Implementation of an E-Payment Security Evaluation System Based on Quantum Blind Computing

Dong-Qi Cai, Xi Chen, Yu-Hong Han, Xin Yi, Jin-Ping Jia, Cong Cao & Ling Fan

International Journal of Theoretical Physics

ISSN 0020-7748
Volume 59
Number 9

Int J Theor Phys (2020) 59:2757-2772
DOI 10.1007/s10773-020-04536-8

International Journal of Theoretical Physics (2020) 59:2757–2772
https://doi.org/10.1007/s10773-020-04536-8

Implementation of an E-Payment Security Evaluation System Based on Quantum Blind Computing

Dong-Qi Cai[1] · Xi Chen[2] · Yu-Hong Han[1] · Xin Yi[3] · Jin-Ping Jia[4] · Cong Cao[5] · Ling Fan[5]

Received: 29 February 2020 / Accepted: 27 June 2020 / Published online: 10 July 2020

Abstract

E-payment has gradually become the mainstream globally in recent years. However, the security and anonymity of the traditional E-payment system are not perfectly guaranteed with the emergence of the quantum computer. In this paper, an E-payment security evaluation system based on quantum blind computing is proposed for evaluating the security of network transactions. Unitary operations and four-qubit cluster state are applied in this system to effectively defend against eavesdroppers. And a shared blind matrix used to encrypt the security scores prevents the curious third-party payment platform from obtaining the private data of users. Furthermore, our system guarantees that users cannot tamper with or disguise their security scores during transactions. We demonstrate the correctness and security of the system in detail and provide theoretical support for its extension to more types of evaluation systems.

Keywords Quantum blind compute · Cluster state · Blind matrix · Security evaluate

1 Introduction

Many electronic payment systems based on blind computing have been proposed since David Chaum [1]. And with the development of E-commerce, E-payment has become a

✉ Ling Fan
fanling@bupt.edu.cn

1 School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China

2 School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China

3 School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, China

4 CRRC Industry Investment CO., LTD, Beijing 100036, China

5 School of Electronic Engineering; State Key Laboratory of Information Photonics and Optical Communications; Beijing Key Laboratory of Space-ground Interconnection and Convergence, Beijing University of Posts and Telecommunications, Beijing 100876, China

mainstream payment method. However, the security of E-payment has not reached a perfect level. Various network attacks towards E-payment system occur from time to time, which causes great economic losses to the users and damages the creditworthiness and confidentiality of the third-party payment platforms [2–12]. To further strengthen the security of E-payment, many optimization schemes that can resist modern information attacks have been proposed [13–20]. Their schemes protect the security of transactions in three stages: establishing a transaction, conducting a transaction, and ending the transaction. This makes most of them have complex algorithms or extremely high costs. However, in recent years, security is no longer the only requirement for E-payment, efficiency and convenience have become increasingly important [21, 22]. So if an assessment scheme can be proposed to evaluate the security of each transactions before payment, it will undoubtedly greatly increase the security of transactions with minimal cost. In another way, it can be used to optimize the complex schemes to reduce their costs. This method has been used by many payment platforms. For example, Alipay, one of the most popular payment application in China, will compare the personal common payment environment with the current payment environment to evaluate the security of each transaction. It warns of unsafe transactions and even closes them. This paper will focus on such scoring scheme, and propose an E-payment security evaluation system to protect the privacy of users and the security of transaction.

Our evaluation system is essentially a kind of quantum secure communication. Quantum mechanics was first proposed for secure communication in [20]. The core of quantum secure communication is quantum entanglement. As long as the two subsystems are in an entangled state, no matter how far away the two systems are, they can not be regarded as mutually independent. This phenomenon is called quantum mechanical nonlocality [23, 24]. In addition to quantum secure communication, quantum mechanics has many important applications, such as deterministic entanglement [25–29], high-capacity quantum communication [30–32], and efficient quantum computation [33–35].

Apart from secure quantum channels supported by quantum entanglement, various quantum cryptography protocols also further ensure the security of quantum communication, such as QBC(Quantum Bit Commitment) and QKD(Quantum Key Distribution). In 1990, Brassard et al. first proposed a quantum bit commitment scheme based on BB84 protocol, and declared that the scheme is unconditionally secure [36]. In recent years, the QKD protocol which strengthens the BB84 protocol has gained popularity. QKD generates a shared random key for the communicating parties, which can be found once it is monitored [37–39]. These quantum cryptography protocols guarantee that quantum communication can resist the attack of QTM(Quantum Turing Machine) and PTM(Probabilistic Turing Machine), which makes it a more secure communication mode than the traditional [40, 41]. Furthermore, the richer implementation of quantum gates [42–46] has been widely studied in recent years, making these quantum cryptography protocols more feasible.

Due to the detectability of eavesdropping and the better security of quantum cryptography, we propose a new quantum evaluation system to further improve the security of modern E-payment systems(shown in the Fig. 1).

Score transmission is the core of our system. The fairness, binding, untraceability, and resistance of the scoring process are greatly guaranteed. That is to say:

1. Fairness. During the transaction, the payee and payer can not get the security score of the other. This ensures that even if one party is dishonest, the other party's private data will not be disclosed.

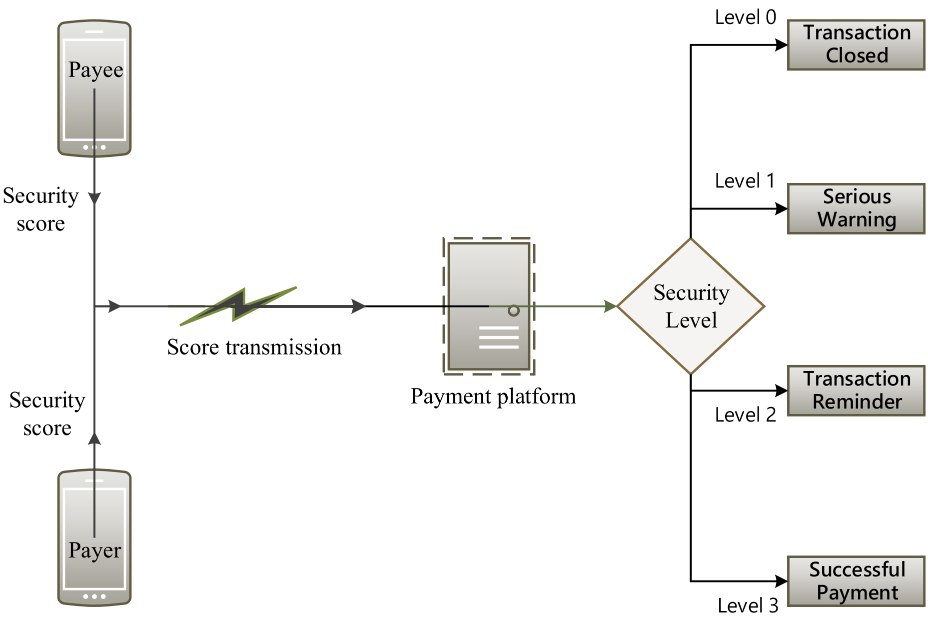

Fig. 1 E-payment security evaluation system. The payment terminal (mobile phone or computer, etc.) of the payer and payee will automatically determine the security score of the transaction according to the current payment environment. And the third-party trading platform will combine the security scores of the two to evaluate the security of the transaction and determine where the transaction will go

2. Binding. Once the security scoring process is over, the security score will be strictly tied to each party respectively. It is impossible for either party to deny it when questioned.
3. Untraceability. The third-party payment platform can only obtain the sum of the security scores of the two, so as to evaluate the security of the transaction. But it can never get the specific security score of each person. This allows people to confidently hand over their data to the platform without worrying about privacy leakage.
4. Resistance. If a third-party eavesdropper wants to steal data for sale, he will never make it and every attempt he made will be discovered.

