Contemporary Mathematics
https://ojs.wiserpub.com/index.php/CM/

Research Article

Quantum Public-Key Cryptosystem Using Orthogonal Product States with High Channel Capacity

Xiaoyu Li*, **Yilin Chen**

School of Computer and Artificial Intelligence, Zhengzhou University, Zhengzhou City, Henan Province, The People's Republic of China
E-mail: iexyli@zzu.edu.cn

Received: 31 December 2024; **Revised:** 5 February 2025; **Accepted:** 6 February 2025

Abstract: A public-key cryptosystem using orthogonal product states is presented. It is based on the non-locality of some orthogonal product states in an untangled two-particle quantum system. Every user creates a group of two-particle quantum systems and shares them with a key management center (KMC) in which the first particle of the two-particle systems are held by the user and the second particle of the two-particle systems are held by KMC. This is the user's (private key, public key) pair. Two users can exchange secret message by this cryptosystem. The laws of quantum physics guarantees that this cryptosystem has unconditional security. There are no entangled states needed in this public-key cryptosystem. Moreover both users and KMC needn't perform complex quantum operations except quantum measurements on a particle or a two-particle system. So the public-key cryptosystem is feasible to implement by today's technology. One orthogonal product quantum system contributes three bits to the key. So the cryptosystem has a high channel capacity.

***Keywords*:** quantum public-key cryptosystem, orthogonal product states, message authentication, measurement, channel capacity

MSC: 94A60, 81P94

Abbreviation

KMC	Key Management Center
XOR	Exclusive OR
QKD	Quantum Key Distribution

1. Introduction

Quantum cryptography is a very active research field of quantum information technology. In quantum cryptography people use quantum particles or composed quantum sysytems as the information media to construct cryptographic protocols and cryptographic systems. The properties of quantum systems guarantee that quantum cryptographic protocols can achieve unconditional security, which is a big advantage in relative to classical cryptographic protocols based on

DOI: https://doi.org/10.37256/cm.6120256333

computation complexity. Bennett and Brassard presented the first quantum key distribution protocol in 1984 [1]. It is called BB84 protocol. Afterwards many QKD schemes were presented [2–10]. Experiments for QKD have also been realized. The first QKD experiment was finished by Bennett et al. in which they carried out BB84 protocl in laboratory [11]. Now people have realized QKD in optical fibred with a distance more than 400 km [12]. QKD in free space was also achieved beyond 1 kilometer [13]. In 2017 experimentalists completed QKD between Micius statelite and the earth station which the distance is over 1,200 kilometers [14].

It's known that key management is a complex and difficult problem in traditional classical cryptosystems. To slove this difficulity people developed public-key cryptographic algotirhms which can greatly reduce the complexity and expense of key mangement. In 1978 Rivest, Shamir and Adleman issued a public-key algorithm which is based on the large number decomposition problem [15]. It is the first public-key algorithm which is called RSA algorithm. Now public-key algorithms are applied widely in business affairs, military affairs, government affairs, personal privacy and so on. But in 1984 Peter Shor showed that RSA algorithm is crashed by a quantum alorithm which is known as Shor algorithm [16]. Later researchers found that most of classical public-key algorithms are unsafe if they are attacked by some quantum algorithms, too. Gottesman provided a quantum one-way function. He showed that it may be used to build a quantum message authentication scheme [17]. He also advised that we can use it to build a quantum public-key algorithm. Nikolopoulos proposed that the first quantum public-key cryptosystem [18] in 2008. In Nikolopoulos' scheme a user Alice creates a group of quantum particles which differ from each other by a angle in Bloch sphere of the state space of the particle. Then she saves the particle sequence in a key management center which is abbreviated KMC as her public-key while the state sequence of the particle sequence is her private key. Another user can send secret message to Alice by the help of KMC. After that researchers have developed many quantum public-key cryptosystems. Nikolopoulos and Ioannou presented a quantum cryptosystem in 2009 [19]. Then Ioannou and Mosca gave a extended version with reusable key based on it [20]. Luo et al. built a quantum public-key algorithm based on parameterized unitary groups [21]. Seyfarth et al. gave a discussion of the security of Ioannou's scheme [22]. Li et al. provided a quantum public-key cryptosystem using a set of non-orthogonal quantum states [23]. Vlachou et al. presented a scheme based on the special property of quantum walk [24]. A quantum public-key cryptosystem is issued by wang et al. in which the Bell states and generalized Pauli operations are appplied to realize a secure communication scheme [25]. Liu et al. gave a quantum public-key encryption scheme in which a user uses a four-state key to accomplish encryption and decryption [26]. Zhang et al. presented a quantum public-key crtptosystem which uses quantum teleportation to transmit secret message [27]. Li and Chen issued a quantum public-key cryptosystem with the Bell states [28]. A ternary quantum public-key crtptosystem utilising qubit rotation is provided by wang et al. [29].

