been encrypted by bank Bob through K_{BD} and obtains $\{m_{BC}(i)\}$ by means of decryption.

Step 2. Diana carries out the single quantum gate operation to the sequence of particle D possessed by her according to the value of $m_{BC}(i)$ and the equation below

$$\begin{cases} m_{BC}(i)=0 & \rightarrow I\left|\varphi\right\rangle_D \\ m_{BC}(i)=1 & \rightarrow Z\left|\varphi\right\rangle_D \end{cases} \quad \textbf{(11)}$$

In this equation, $I=|0\rangle\langle 0|+|1\rangle\langle 1|$ is the identity operation and $\mathrm{Z}=|0\rangle\langle 0|-|1\rangle\langle 1|$ is the operation of quantum gate Z.

Step 3. Diana measures the particle D which has passed gate I or gate Z under basis B_x, with the measurement result expressed as $\mathrm{M_D}=\{\mathrm{m}_D(\mathrm{i})\}$, the classical message of binary system,

$$\begin{cases} \left|+x\right\rangle_D \rightarrow & \mathrm{m}_D(\mathrm{i})=0 \\ \left|-x\right\rangle_D \rightarrow & \mathrm{m}_D(\mathrm{i})=1 \end{cases} \quad \textbf{(12)}$$

Step 4. Merchant Diana receives the shopping message M=$\{M_1$; $M_2\}$ from Alice and obtains M_1 and M_2 after the decryption through the shared key K_{AD}, in which $M_2=\{m(\mathrm{i})\}$. Merchant Diana verifies whether $\mathrm{M_D}=\{\mathrm{m}_D(\mathrm{i})\}$ and $M_2=m(\mathrm{i})$ conform to the verification rule below. If they do, merchant Diana will announce that the signature is effective, the detailed billing information M_2 is correct, and the goods can be delivered; otherwise, Diana will refuse the signature.

$$m_D(\mathrm{i})=m(\mathrm{i}) \text{ or } M_2=M_D \quad \textbf{(13)}$$

3.6 The Deduction of Customer Alice and the Deposit of Merchant Diana

Step 1. If Bob and Charlie receive the message that Diana accepts the signature and the delivery message from the Diana, they will deduct the corresponding amount from Alice's account according to M_1 and add (deposit) the corresponding amount into Diana's account.

Step 2. If customer Alice and merchant Diana can confirm that the amount that has been deducted and deposited is correct, the transaction is finished.

4 Analysis on Scheme Security

4.1 Blindness

The blind message M_2' is obtained by encrypting M_2, the detailed billing information about the goods purchased by customer Alice, through K_{AD}, the shared key of Alice and merchant Diana, so M_2' is blind for the signers, bank Bob and mobile terminal Charlie.

4.2 Correctness of the Scheme

If all the parties implement the operation according to the protocol procedures, the blind signature and signature verification will work out and the shopping and delivery can be carried out successfully. Because the entanglement coherence rule of four-particle GHZ state is as follows: if the measurement results of Bob and Charlie are the same, the measurement results of Diana and Alice must be the same; and conversely, if the measurement results of Bob and Charlie are converse, the measurement results of Diana and Alice must be converse. If all the parties implement the operation according to the protocol procedures honestly, the equation (4) must be correct and the signatures can be verified successfully.

4.3 Prevention of Fraudulence of the Scheme

It is assumed in this protocol that bank Bob is honest, so it can be known from the analysis that the other three parties cannot cheat or disavow unilaterally and the attacker cannot pretend successfully, including:

(1) Alice cannot cheat successfully or the attacker cannot pretend to be Alice successfully;

(2) Diana cannot disavow successfully;

(3) Charlie cannot forge the transaction of Alice or Diana successfully.