In this paper, we first construct a minimalist model with only one transaction, and then extend it to the case of N transactions. According to the usual naming method, three participants are named as $Alice$, Bob, and $Trent$. The basic assumption about the three of them are as follows:

1. Alice is the payee in the transaction. Considering that a payee will have more transactions than a payer, we give her three security scores, namely 0(unsafe), 1(medium), 2(safe). Before the scoring starts, Alice can share part of the blind matrix with Bob. But after the scoring starts, in order to ensure privacy security, Alice can not communicate with Bob anymore.
2. Bob is the payer in the transaction. He has only two security scores, namely 0(unsafe), 1(safe). He can share the blind matrix before scoring, but cannot communicate with others after it.

3. Trent is the third-party trading platform, such as eBay, Amazon, Alipay, and so on. He is semi-trusted, which means that he can know the total security score of the other participants, but not the specific score of each person.

The scoring process of our system is shown in Fig. 2 : Firstly, the three generate a shared blind matrix by quantum cryptography protocol. The quantum cryptography protocol and its security have been discussed in many articles [37–41, 47, 48]. Secondly, Alice(Bob) starts security scoring and combines her(his) own real security score with the blind matrix to get an encrypted score. Then Alice and Bob send their encrypted scores on the quantum channel(four-qubit cluster state) by unitary operation. Finally, Trent calculates the total score of the two by analyzing the final cluster state, and evaluates the security level of the transaction to decide whether the transaction will be successful or closed.

In this work, we first introduce the basic knowledge needed by the scoring scheme in Section 2, including the introduction of the blind matrix and cluster state. After that, in Section 3, the algorithm flow of this scheme is introduced systematically. In Section 4, the security of the scheme is analyzed from three parts: internal attack, Trent attack, and external attack. Finally, we summarize the whole system and discuss its extended application in Section 5.

2 Basic Theory

2.1 Blind Matrix

The blind matrix is used to encrypt the score, which protects the scoring information of each party from leaking. Its form is:

$$\begin{bmatrix} a_{11} & .. & a_{1n} \\ .. & a_{ij} & .. \\ a_{n1} & .. & a_{nn} \end{bmatrix}_{n*n} \tag{1}$$

Where the result of each line modulo $(n+1)$ is 0, that is $\left(\sum_{j=1}^{n} a_{ij}\right) (\text{mod } n+1) = 0$. This special restriction brings an extraordinary and useful characteristic. Suppose we have n positive integers $b_j \in Z^+$, $j = 1, 2, ..., n$, and the sum of them is less than n, set as s. That is, $s = \left(\sum_{j=1}^{n} b_j\right) < n$. Now we set a encrypted number $\hat{b}_j = \left(b_j + \sum_{i=1}^{n} a_{ij}\right) (\text{mod } n+1)$. If we do not know the specific form of the blind matrix (1), we can hold that $\hat{b_j}$ and b_j can not be deduced from each other, which means b_j has been hidden when transmitting $\hat{b_j}$.

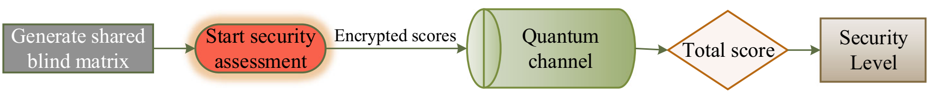

Fig. 2 Scoring algorithm flow chart

However, if we compute the sum $\hat{s} = \left(\sum_{j=1}^{n} \hat{b}_j\right) (\bmod\ n+1)$, we will find that $\hat{s}$ = s. That is because

$$\begin{aligned}
\hat{s} &= \left(\sum_{j=1}^{n} \hat{b}_j\right) (\bmod n+1) \\
&= \left[\sum_{j=1}^{n} \left(b_j + \sum_{i=1}^{n} a_{ij}\right) (\bmod n+1)\right] (\bmod n+1) \\
&= \left(\sum_{j=1}^{n} b_j\right) (\bmod n+1) + \left(\sum_{j=1}^{n} \sum_{i=1}^{n} a_{ij}\right) (\bmod n+1) \\
&= \left(\sum_{j=1}^{n} b_j\right) (\bmod n+1) + \left(\sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij}\right) (\bmod n+1)
\end{aligned} \tag{2}$$

As ruled before,

$$\left(\sum_{j=1}^{n} a_{ij}\right) (\bmod n+1) \equiv 0, s = \left(\sum_{j=1}^{n} b_i\right) < n. \tag{3}$$

Then we get

$$\hat{s} = (\sum_{j=1}^{n} b_j) = s \tag{4}$$

The sum of b_j is calculated without knowing each b_j. This means that we can transmit the encrypted number $\hat{b_j}$ instead of the original number b_j, but the receiver can still obtain the sum of the original number $s = \left(\sum_{j=1}^{n} b_j\right)$ accurately. And in the whole process, the receiver can not know the specific value of each b_j. This feature will be of great help to our following scheme construction [49].

2.2 Cluster State

The cluster state, as a common entangled state of n-particles, was first introduced by Bridgel and Raussendorf [50]. Its general state can be expressed as:

$$|\Psi_n\rangle = \frac{1}{2^{\frac{n}{2}}} \bigotimes_{a=1}^{n} (|0\rangle_a \sigma_z^{a+1} + |1\rangle_a) \qquad notes : \sigma_z^{n+1} \equiv 1 \tag{5}$$

When $n > 3$, the cluster state has some special properties of its own, such as better maximum relevance, durability, and discrimination. Due to its excellent particle properties, the cluster state is widely used in the design of quantum blind signature protocols and quantum secure direct communication protocols in recent years [24]. Its communication security has been strictly proved in many articles [24, 51–64]. Furthermore, the cluster state is physically achievable. The specific preparation method has been described clearly in [65–69]. In this paper, we choose the four-qubit cluster state as the initial state, that is, apply $n = 4$ to the expression (5) and get the initial standard form as follows:

$$|C\rangle_{1234} = \frac{1}{\sqrt{2}} (|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle)_{1234} \tag{6}$$