In this paper we present a quantum public-key cryptosystem with high channel capacity. It uses the property of a set of orthogonal product states in a two-particle quantum system. Users creates a group of two-particle systems as the (public key, private key) pair. Every two-particle system is in one of nine orthogonal product states at random. Then user keeps the private key while KMC keeps the public key. N users can accomplish secret communications with each other in virtue of of KMC. Furthermore users can perform message authentication on the message exchanged. There are no entangled states used in secret communication or message authentication. Users and KMC needn't perform complex operations except quantum measurement on a single particle or a tow-particle composed system. So it's feasible to implement by today's technology in laboratory. User can accomplish message authentication to guarantee the truth and the integrity of the message. The cryptosystem is proved to be secure. One two-particle system can contribute three bits to the binary string which is actually used to encrypt the message. So the cryptosystem has a high channel capacity.

2. Main idea

In quantum science people often call a 3-level quantum system "a qutrit". We denote the three eigenstate states of a qutrit as $|0>$, $|1>$, $|2>$. In 1999 Bennett et al. [30] issued that there are nine states of a composed system which contains two qutrits

$$|\phi_1>=|1>|1>|\phi_2>=|0>\frac{1}{\sqrt{2}}(|0>+|1>)|\phi_3>=|0>\frac{1}{\sqrt{2}}(|0>-|1>)$$

$$|\phi_4>=|2>\frac{1}{\sqrt{2}}(|1>+|2>)|\phi_5>=|2>\frac{1}{\sqrt{2}}(|1>-|2>)|\phi_6>=\frac{1}{\sqrt{2}}(|1>+|2>)|0>$$

$$|\phi_7>=\frac{1}{\sqrt{2}}(|1>-|2>)|0>|\phi_8>=\frac{1}{\sqrt{2}}(|0>+|1>)|2>|\phi_9>=\frac{1}{\sqrt{2}}(|0>-|1>)|2>. \tag{1}$$

They compose a complete orthogonal state set denoted as

$$B_\phi=\{|\phi_1>,\ |\phi_2>,\ ...,\ |\phi_9>\} \tag{2}$$

which form a orthogonal measurement basis for a two-qutrit system. So a person can do measurement on a two-qutrit system in B_ϕ. On the other hand if a person wants to measure one qutrit in the two-qutrit system, he or she can measure it in any one the following three base

$$B_0=\{|0>,\ |1>,\ |2>\} \tag{3}$$

$$B_1=\left\{\frac{1}{\sqrt{2}}(|0>+|1>),\ \frac{1}{\sqrt{2}}(|0>-|1>),\ |2>\right\} \tag{4}$$

$$B_2=\left\{|0>,\ \frac{1}{\sqrt{2}}(|1>+|2>),\ \frac{1}{\sqrt{2}}(|1>-|2>)\right\}. \tag{5}$$

Bennett et al. proposed that such a two-qutrit system can show non-locality to a certain extent. Considering two persons, they can only do local operations on one qutrit of the two-qutrit system respectively. On the other hand they can’t exchange qutrits. Only classical information can be exchaged between them by a classical channel. If a qutrit’s state is one of the nine states, the two persons can’t determine in which state the two-qutrit system is for sure. Since then many cryptographic schemes based on these orthogonal product states have been developed [31–39]. In this paper we present a quantum public-key cryptosystem based on the non-locality of the orthogonal product states.

We assume that there are two users who are named as Alice and Bob. Just like that in classical public-key cryotosystem, a key management center (KMC) help the users to complete the secret communications. Then Alice produces M two-qutrit systems. Each two-qutrit system is randomly in one state of the state set $\{|\phi_1>,\ |\phi_2>,\ ...,\ |\phi_9>\}$. Alice records the state of each two-qutrit system. Finally she gets a state sequence

$$\varphi=(\psi^1\psi^2...\psi^i...\psi^M),\ \psi^i\in\{|\phi_1>,\ |\phi_2>,\ ...,\ |\phi_9>\} \tag{6}$$

Now the following coding rule is given which both Alice and Bob consent to.