The reason is that the quantum state of the particle possessed by one party cannot be determined unless the other three parties combine their measurement results according to the entanglement coherence rule of four-particle GHZ state as shown in Table 1. Any party cannot obtain more information unilaterally even if the measurement basis is changed. It is proved as follows:

As for any party of Alice, Bob, Charlie and Diana, it is assumed that Diana adopts the measurement basis that doesn't conform to the regulations of protocol, with this basis expressed as:

$$\begin{aligned} |d_+\rangle &= a_+|0\rangle + b_+|1\rangle \\ |d_-\rangle &= a_-|0\rangle + b_-|1\rangle \end{aligned} \quad \textbf{(14)}$$

Any set of basis in the 2D Hilbert space generated by $|0\rangle$ and $|1\rangle$ can be expressed through the equation above. Setting $|d_+\rangle$ and $|d_-\rangle$ as a set of unit orthogonal bases, we can obtain that

$$\begin{cases} a_+a_- + b_+b_- = 0 \\ \left|a_+\right|^2 + \left|b_+\right|^2 = 1 \\ \left|a_-\right|^2 + \left|b_-\right|^2 = 1 \end{cases} . \qquad \textbf{(15)}$$

It can be known from equation (14) that

$$\begin{cases} \left|0\right\rangle = \dfrac{b_-}{a_+b_- - a_-b_+}\left|d_+\right\rangle - \dfrac{b_+}{a_+b_- - a_-b_+}\left|d_-\right\rangle \\ \left|1\right\rangle = \dfrac{a_-}{b_+a_- - b_-a_+}\left|d_+\right\rangle - \dfrac{a_+}{b_+a_- - b_-a_+}\left|d_-\right\rangle \end{cases} \qquad \textbf{(16)}$$

Setting

$$\begin{cases} A_0 = \dfrac{b_-}{a_+b_- - a_-b_+}, \quad B_0 = \dfrac{b_+}{a_+b_- - a_-b_+} \\ A_1 = \dfrac{a_-}{b_+a_- - b_-a_+}, \quad B_1 = \dfrac{a_+}{b_+a_- - b_-a_+} \end{cases} \qquad \textbf{(17)}$$

We can obtain that

$$\begin{cases} \left|0\right\rangle = A_0\left|d_+\right\rangle - B_0\left|d_-\right\rangle \\ \left|1\right\rangle = A_1\left|d_+\right\rangle - B_1\left|d_-\right\rangle \end{cases} \qquad (18)$$

It can be known from the equation above that

$$\begin{cases} \mathrm{A}_0\mathrm{A}_1 + B_0B_1 = 0 \\ \left|A_0\right|^2 + \left|B_0\right|^2 = 1 \\ \left|A_1\right|^2 + \left|B_1\right|^2 = 1 \end{cases} . \qquad \textbf{(19)}$$

Considering the conciseness of equation expression, the measurement basis B_X adopted by the protocol can be concisely expressed as: $|+\rangle = \left|+x\right\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \left|-x\right\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Substituting equation (3) and (18) into equation (1), it can be obtained that

$$\begin{aligned} |\psi\rangle_{\mathrm{ABCD}} &= \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)_{\mathrm{ABCD}} \\ &= \frac{A_0 + A_1}{16}(\left|+++\right\rangle + \left|+--\right\rangle + \\ &\quad \left|-+-\right\rangle + \left|--+\right\rangle)_{\mathrm{ABC}}\left|d_+\right\rangle_{\mathrm{D}} \\ &\quad + \frac{A_0 - A_1}{16}(\left|++-\right\rangle + \left|+-+\right\rangle \\ &\quad + \left|-++\right\rangle + \left|---\right\rangle)_{\mathrm{ABC}}\left|d_+\right\rangle_{\mathrm{D}} \\ &\quad - \frac{B_0 + B_1}{16}(\left|+++\right\rangle + \left|+--\right\rangle \\ &\quad + \left|-+-\right\rangle + \left|--+\right\rangle)_{\mathrm{ABC}}\left|d_-\right\rangle_{\mathrm{D}} \\ &\quad - \frac{B_0 - B_1}{16}(\left|++-\right\rangle + \left|+-+\right\rangle \\ &\quad + \left|-++\right\rangle + \left|---\right\rangle)_{\mathrm{ABC}}\left|d_-\right\rangle_{\mathrm{D}} \end{aligned} \qquad \textbf{(20)}$$

The four coefficients in the equation are: $\frac{A_0 + A_1}{16}$, $\frac{A_0 - A_1}{16}$, $-\frac{B_0 - B_1}{16}$, $-\frac{B_0 + B_1}{16}$.