In quantum computing, especially in the computing model of quantum circuit, a quantum gate (or unitary operation) is a basic quantum circuit. Just like the common logic gate is generally operated on one or two bits, the common quantum gates are also operated on one or two qubits [70]. In this paper, we mainly use four kinds of quantum gates: I gate, X gate, Z gate, iY gate. They can be defined as follows:

$$\begin{aligned} I &= |0\rangle\langle 0| + |1\rangle\langle 1| \\ Z &= |0\rangle\langle 0| + |1\rangle\langle 1| \\ X &= |0\rangle\langle 1| - |1\rangle\langle 0| \\ iY &= |0\rangle\langle 1| - |1\rangle\langle 0| \end{aligned}$$

If those unitary operations are operated on the second and fourth particles of the cluster state respectively, we will get a new cluster state. For instance, do I or Z gate operation on the second particle of (6), and do I or Z gate operation on the fourth particle. After calculation, the new cluster state will appear, and only one of the following four situations will appear.

$$\begin{aligned} |C_1\rangle = I \bigotimes I|C\rangle_{1234} &= I \bigotimes I[\frac{1}{\sqrt{2}}(|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle)_{1234}] \\ &= \frac{1}{\sqrt{2}}(|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle)_{1234} \\ |C_2\rangle = I \bigotimes Z|C\rangle_{1234} &= I \bigotimes Z[\frac{1}{\sqrt{2}}(|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle)_{1234}] \\ &= \frac{1}{\sqrt{2}}(|0000\rangle - |0011\rangle + |1100\rangle + |1111\rangle)_{1234} \\ |C_3\rangle = Z \bigotimes I|C\rangle_{1234} &= Z \bigotimes I[\frac{1}{\sqrt{2}}(|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle)_{1234}] \\ &= \frac{1}{\sqrt{2}}(|0000\rangle + |0011\rangle - |1100\rangle + |1111\rangle)_{1234} \\ |C_4\rangle = Z \bigotimes Z|C\rangle_{1234} &= Z \bigotimes Z[\frac{1}{\sqrt{2}}(|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle)_{1234}] \\ &= \frac{1}{\sqrt{2}}(|0000\rangle - |0011\rangle - |1100\rangle - |1111\rangle)_{1234} \end{aligned}$$

Where the $|0\rangle$ and $|1\rangle$ is the result of Z-based measurement. Different operations will produce different and non-overlapping results. That is, unitary operation corresponds to the final result one by one. It is easy to prove as above, if we can do 4 different unitary operations on the particles of four-qubit cluster state, there will be 16 different codes(shown in Table 1).

3 The Algorithm Flow of the Scoring Scheme

As we stipulated in the introduction, the two scorers responsible for scoring are Alice and Bob, and Trent is only responsible for statistics of the total score, which means he does not score. Alice is the payee, she has a security score $s_1 \in \{0, 1, 2\}$. Bob is the payer, he has a security score $s_2 \in \{0, 1\}$. Our scoring scheme is divided into three parts: blind stage, implementation stage, calculation stage.

Table 1 Encoding rule

Unitary operation[a]	Finial states after operation[b]
$I \bigotimes I$	$\|C1\rangle = \|0000\rangle + \|0011\rangle + \|1100\rangle - \|1111\rangle$
$I \bigotimes Z$	$\|C2\rangle = \|0000\rangle - \|0011\rangle + \|1100\rangle + \|1111\rangle$
$Z \bigotimes I$	$\|C3\rangle = \|0000\rangle + \|0011\rangle - \|1100\rangle + \|1111\rangle$
$Z \bigotimes Z$	$\|C4\rangle = \|0000\rangle - \|0011\rangle - \|1100\rangle - \|1111\rangle$
$I \bigotimes X$	$\|C5\rangle = \|0001\rangle + \|0010\rangle + \|1100\rangle - \|1110\rangle$
$I \bigotimes iY$	$\|C6\rangle = \|0001\rangle - \|0010\rangle + \|1101\rangle + \|1110\rangle$
$Z \bigotimes X$	$\|C7\rangle = \|0001\rangle + \|0010\rangle - \|1101\rangle + \|1110\rangle$
$Z \bigotimes iY$	$\|C8\rangle = \|0001\rangle - \|0010\rangle - \|1101\rangle - \|1110\rangle$
$X \bigotimes I$	$\|C9\rangle = \|0100\rangle - \|0111\rangle + \|1000\rangle - \|1011\rangle$
$X \bigotimes Z$	$\|C10\rangle = \|0100\rangle - \|0111\rangle + \|1000\rangle + \|1011\rangle$
$iY \bigotimes I$	$\|C11\rangle = \|0100\rangle + \|0111\rangle - \|1000\rangle + \|1011\rangle$
$iY \bigotimes Z$	$\|C12\rangle = \|0100\rangle - \|0111\rangle - \|1000\rangle - \|1011\rangle$
$X \bigotimes X$	$\|C13\rangle = \|0101\rangle + \|0110\rangle + \|1001\rangle - \|1010\rangle$
$X \bigotimes iY$	$\|C14\rangle = \|0101\rangle - \|0110\rangle + \|1001\rangle - \|1010\rangle$
$iY \bigotimes X$	$\|C15\rangle = \|0101\rangle - \|0110\rangle - \|1001\rangle + \|1010\rangle$
$iY \bigotimes iY$	$\|C16\rangle = \|0101\rangle - \|0110\rangle - \|1001\rangle - \|1010\rangle$

[a]The table describes the relationship of the transformed state and the unitary operation on the qubits 2 and 4 of cluster state $|C\rangle_{1234}$

[b]The 16 final states are completely distinguishable by current physical technology

3.1 Blind Stage(shown in Fig. 3)

Trent pre-generates 3 random positive integers a_{31}, a_{32}, a_{33} as the third row of the $3 * 3$ matrix, of which the sum $\sum_j a_{ij}$ are congruent modulo 4. That is, $\sum_j a_{ij}(mod\ 4) \equiv 0$. Then Alice and Bob separately fill in the first and second row of the matrix according to the same rule. We get the matrix as follows:

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \tag{7}$$

For each $i, j \in \{1, 2, 3\}$, the filler of the i-th **row** V_i sends a_{ij} to V_j by quantum cryptography protocol discussed in many papers [37–41, 47]. Now for every $i \in \{1, 2, 3\}$, the filler V_i knows exactly the i-th column a_{1i}, a_{2i}, a_{3i}. Then he computes the sum of i-th **column** as the encrypted key $\hat{a}_i = \sum_{m=1}^{3} a_{mi}$.