Coding Rule

$$|\phi_1>\rightarrow null,\ |\phi_2>\rightarrow 001,\ |\phi_3>\rightarrow 010,$$

$$|\phi_4>\rightarrow 011,\ |\phi_5>\rightarrow 100,\ |\phi_6>\rightarrow 101,$$

$$|\phi_7>\rightarrow 110,\ |\phi_8>\rightarrow 111,\ |\phi_9>\rightarrow 000 \tag{7}$$

The code word "null" means that if the state is $|\phi_1>$, it will be ignored. Alice takes out the second qutrit (denoted as qutrit 2) of every two-qutrit system and gives them to KMC. She keeps the first qutrit (denoted as qutrit 1) at her hands. Now Alice holds an M-qutrit sequence denoted as d while KMC holds an M-qutrit sequence denoted as e. So we define e as Alice's public key. Accordingly, $< d,\ \varphi >$ is defined as Alice's private key.

Now Bob can sends a secret message to Alice by the help of KMC. First he contacts KMC to get the public key e of Alice. When Bob receives e, he asks Alice to perform an error-checking with him. They mutually select m qutrits from e at random. Then Bob measures these qutrits in B_0, B_1 or B_2 at random and writes down his measurement results. If Bob chooses the correct measurement basis, he will get the correct measurements result which is just the same as the original state of the qutrit. The correct measurement basis is showed as follows

Correct Basis Rule

If the state is $|\phi_1>$, $|\phi_6>$, $|\phi_7>$, $|\phi_8>$ or $|\phi_9>$, the correct basis is B_0; if the state is $|\phi_2>$ or $|\phi_3>$, the correct basis is B_1; if the state is $|\phi_4>$ or $|\phi_5>$, the correct basis is B_2.

Then Bob declares his measurement base and measurement results in the classical channel. To each qutrit which Bob has chosen the correct measurement basis, Aliice compares the state of qutrit 2 in φ and Bob's measurement result. They should be exactly identical if no eavesdroppers exist. It can be shown in Table 1.

Table 1. error-checking

State of two-qutrit system	State of qutrit 2	Correct measurement basis for Bob	Bob's result
$\vert\phi_1>$	$\vert 1>$	B_0	$\vert 1>$
$\vert\phi_2>$	$\frac{1}{\sqrt{2}}(\vert 0>+\vert 1>)$	B_1	$\frac{1}{\sqrt{2}}(\vert 0>+\vert 1>)$
$\vert\phi_3>$	$\frac{1}{\sqrt{2}}(\vert 0>-\vert 1>)$	B_1	$\frac{1}{\sqrt{2}}(\vert 0>-\vert 1>)$
$\vert\phi_4>$	$\frac{1}{\sqrt{2}}(\vert 1>+\vert 2>)$	B_2	$\frac{1}{\sqrt{2}}(\vert 1>+\vert 2>)$
$\vert\phi_5>$	$\frac{1}{\sqrt{2}}(\vert 1>-\vert 2>)$	B_2	$\frac{1}{\sqrt{2}}(\vert 1>-\vert 2>)$
$\vert\phi_6>$	$\vert 0>$	B_0	$\vert 0>$
$\vert\phi_7>$	$\vert 0>$	B_0	$\vert 0>$
$\vert\phi_8>$	$\vert 2>$	B_0	$\vert 2>$
$\vert\phi_9>$	$\vert 2>$	B_0	$\vert 2>$

If Alice and Bob gets too many different results, they come to a conclusion that eavesdroppers exist. They abandon the communication process. Or the error-checking passes. Alice and Bob go into the next step.

Alice sends Bob the left M-m qutrits in e using the quantum channel. When Bob gets them, he puts each qutrit together with the corresponding qutrit in d at his hands. At last Bob gets M-m two-qutrit systems. Bob performs collective measurements on every two-qutrit system in basis B_ϕ and writes down all the measurement results he gets. So he gets a state sequence φ' with a length M-m.

Then Alice and Bob perform the second error-checking. Considering that the state $|\phi_1>$ doesn't contribute code word in accordance with the Coding Rule, so all the two-qutrit systems in $|\phi_1>$ should be used in the error-checking. So at first Bob chooses $m1$ two-qutrit systems. They include all the two-qutrit systems which is in the state $|\phi_1>$ and some two-qutrit systems which is in one of $\{|\phi_2>, |\phi_2>, ..., |\phi_9>\}$ at random. Then Bob declares the $m1$ states in φ' through the classical channel. Next Alice compares them with the corresponding states in φ of her private key $< d, \varphi >$. If Alice and Bob find many disagreements, they confirm that some eavesdroppers have intervened. So they abandon the communication process. Or the second error-checking succeeds. They can continue.