Among which it's required that $\frac{A_0 + A_1}{16}$ and $\frac{A_0 - A_1}{16}$ cannot be zero at the same time, and $-\frac{B_0 - B_1}{16}$ and $-\frac{B_0 + B_1}{16}$ cannot be zero at the same time, either.

It should be pointed out that $\left\{\left|d_+\right\rangle, \left|d_-\right\rangle\right\}$ represents all the bases that may be selected by Diana. It can be shown from equation (20) that Diana has at least four potential combinations of the measurement results of A, B and C, namely, the phases in the four brackets of equation (20), with regard to any measurement result under any measurement bases. It can be seen from the four items in each bracket that the probability is 1/2 for any photon measurement result of A, B and C being $\left|+\right\rangle$ or $\left|-\right\rangle$, which shows that Diana cannot obtain more information by changing the measurement bases.

Therefore, any party cannot speculate the state of the particle possessed by others only depending on the measurement result of the particle possessed by himself/herself nor obtain more information by changing the measurement bases. Therefore, it is impossible to forge the signature or cheat, and the dishonest activities cannot be implemented successfully.

It is assumed in this protocol that Bob is honest, so it is impossible that the other three parties have the intention to cheat or implement other dishonest activities. Therefore, we take no account of this situation.

4.4 Unconditional Security of the Scheme

The scheme takes the four-particle GHZ state as the quantum channel, achieves the overall process of e-payment through the physical properties for the entanglement coherence of four-particle GHZ state and adopts the quantum key distribution (QKD) to make every party share the key, so it is unconditionally secure.

5 Conclusion

We choose the four-particle GHZ entangled state as the quantum channel, take the quantum blind signature as the basis and distribute the key through quantum key distribution protocol to build a mobile quantum payment system. The scheme has the characteristics of blindness, prevention of fraudulence and unconditional security. And it's unnecessary for the scheme to use the complex quantum fingerprint function and adopt the post audit, so it is more concise and reliable and more applicable to the mobile payment system that is under the booming development.

Acknowledgements

This work was partially supported by National Natural Science Foundation of China (No. 61771222), Science and technology projects of Guangdong Province (No. 2016A010101017, No. 2016A030313023), Science and Technology Project of Guangzhou (No. 201707010253), 2018 Shenzhen Discipline Layout Project (No. JCYJ20170815145900474), and Shenzhen Basic Research Project (No. JCYJ20170818115704188).

References

[1] D. Chaum, Blind Signatures for Untraceable Payments, in: D. Chaum, R. L. Rivest, A. T. Sherman (Ed.), *Advances in cryptology*, Springer, 1983, pp. 199-203.

[2] W. S. Juang, H. T. Liaw, A Practical Anonymous Multi-authority E-cash Scheme, *Applied Mathematics and Computation*, Vol. 147, No. 3, pp. 699-711, January, 2004.

[3] C. L. Chen, M. H. Liu, A Traceable E-cash Transfer System Against Blackmail Via Subliminal Channel, *Electronic Commerce Research and Applications*, Vol. 8, No. 6, pp. 327-333, November-December, 2009.

[4] J. S. Wang, F. Y. Yang, I. Paik, A Novel E-cash Payment Protocol Using Trapdoor Hash Function on Smart Mobile Devices, *International Journal of Computer Science and Network Security*, Vol. 11, No. 6, pp. 12-19, June, 2011.

[5] S. Srivastava, V. Saraswat, E-cash Payment Protocols, *International Journal on Computer Science and Engineering*, Vol. 4, No. 9, pp. 1603-1607, September, 2012.

[6] H. Chien, J. Jan, Y. Tseng, RSA-based Partially Blind Signature with Low Computation, *Eighth International Conference on Parallel and Distributed Systems (ICPADS 2001)*, Kyongju City, South Korea, 2001, pp. 385-389.

[7] S. Canard, J. Traoré, On Fair E-cash Systems Based on Group Signature Schemes, *Australasian Conference on Information Security and Privacy*, Wollongong, Australia, 2003, pp. 237-248.

[8] I. R. Jeong, D. H. Lee, J. I. Lim, Efficient Transferable Cash with Group Signatures, *International Conference on Information Security*, Malaga, Spain, 2001, pp. 462-474.