3.2 Implementation Stage

After completing the blind matrix above, Alice and Bob start scoring. The score of Alice is $s_1 \in \{0, 1, 2\}$, and the score of Bob is $s_2 \in \{0, 1\}$. And they will score via doing unitary operation on a four-qubit cluster state.(Shown in Fig. 4)

Before starting the score transmission, Trent prepares a four-qubit cluster state in advance. Its initial form is:

$$|C_{1234}\rangle = (|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle)_{1234}$$

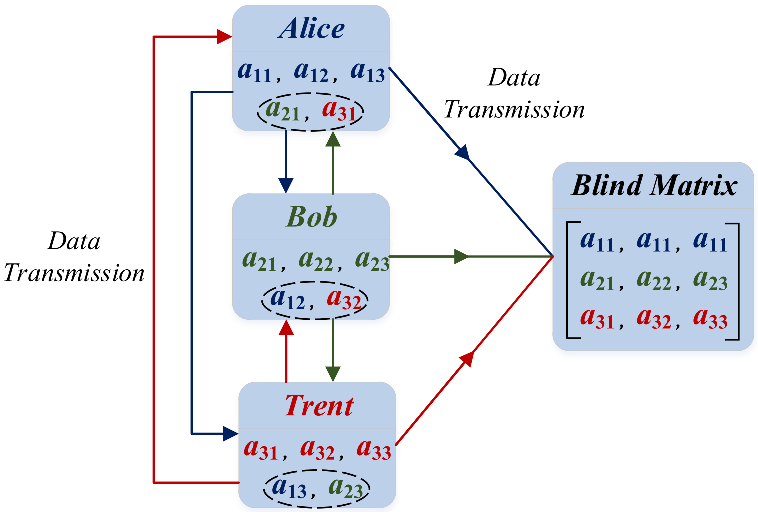

Fig. 3 Generation of the blind matrix. Everyone in the scheme will prepare three numbers and start data transmission. Numbers with the same color as the name are prepared by themselves, those with different color are from others

Then Trent transmits the second and fourth particles to Alice and Bob respectively. Now, both Alice and Bob have got a particle. They need to score by changing the state of the particle. The scoring method adopted in this paper is to operate the quantum gate(unitary operation) on each particle. Different scores correspond to different quantum gates uniquely, and their corresponding relations are defined in Table 2.

In order to encrypt each person's score, now Alice and Bob respectively add their original score s_i to the encrypted key $\hat{a}_i$ obtained in the step of blind matrix generation, modulo 4, finally get a encrypted score $\hat{s}_i = (s_i + \hat{a}_i) mod\ 4$.

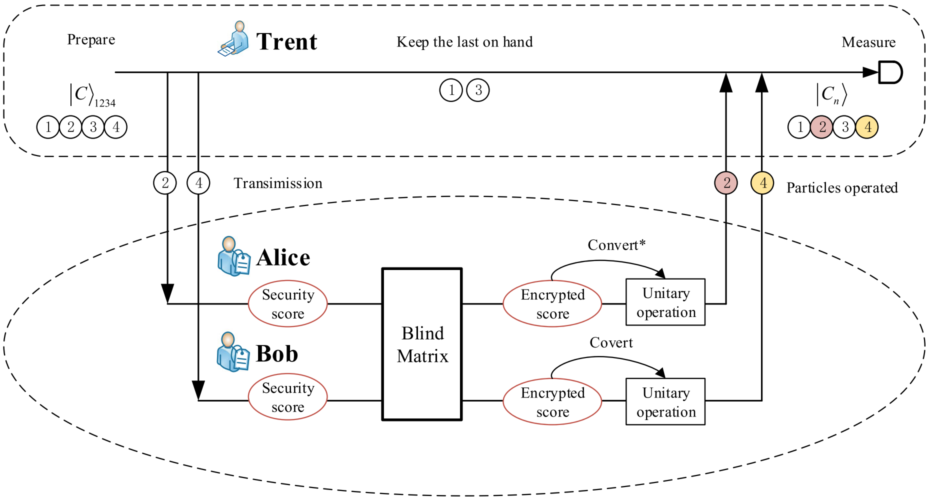

Fig. 4 Scoring via doing unitary operation on four-qubit cluster state

Table 2 Reference

Blind score	0	1	2	3
Unitary operators	I	X	Z	iY

Alice and Bob do quantum gate operation corresponding to $\hat{s_i}$ instead of s_i on their own particles, and pass the operated particles back to the Trent.

3.3 Calculation Stage

Trent receives the second and fourth particles operated. He measures the current state of the four-qubit cluster state. There are 16 different states (shown in Table 1) corresponding to different operations that Alice and Bob made. Combining Table 1 with the final four-qubit cluster state in his hand, Trent can deduce the quantum gate operations did by Alice and Bob, thus he can get the encrypted scores $\hat{s_i}(i \in 1, 2)$. Then he adds $\hat{s_1}$, $\hat{s_2}$ to the sum of the first column of the blind matrix, and modulo 4 to calculate the final number $\hat{s} = (\hat{s_1} + \hat{s_2} + \sum_{i=1}^{3} a_{i3}) mod\ 4$. According to the proof of formula (2)(3)(4), we can demonstrate that,

$$\begin{aligned}
\hat{s} &= (\hat{s_1} + \hat{s_2} + \sum_{i=1}^{3} a_{i3}) mod\ 4 \\
&= (s_1 + \sum_{i=1}^{3} a_{i1} + s_2 + \sum_{i=1}^{3} a_{i2} + \sum_{i=1}^{3} a_{i3}) mod\ 4 \\
&= s_1 + s_2 = s
\end{aligned}$$

Which is the accurate sum of the real security scores of Alice and Bob. That is the number Trent needs to know, so as to evaluate the security of transaction.

4 Security Analysis

In order to ensure the security of the transaction and the privacy of the users, our system must guarantee the fairness, binding, untraceability, and resistance of the scoring scheme. We will demonstrate it from three common attacks.

4.1 Internal Attack

In the process of scoring, the scorer should not be able to tamper the security score of another, and after scoring, he should be responsible for his own score, and cannot deny his own score. The following is an analysis from two aspects: tampering crisis and denying crisis.

4.1.1 Tampering Crisis

Suppose Alice intends to tamper the score of Bob during the scoring process, in the whole scoring process, Alice can only contact the second particle of the cluster state, but she is impossible to contact the fourth particle, so Alice can never know or tamper Bob's score. Assuming Bob intents to tamper, Alice's score can get the same level of security guarantee.