To the left M-m-$m1$ states in φ, Alice records in accordance with the coding rule while to the left M-m-$m1$ states in φ', Bob records in accordance with the coding rule. Finally Alice will get a string K_a and Bob will get a string K_b. Obviously K_a should be equal to K_b if no eavesdroppers exist. So Bob can send Alice a n-bit secret message denoted P in which $n = 3(M\text{-}m\text{-}m1)$. Bob does an XOR operation on P and K_b. Then he gets $PS = P \oplus K_b$. Next Bob transmits PS to Alice. When Alice receives PS, she does an XOR operation on PS and K_a. It's obvious that Alice gets

$$P' = PS \oplus K_a = P \oplus K_b \oplus K_a = P \tag{8}$$

because $K_a = K_b$. Now Alice obtains the original secret message P. It will be proved in section 4.1 that no third party can get P. So Bob successfully makes Alice to receive a secret message. On the contrary, if Alice needs to send secret information to Bob, what they should do is to exchange their roles.

Finally we have to sovle the last problem. Alice's (public key, private key) pair is spent after Bob transmits her a secret message. It impossible for another user to implement secret communication with Alice just as Bob does. To solve this problem Alice should create many (public key, private key) pairs. All Alice's public keys are saved in KMC's storage.

3. The public-key cryptosystem using othogonal product states

In the cryptosystem N users want to perform secret communications with each other. Every user creates a sequence consisting of M two-qutrit systems. This is his or her (public key, private key) pair in which every two-qutrit system is in one state in $\{|\phi_1>, |\phi_2>, ..., |\phi_9>\}$ at random. A user has L (public key, private key) pairs. For example, Alice's private key set is

$$(K^d)_{Alice} = \{< d_i, \varphi_i >, i = 1, 2, ..., L\} \tag{9}$$

in which

$$\varphi_i = (\psi^1 \psi^2 ... \psi^j ... \psi^M), \ \psi^j \in \{|\phi_1>, |\phi_2>, ..., |\phi_9>\} \tag{10}$$

Alice keeps her public key set

$$(K^e)_{Alice} = \{e_i, \ i = 1, 2, ..., L\} \tag{11}$$

in KMC. Everyone can send and receive classical information through a public classical channel. On the other hand the classical channel is authenticated, or in other words, everyone can affirm who is exchanging classical information with him. There is an public quantum channel needed. Two persons can can exchange qutrits through the quantum channel. But the quantum channel is insecure. It's open to all persons.

3.1 *Secret communication process*

Without losing generality, we assume that two users Alice and Bob wants to perform secret communication. Bob decides to send Alice a binary string P which can't be obtained by any other one except Alice. Alice and Bob execute the process.

Step 1: Bob contacts KMC asking for one of Alice's public keys, for example e_j. Then KMC sends e_j to Bob through the quantum channel

Step 2: Bob tells Alice and asks Alice to perform the first error-checking process together with him.

Step 3 (the first error-checking): Alice and Bob mutually choose m qutrits in e_j at random. Then Bob measures them in B_0, B_1 or B_2 at random and records his (measure basis, measurement result) for each qutrit. Bob declares his (measure basis, measurement result) sequence through the classical channel. Alice chooses the corresponding states in φ_j of her private key $< d_j,\ \varphi_j >$ and compares with Bob's (measure basis, measurement result) sequence in accordance with the Correct Basis Rule in section 2. To each qutrit if Bob has just chosen the correct basis, his measurement result must be identical to the corresponding state in φ_j at Alice's hands. If Alice and Bob find that they gets too many different results, they stop the communication and go back to step 1. Or they continue to perform the next step.

Step 4: Bob throws the m checking qutrits in e_j while Alice throws the corresponding m qutrits in d_j. Then Alice sends the left M-m qutrits in d_j to Bob.

Step 5 (the second error-checking): After Bob receives these qutrits from Alice, he puts them together with the corresponding M-m qutrits in e_j. So Bob gets M-m two-qutrit systems. Then Bob measures them in basis B_ϕ. Next Bob chooses $m1$ two-qutrit systems which include all the two qutrit systems which are in $|\phi_1 >$ and some two-qutrit systems which are in one state of the eight-state set $\{|\phi_2 >,\ |\phi_3 >,\ ...,\ |\phi_9 >\}$. Bob declares the measurement results of the $m1$ two-qutrit systems through the classical channel. Then Alice compares Bob's measurement results of the $m1$ two-qutrit systems with the corresponding states in φ_j. If Alice finds two many disagreements, she tells Bob to stop communication and go back to step 1. Or they enter the next step.