[9] G. Maitland, C. Boyd, Fair Electronic Cash Based on a Group Signature Scheme, *International Conference on Information and Communications Security*, Xian, China, 2001, pp. 461-465.

[10] G. Zeng, W. Ma, X. Wang, H. Zhu, Signature Scheme Based on Quantum Cryptography, *Acta Electronica Sinica*, Vol. 29, No. 8, pp. 1098-1100, August, 2001.

[11] G. Zeng, C. H. Keitel, Arbitrated Quantum-signature Scheme, *Physics Review A*, Vol. 65, No. 4, pp. 042312, April, 2002.

[12] D. Gottesman, I. Chuang, Quantum Digital Signatures, *arXiv preprint* quant-ph/0105032, May, 2001.

[13] H. Lee, C. Hong, H. Kim, J. Lim, H. J. Yang, Arbitrated Quantum Signature Scheme with Message Recovery, *Physics Letters A*, Vol. 321, No. 5-6, pp. 295-300, February, 2004.

[14] X. Lü, D. G. Feng, An Arbitrated Quantum Message Signature Scheme, *International Conference on Computational and Information Science*, Shanghai, China, 2004, pp. 1054-1060.

[15] X. Wen, Y. Liu, Y. Sun, Quantum Multi-signature Protocol Based on Teleportation, *Zeitschrift für Naturforschung A,* Vol. 62, No. 3-4, pp. 147-151, April, 2007.

[16] X. Wen, Y. Liu, A Realizable Quantum Sequential Multi-signature Scheme, *Dianzi Xuebao (Acta Electronica Sinica)*, Vol. 35, No. 6, pp. 1079-1083, June, 2007.

[17] X. Wen, Y. Liu, P. Zhang, Digital Multi-signature Based on the Controlled Quantum Teleportation, *Wuhan University Journal of Natural Sciences*, Vol. 12, No. 1, pp. 29-32, January, 2007.

[18] X. Wen, Y. Liu, Secure Authentic Digital Signature Scheme Using Quantum Fingerprinting, *Chinese Journal of Electronics*, Vol. 17, No. 2, pp. 340-344, April, 2008.

[19] X. Wen, X. Niu, L. Ji, Y. Tian, A Weak Blind Signature Scheme Based on Quantum Cryptography, *Optics Communications*, Vol. 282, No. 4, pp. 666-669, February, 2009.

[20] X. Wen, An E-payment System Based on Quantum Group Signature, *Physica Scripta*, Vol. 82, No. 6, 065403, December, 2010.

[21] C. H. Bennett, G. Brassard, Quantum Cryptography: Public Key Distribution and Coin Tossing, *Proc. of IEEE International Conference on Computers*, *Systems and Signal Processing*, Bangalore, India, 1984, pp. 175-179.

[22] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, *Physical Review Letters*, Vol. 67, No. 6, pp. 661-663, August, 1991.

[23] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Quantum Cryptography, *Reviews of Modern Physics*, Vol. 74, No. 1, pp. 145-195, January-March, 2002.

Biographies

Xiaojun Wen received the Ph.D. degree from Beijing Jiaotong University, China, in 2008. He is currently a Professor with the School of Computer Engineering, Shenzhen Polytechnic. His research focuses on quantum cryptography, security of computer network.

Yongzhi Chen received the Ph.M. degree from Hebei Normal University, China, in 2003. He is currently an associate Professor with the School of Mechanical and Electrical Engineering, Shijiazhuang University. His research focuses on quantum cryptography, security of computer network.

Wei Zhang received the Master of Engineering degree from Hebei University of Science and Technology, China, in 2010. He is currently a lecturer with the School of Mechanical and Electrical Engineering, Shijiazhuang University. His research focuses on security of computer network.

Zoe L. Jiang received the Ph.D. degree from The University of Hong Kong in 2010. She is currently an Associate Professor with the School of Computer Science and Technology, Harbin Institute of Technology, Shenzhen, Shenzhen 510855, China. Her research interests include quantum cryptography, digital forensics and applied cryptography.

Junbin Fang received the Ph.D. degree from South China Normal University, China, in 2008. He is currently a Professor with the Department of Optoelectronic Engineering, Jinan University. His research focuses on quantum cryptography, security of Inter of Things and digital forensics.