4.1.2 Denying Crisis

Assuming that Alice intends to deny her score after finishing the scoring process, in this case, Bob can make a query to Trent and inform Trent of the value of his own blind matrix. At this point, Trent already knows all the exact values of the second and third column and row of the blind matrix. Set the number unknown as x_1, we get the matrix:

$$\begin{bmatrix} x_1 & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \tag{8}$$

Combined with the definition (3), we take n = 3 and get that the sum of each row of the blind matrix is a multiple of 4. That is

$$\begin{aligned} x_1 + a_{12} + a_{13} &= 4k, k \in Z^+ \\ x_1 &= 4k - a_{12} - a_{13} \end{aligned} \tag{9}$$

We assume the real score of Alice is s_1, and the encrypted score is $\hat{s_1}$. That is $\hat{s_1} = (s_1 + x_1 + a_{21} + a_{31}) mod\ 4$. Apply the expression (9) to it, and add $(\sum_{i=1}^{n} a_{i2} + \sum_{i=1}^{n} a_{i3})$ on both sides of the equation, we get

$$\begin{aligned} \hat{s_1} &= [s_1 + (4k - a_{12} - a_{13}) + a_{21} + a_{31}] mod\ 4 \\ \sum_{i=1}^{n} a_{i2} + \sum_{i=1}^{n} a_{i3} + \hat{s_1} &= (s_1 - a_{12} - a_{13} + a_{21} + a_{31}) mod\ 4 + \sum_{i=1}^{n} a_{i2} + \sum_{i=1}^{n} a_{i3} \\ &= s_1 + \sum_{j=1}^{3} a_{2j} + \sum_{j=1}^{3} a_{3j} - 4t, t \in Z \end{aligned} \tag{10}$$

Since knowing that $(\sum_{j=1}^{3} a_{ij}) mod\ 4 = 0$, we can calculate the expression (10) to get $(\sum_{i=1}^{n} a_{i2} + \sum_{i=1}^{n} a_{i3} + \hat{s_1}) mod\ 4 = s_1$. Trent already knows $\sum_{i=1}^{n} a_{i2}$ and $\sum_{i=1}^{n} a_{i3}$ from (8). And he can deduce $\hat{s_1}$ from the final cluster state using Table 1 and Table 2. Undoubtedly, Trent can know what the security score s_1 of Alice is. If Bob wants to deny, Alice can do the same to guarantee her rights.

4.2 Trent Attack

In order to protect the rights and interests of the two parties to the transaction, Trent can only know the sum of the scores, but not the separate score of the two. We suppose that Trent wants to parse the second particles returned from Alice to get her real security score. Although Trent can deduce the encrypted score of Alice, set as $\hat{s_1}$. Due to the existence of the blind matrix, the quantum gate information attached to the second particle obtained by Trent is encrypted, not directly corresponding to the score, that is $\hat{s_1} \neq s_1$. And we know that $\hat{s_1} = (s_1 + \sum_{i=1}^{3} a_{i1}) mod\ 4$. Where a_{11}, a_{21}, a_{31} are the first column of the blind matrix (7). If he wants to reverse the evaluation, he must know all the number a_{11}, a_{21}, a_{31} exactly. However, a_{11}, a_{21} were filled by Alice and Bob separately and randomly. And they are not transmitted during the whole scoring process. So it is impossible for Trent to deduce the number a_{11}, a_{21} by himself.

To improve and perfect our theory, we need to prove that even if Trent uses information theory methods for cryptanalysis, it can be prevented as well [71]. That means Trent shall have no way to infer Alice's score s_1 by analyzing the probability distribution of $\hat{s_1}$, set as $P(\hat{s_1})$. Since Trent knows exactly a_{31}, what he needs to analyze is the probability distribution of $X = (a_{11} + a_{21} + s_1) mod\ 4$, set as $P(X)$. Because a_{11}, a_{21} are randomly filled in by Alice and Bob respectively, and the score of Alice is random. Therefore,

$$
\begin{aligned}
P(a_{11} = 0) = P(a_{11} = 1) &= P(a_{11} = 2) = P(a_{11} = 3) = \frac{1}{4} \\
P(a_{21} = 0) = P(a_{21} = 1) &= P(a_{21} = 2) = P(a_{21} = 3) = \frac{1}{4} \\
P(s_1 = 0) &= P(s_1 = 1) = P(s_1 = 2) = \frac{1}{3}
\end{aligned}
$$

As we know, a_{11}, a_{21}, s_1 is independent of each other, so we can calculate the probability distribution of X now.

$$
\begin{aligned}
P(X = 0|s_1 = 0) = P(X = 1|s_1 = 0) = P(X = 2|s_1 = 0) = P(X = 3|s_1 = 0) = \frac{1}{4} \\
P(X = 0|s_1 = 1) = P(X = 1|s_1 = 1) = P(X = 2|s_1 = 1) = P(X = 3|s_1 = 1) = \frac{1}{4} \\
P(X = 0|s_1 = 2) = P(X = 1|s_1 = 2) = P(X = 2|s_1 = 2) = P(X = 3|s_1 = 2) = \frac{1}{4}
\end{aligned}
$$

That is $P(X|s_1 = 0) = P(X|s_1 = 1) = P(X|s_1 = 2)$, which prevents Trent from inferring the real security score s_1 of Alice by analyzing the probability distribution of X. If Trent is curious of the score of Bob, he will get nothing meaningful as well. For example, we suppose that Alice's security score is $s_1 = 1$, and Bob's security score is $s_2 = 0$. And the form of the blind matrix is as follows.

$$
\begin{bmatrix} 0 & 3 & 1 \\ 2 & 2 & 0 \\ 1 & 2 & 1 \end{bmatrix}
$$

We calculate the encrypted scores $\hat{s_1} = (1 + 0 + 2 + 1) mod\ 4 = 0$, $\hat{s_2} = (0 + 3 + 2 + 2) mod\ 4 = 3$, which are related to the unitary operations made on the particles and can be deduced from Trent. Now we assume that Trent wants to get real security score of Alice and Bob using his known data. All the information that Trent knows without outer help are $\hat{s_1} = 0$, $\hat{s_2} = 3$ and a partially known matrix as follows:

$$
\begin{bmatrix} x_1 & x_2 & 1 \\ x_3 & x_4 & 0 \\ 1 & 2 & 1 \end{bmatrix}
$$

Where the numbers x_1, x_2, x_3, x_4 are unknown. Considering that the sum of each row modulo 4 is 0, there are 16 non-repeating possible scenarios. In one case, Trent assumes that $x_1 = 3, x_2 = 0, x_3 = 1, x_4 = 3$, and calculates that the real security score of Alice is $s_1 = (\hat{s_1} - x_1 - x_3 - 1) mod\ 4 = (0 - 3 - 1 - 1) mod\ 4 = 2$, the score of Bob is $s_2 = (\hat{s_2} - x_2 - x_4 - 2) mod\ 4 = (3 - 0 - 3 - 2) mod\ 4 = 2$. Do as the same, we get Table 3.

Considering the real score can not be 3, Trent aborts the results having $s_1 = 3$ or $s_2 = 3$. After that, Trent has a $\frac{1}{2}$ probability of getting the correct answer($s_1 = 1, s_2 = 0$), and has a $\frac{1}{2}$ probability of getting the wrong answer. This probability is not enough to help Trent get the real score of Alice and Bob, which means the real security scores are hidden successfully and Trent has no way to get them.

4.3 External Attack

If an eavesdropper wants to know or tampers with the score, then our system should be safe enough to resist it. Without loss of generality, we only discuss the case of the attack on Alice. And the case of the attack on Bob can be demonstrated in the same way.

In one case, the eavesdropper intercepted the second particle in the transmission process and wanted to tamper the score it carried. He attempts to extract the information in the second particle and forge a particle transmission with false information. Then, due to the characteristics of the cluster state, once the second particles were detected, and the untransmitted particles(first and third particles of the four-qubit cluster states) on Trent's hand would collapse, so that Trent could know that it was eavesdropped, thereby avoiding information leakage. In another case, the eavesdropper wants to parse Alice's score information directly from the second particle. Since the number a_{11} in the blind matrix(used to encrypt the score) was filled in by Alice randomly. And a_{11} is not transmitted during the process. It is impossible for the eavesdropper to know the encryption key on the particle, so he can not complete the analysis. In summary, in the process of particle transmission, security is greatly guaranteed, and it is impossible for eavesdroppers to destroy or crack this scoring process.

Table 3 All decryption possibilities[a]

x_1	x_2	x_3	x_4	s_1	s_2	x_1	x_2	x_3	x_4	s_1	s_2
1	2	1	3	1	0	3	0	1	3	3	2
1	2	2	2	0	1	3	0	2	2	2	3
1	2	3	1	3	2	3	0	3	1	1	0
1	2	4	0	2	3	3	0	4	0	0	1
2	1	1	3	0	1	0	3	1	3	2	3
2	1	2	2	3	2	0	3	2	2	1	0
2	1	3	1	2	3	0	3	3	1	0	1
2	1	4	0	1	0	0	3	4	0	3	2

[a]When $x_n > 3$, modulo 4 and apply the new $\tilde{x_n} = (x_n\ mod\ 4) \leq 3$ to find the result. Due to the special row rule that the sum of each row modulo 4 is 0, we can think that the result of querying with $\tilde{x_n}$ is the same as using x_n.($n \in \{1, 2, 3, 4\}$)

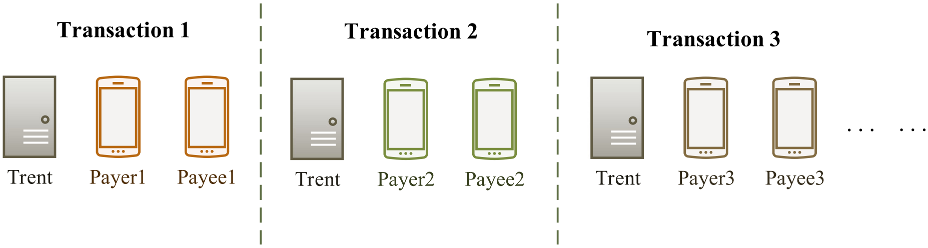

Fig. 5 Expanding to more transactions

5 Conclusion and Future Work

This paper proposes an E-payment security evaluation system based on quantum blind computing for evaluating security of network transactions. The complete evaluation algorithm flow of one transaction has been clearly described. Its correctness and security have been thoroughly analyzed in the paper. If we want to extend it to the N transactions, we only need Trent(the third-party trading platform) to prepare n four-qubit cluster states in advance and organize scoring in each transaction in the same process. Shown in Fig. 5, each transaction has the same Trent and two participants, which is the same as the simplest algorithm. After each group finishes scoring, Trent adds all the scores up, and to decide whether to continue trading or not. Our system can protect the privacy of each person in transaction to the greatest extent, and it can be realized physically by the current technology.

Furthermore, our evaluation system can be applied to more situations, such as teacher-student mutual assessment system, blind voting system, inequality scoring system and so on. As long as the assumptions given in this article are met, the security of the systems and the privacy of participants can be greatly guaranteed. However, there are still some imperfections in our system. For example, its best application is for transactions involving large amounts of money and those transactions that are not in a hurry. Because the entire security scoring process requires a complete quantum channel transmission, it cannot perfectly fit the daily short and flat trading rhythm.

In the future, we will focus on implementing the cluster state transmission [67, 72–74] to make our evaluation system come true. And on the basis of ensuring security, more efficient and convenient scoring methods will be explored [75–78]. Hyperentanglement has been widely studied in the past years. Photons possess several DOFs, such as polarization, spatial mode, time bin, frequency, and orbital angular momentum (OAM), and each DOF can be manipulated independently. In particular, photonic hyperentanglement [79], which involves photons simultaneously entangled in several DOFs, and can be completely analyzed by many schemes [80–82]. Hyperentanglement to achieve scoring system may be one of our future directions.

Acknowledgments This work was supported by the National Natural Science Foundation of China under Grant No. 61701035 and the Research Innovation Fund for College Students of Beijing University of Posts and Telecommunications.

References

1. Chaum, D.: Blind signatures for untraceable payments. In: Advances in cryptology, pp. 199–203. Springer (1983)
2. Kim, C., Tao, W., Shin, N., Kim, K.i.-S.: An empirical study of customers' perceptions of security and trust in e-payment systems. Electron. Commer. Res. Appl. **9**(1), 84–95 (2010)
3. Cai, X.Q., Wei, C.Y.: Cryptanalysis of an inter-bank e-payment protocol based on quantum proxy blind signature. Quantum Inf. Process **12**(4), 1651–1657 (2013)
4. Zhang, H.-Y.: Research on security and development of electronic payment. Modern Marketing (Information Edition)(01), 223 (2020)
5. Asokan, N., Janson, P.A., Steiner, M., Waidner, M.: The state of the art in electronic payment systems. Computer **30**(9), 28–35 (1997)
6. Wen, X., Chen, Y., Fang, J.: An inter-bank e-payment protocol based on quantum proxy blind signature. Quantum Inf. Process. **12**(1), 549–558 (2013)
7. Teoh, W.M.-Y., Chong, S.C., Lin, B., Chua, J.W.: Factors affecting consumers' perception of electronic payment: an empirical analysis. Int. Res. (2013)
8. Fernando, L., Rafii, A., Williams, N., Bunn, E.A., Valliani, A.: Modular signature and data-capture system and point of transaction payment and reward system. US Patent, (6,193,152) (2001)
9. Vakhitov, A., Makarov, V., Hjelme, D.R.: Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography. Journal of modern optics **48**(13), 2023–2038 (2001)
10. Makarov, V., Hjelme, D.R.: Faked states attack on quantum cryptosystems. J. Mod. Opt. **52**(5), 691–705 (2005)
11. Jain, N., Stiller, B., Khan, I., Elser, D., Marquardt, C., Leuchs, G.: Attacks on practical quantum key distribution systems (and how to prevent them). Contemp. Phys. **57**(3), 366–387 (2016)
12. Horoshko, D., Kilin, S.: Quantum anonymous voting with anonymity check. Phys. Lett. A **375**(8), 1172–1175 (2011)
13. Niu, X.-F., Zhang, J.-Z., Xie, S.-C., Chen, B.-Q.: A third-party e-payment protocol based on quantum multi-proxy blind signature. Int. J. Theor. Phys. **57**(8), 2563–2573 (2018)
14. Tiliwalidi, K., Zhang, J.-Z., Xie, S.-C.: A multi-bank e-payment protocol based on quantum proxy blind signature. Int. J. Theor. Phys. **58**(10), 3510–3520 (2019)
15. Bierbaum, C.J., Cope, W.B., Katzer, R.D., Paczkowski, L.W.: Electronic payment using a proxy account number stored in a secure element. US Patent, (8,566,168) (2013)
16. Rowney, K.T.B., Nadig, D.S.: System, method and article of manufacture for secure network electronic payment and credit collection. US Patent, (5,987,140) (1999)
17. Resnick, D., Callanan, M.J.: Electronic payment system utilizing intermediary account. US Patent, (6,185,545) (2001)
18. Cho, B.H., Ki, B.K., Cho, B.S.: Payment system, electronic device and payment method thereof. US Patent, (10,521,789) (2019)
19. Yin, W., Wen, Q., Li, W., Zhang, H., Jin, Z.: An anti-quantum transaction authentication approach in blockchain. IEEE Access **6**, 5393–5401 (2018)
20. Wiesner, S.: Conjugate coding. ACM Sigact News **15**(1), 78–88 (1983)
21. Cai, X.-Q., Wang, X.-X., Wang, T.-Y.: Fair and optimistic contract signing based on quantum cryptography. Int. J. Theor. Phys. (2019)
22. Wang, T.Y., Ma, J.F., Cai, X.Q.: The postprocessing of quantum digital signatures. Quantum Inf. Process **16**(1), 19 (2017)
23. Horodecki, R., Horodecki, P., Horodecki, M., Horodecki, K.: Quantum entanglement. Rev. Mod. Phys. **81**(2), 865 (2009)
24. Briegel, H.J., Raussendorf, R.: Persistent entanglement in arrays of interacting particles. Phys. Rev. Lett. **86**(5), 910 (2001)
25. Cao, C., Wang, C., He, L.Y., Zhang, R.: Atomic entanglement purification and concentration using coherent state input-output process in low-q cavity qed regime. Opt. Express **21**(4), 4093 (2013)
26. Sheng, Y.B., Deng, F.G.: One-step deterministic polarization-entanglement purification using spatial entanglement. Phys. Rev. A **82**(4), 44305–0 (2010)
27. Humphreys, P.C., Kalb, N., Morits, J.aco.P.J., Schouten, R.N., Vermeulen, R.F.L., Twitchen, D.J., Markham, M., Hanson, R.: Deterministic delivery of remote entanglement on a quantum network. Nature **558**(7709), 268–273 (2018)
28. Martin, L.S., Whaley, K.B.: Single-shot deterministic entanglement between non-interacting systems with linear optics. arXiv preprint arXiv:1912.00067 (2019)

29. Cao, C., Chen, X., Duan, Y.W., Fan, L., Zhang, R., Wang, T.J., Wang, C.: Concentrating partially entangled w-class states on nonlocal atoms using low-qoptical cavity and linear optical elements. Sci China Phys Mech Astron **59**(10), 100315 (2016)
30. Du, F.F., Li, T., Long, G.L.: Refined hyperentanglement purification of two-photon systems for high-capacity quantum communication with cavity-assisted interaction. Ann. Phys. **375**, 105–118 (2016)
31. Wang, G.-Y., Li, T., Ai, Q., Alsaedi, A., Hayat, T., Deng, F.G.: Faithful entanglement purification for high-capacity quantum communication with two-photon four-qubitsystems. Phys. Rev. Appl. **10**(5) (2018)
32. Yuan, H., Song, J., Zhou, J., Zhang, G., Wei, X.F.: High-capacity deterministic secure four-qubit w state protocol for quantum communication based on order rearrangement of particle pairs. Int. J. Theor. Phys. **50**(8), 2403–2409 (2011)
33. Jeong, H., Kim, M.S.: Efficient quantum computation using coherent states. Phys. Rev. A **65**(4), 042305 (2002)
34. Cao, C., Wang, C., Wang, T.J., Zhang, R.: Scalable quantum computation via a coherent state input-output process in a low-q cavity in the atom-cavity intermediate coupling region. Laser Phys. **23**(12), 125201 (2013)
35. Fried, E.S., Sawaya, N.P.D., Cao, Y., Kivlichan, I.D., Romero, J., Aspuru-Guzik, A.: qtorch: The quantum tensor contraction handler. PLos ONE (2018)
36. Brassard, G., Crépeau, C.: Quantum bit commitment and coin tossing protocols. In: Conference on the Theory and Application of Cryptography, pp. 49–61. Springer (1990)
37. Renner, R.: Security of quantum key distribution. Int. J. Quantum Inf. **6**(01), 1–127 (2008)
38. Shih, H.-C., Lee, K.-C., Hwang, T.: New efficient three-party quantum key distribution protocols. IEEE J. Sel. Top. Quantum Electron. **15**(6), 1602–1606 (2009)
39. Lo, H.-K., Curty, M., Qi, B.: Measurement-device-independent quantum key distribution. Phys. Rev. Lett. **108**(13), 130503 (2012)
40. Nishimura, H., Ozawa, M.: Computational complexity of uniform quantum circuit families and quantum turing machines communicated by o. watanabe. Theor. Comput. Sci. **276**(1-2), 147–181 (2002)
41. Dumais, P., Mayers, D., Salvail, L.: Perfectly concealing quantum bit commitment from any quantum one-way permutation. In: International Conference on the Theory and Applications of Cryptographic Techniques, pp. 300–315. Springer (2000)
42. Eisert, J., Jacobs, K., Papadopoulos, P., Plenio, M.B.: Optimal local implementation of non-local quantum gates. Physics **62**(5), 414–416 (2000)
43. Zhu, S., Wang, Z.D.: Erratum: Implementation of universal quantum gates based on nonadiabatic geometric phases. Phys. Rev. Lett. 89(9) (2002), 097902 (2002)
44. Cao, C., Duan, Y., Chen, X., Zhang, R., Wang, T., Wang, C.: Implementation of single-photon quantum routing and decoupling using a nitrogen-vacancy center and a whispering-gallery-mode resonator-waveguide system. Opt. Express **25**(15), 16931–16946 (2017)
45. Karol, B., Cernoch, A., Lemr, K.: Implementation of an efficient linear-optical quantum router. Sci. Rep. (2018)
46. Cao, C., Han, Y.H., Zhang, L., Fan, L., Zhang, R.: Highfidelity universal quantum controlled gates on electronspin qubits in quantum dots inside singlesided optical microcavities. Adv. Quantum Technol. **2**(10) (2019)
47. Mayers, D.: Unconditionally secure quantum bit commitment is impossible. Phys. Rev. Lett. **78**(17), 3414 (1997)
48. Wang, T.Y., Cai, X.Q., Ren, Y.L., Zhang, R.L.: Security of quantum digital signatures for classical messages. Sci. Rep. **5**, 9231 (2015)
49. Sun, X., Wang, Q., Kulicki, P., Sopek, M.: A simple voting protocol on quantum blockchain. Int. J. Theor. Phys. **58**(1), 275–281 (2019)
50. Raussendorf, R., Briegel, H.J.: A one-way quantum computer. Phys. Rev. Lett. **86**(22), 5188 (2001)
51. Zhang, Q., Li, C., Li, Y., Nie, Y.: Quantum secure direct communication based on four-qubit cluster states. Int. J. Theor. Phys. **52**(1), 22–27 (2013)
52. Cao, W., Yang, Y., Wen, Q.: Quantum secure direct communication with cluster states. Sci. China Phys. Mech. Astron. **53**(7), 1271–1275 (2010)
53. Sun, Z.-W., Du, R.-G., Long, D.ong.-Y.ang.: Quantum secure direct communication with two-photon four-qubit cluster states. Int. J. Theor. Phys. **51**(6), 1946–1952 (2012)
54. Zhang, J., Braunstein, S.L.: Continuous-variable gaussian analog of cluster states. Phys. Rev. A **73**(3), 032318 (2006)
55. Li, W., Shi, J., Shi, R., Guo, Y.: Blind quantum signature with controlled four-particle cluster states. Int. J. Theor. Phys. **56**(8), 2579–2587 (2017)

56. Zhao, N., Li, M., Chen, N., Zhu, C., Pei, C.: Quantum teleportation of eight-qubit state via six-qubit cluster state. Int. J. Theor. Phys. **57**(2), 516–522 (2018)
57. Tan, X., Zhang, X., Fang, J.: Perfect quantum teleportation by four-particle cluster state. Inf. Process. Lett. **116**(5), 347–350 (2016)
58. Kim, J., Lee, J., Ji, S.-W., Nha, H., Anisimov, P.M., Dowling, J.P.: Coherent-state optical qudit cluster state generation and teleportation via homodyne detection. Opt. Commun. **337**, 79–82 (2015)
59. Muralidharan, S., Jain, S., Panigrahi, P.K.: Splitting of quantum information using n-qubit linear cluster states. Opt. Commun. **284**(4), 1082–1085 (2011)
60. Ma, P.-C., Zhan, Y.-B.: Scheme for remotely preparing a four-particle entangled cluster-type state. Opt. Commun. **283**(12), 2640–2643 (2010)
61. Zhang, W., Liu, Y., Wang, Z., Zhang, Z.: Preparation of multi-atom cluster state and teleportation of arbitrary two-atom state via thermal cavity. Opt. Commun. **281**(17), 4549–4552 (2008)
62. Li, D.-C., Cao, Z.-L.: Teleportation of two-particle entangled state via cluster state. Commun. Theor. Phys. **47**(3), 464 (2007)
63. Wang, X.-W., Shan, Y.-G., Xia, L.-X., Lu, M.-W.: Dense coding and teleportation with one-dimensional cluster states. Phys. Lett. A **364**(1), 7–11 (2007)
64. Shen, D.-S., Ma, W.-P., Wang, L.-L.: Two-party quantum key agreement with four-qubit cluster states. Quantum Inf. Process. **13**(10), 2313–2324 (2014)
65. Zhan, Y.-B., Ma, P.C.: Deterministic joint remote preparation of arbitrary two-and three-qubit entangled states. Quantum Inf. Process. **12**(2), 997–1009 (2013)
66. Kiesel, N., Schmid, C., Weber, U., Tóth, G., Gühne, O., Ursin, R., Weinfurter, H.: Experimental analysis of a four-qubit photon cluster state. Phys. Rev. Lett. **95**(21), 210502 (2005)
67. Schwartz, I., Cogan, D., Schmidgall, E.R., Don, Y., Gantz, L., Kenneth, O., Lindner, N.H., Gershoni, D.: Deterministic generation of a cluster state of entangled photons. Science **354**(6311), 434–437 (2016)
68. Dong, P., Xue, Z.-Y., Yang, M., Cao, Z.-L.: Generation of cluster states. Phys. Rev. A **73**(3), 033818 (2006)
69. Zhang, X., Feng, M., Gao, K.L.: Cluster-state preparation and multipartite entanglement analyzer with fermions. Phys. Rev. A **73**(1), 014301 (2006)
70. Feynman, R.P.: Quantum mechanical computers. Found. Phys. **16**(6), 507–532 (1986)
71. Cai, X., Wang, T., Wei, C., Gao, F.: Cryptanalysis of multiparty quantum digital signatures. Quantum Inf. Process **18**(8), 252 (2019)
72. Horsman, C., Brown, K.L., Munro, W.J., Kendon, V.M.: Reduce, reuse, recycle for robust cluster-state generation. Phys. Rev. A **83**(4), 042327 (2011)
73. Zhang, C., Huang, Y.F., Liu, B.H., Li, C.F., Guo, G.C.: Experimental generation of a high-fidelity four-photon linear cluster state. Phys. Rev. A **93**(6), 062329 (2016)
74. Gimeno-Segovia, M., Rudolph, T., Sophia, E.: Economou Deterministic generation of large-scale entangled photonic cluster state from interacting solid state emitters. Physical review letters **123**(7), 070501 (2018)
75. Cao, Y., Parker, I.D., Yu, G., Zhang, C., Heeger, A.J.: Improved quantum efficiency for electroluminescence in semiconducting polymers. Nature **397**(6718), 414–417 (1999)
76. Li, S., Wang, L., Tang, D., Cho, Y., Xuejian, L.: Achieving high quantum efficiency narrow-band beta-sialon:eu2+ phosphors for high-brightness lcd backlights by reducing the eu3+ luminescence killer. In: Chemistry of Materials a Publication of the American Chemistry Society (2018)
77. Ajmal Khan, M., Matsumoto, T., Maeda, N., Kamata, N., Hirayama, H.: Improved external quantum efficiency of 293 nm algan uvb led grown on an aln template. Jpn. J. Appl. Phys. **58**(SA) (2019)
78. Karmalawi, A.M., Rayan, D.A., Rashad, M.M.: Establishment and evaluation of photovoltaic quantum efficiency system at central metallurgical research and development institute. Optik. 164931 (2020)
79. Deng, F.G., Ren, B.C., Li, X.H.: Quantum hyperentanglement and its applications in Quantum information Process. Sci. Bull. **62**(1), 46–68 (2017)
80. Cao, C., Wang, T., Mi, S., Zhang, R., Wang, C.: Nonlocal hyperconcentration on entangled photons using photonic module system. Ann. Phys. **369**, 128–138 (2016)
81. Ren, B.C., Long, G.L.: General hyperentanglement concentration for photon systems assisted by quantum-dot spins inside optical microcavities. Opt. Express **22**(6), 6547 (2014)
82. Cao, C., Zhamg, L., Han, Y., Yin, P., Fan, L., Duan, Y., Zhang, R.: Complete and faithful hyperentangled-bell-state analysis of photon systems using a failure-heralded and fidelity-robust quantum gate. Opt. Express **28**(3), 2857–2872 (2020)