Step 6: Bob records in accordance with the coding rule to the left M-m-$m1$ measurement results. Finally Bob obtains K_b which is a n-bit binary string with $n = 3(M\text{-}m\text{-}m1)$.

Step 7: To the left M-m-$m1$ states in φ_j, Alice records in accordance with the coding rule. So Alice obtains K_a. It is an n-bit binary string with $n = 3(M\text{-}m\text{-}m1)$. Obviously we have $K_a = K_b$.

Step 8: In order to send P to Alice, Bob implements an XOR operation on P and K_b. So he has $EP = P \oplus K_b$. Next Bob transmits EP to Alice.

Step 9: Alice implements an XOR operation on EP and K_a when she receives EP, So she gets

$$P' = EP \oplus K_a = P \oplus K_b \oplus K_a = P.$$

Now Alice obtains P. It is just what Bob hope to transmit to Alice. It's easy to find out that every two-qutrit system contribute three bit for K_a or K_b. So the cryptosystem has a high channel capacity.

On the contrary, if Alice decides to transmit Bob a message secretly, what they should do is exchanging their roles in the above communication process.

3.2 *Message authentication*

To guarantee the reality and integrity of the message, Bob can apply message authentication to the message before he sends it to Alice. After receiving the message, Alice verify it. If the verification is successfull, Alice can assure that the message is really sent by Bob. Moreover it hasn't been tampered before arriving to Alice.

3.2.1 *Authentication process*

First every user agrees to the authentication rule.

Authentication Rule

$$\frac{1}{\sqrt{2}}(|0>+|1>)\rightarrow 0,\ \frac{1}{\sqrt{2}}(|0>-|1>)\rightarrow 1,$$

$$\frac{1}{\sqrt{2}}(|1>+|2>)\rightarrow 0,\ \frac{1}{\sqrt{2}}(|1>-|2>)\rightarrow 1,$$

$$|1>\rightarrow 1,\ |0>\rightarrow 0,\ |2>\rightarrow 1 \tag{12}$$

Before Bob sends the message to Alice, he performs message authentication on it. To produce the authentication token, Bob does as follows.

Step 1: Bob applies SHA-1 algorithm to P. At last he gets a $n1$-bit string AP which is the abstract of P.

Step 2: Bob randomly selects $< d_k,\ \varphi_k >$ from his private key set and takes out the first $n1$ states in φ_k.

Step 3: To every one of the $n1$ states, Bob gets the state of the second qutrit and records in accordance with the authentication rule. At last he obtain S_B which is a $n1$-bit binary string.

Step 4: Bob apply an XOR operation to AP with S_B. So he has $PS = AP \oplus S_B$.

Step 5: Bob puts k and PS together with P. Then he gets a string PDS.

Now Bob sends PDS to Alice in accordance with the communication process in section 3.1. It must be pointed that the length of the string PDS is n in order to guarantee it to be sent as the communication process asks. It's easy to be realized by dividing the origin message into several parts with appropriate length.

3.2.2 *Verification process*

When Alice receives PDS after the communication process, she performs as follows.

Step 1: Alice divides PDS into k, P and PS. Then Alice gets the public key e_k of Bob from KMC.

Step 2: Alice takes out the first $n1$ qutrits in e_k. Then Alice informs Bob to declare the correct measurement basis sequence for these qutrits.

Step 3: Bob declares the correct measurement basis sequence

$$B_V = (B_1 B_2 ... B_i ... B_{n1}),\ B_i \in \{B_0,\ B_1,\ B_2\} \tag{13}$$

in accordance with the correct basis rule in section 2.

Step 4: Alice measures each qutrit in accordance with B_V. She writes down all the measurement results in accordance with the authentication rule. So Alice has an $n1$-bit binary string S_A.

Step 5: Alice apply an XOR operation to PS with S_A. As a result, she obtains $AP' = PS \oplus S_A$.

Step 6: Alice applies SHA-1 algorithm to P. Then she obtains an $n1$-bit string AP. As known AP is the abstract of P.

Step 7: Alice compares AP and AP'. If $AP' = AP$, the verification is valid. Alice comes to a conclusion that it's Bob for sure who sends the message to her and the message is complete with out being distorted.

Obviously we have $S_B = S_A$ if no eavesdroppers exist. It's summarized in the following Table 2.

Table 2. Relations of S_B and S_A

The state in φ_k	The bit in S_B	The state of qutrit in e_k	Alice's measurement basis	The bit in S_A
$\|\phi_1>$	1	$\|1>$	B_0	1
$\|\phi_2>$	0	$\frac{1}{\sqrt{2}}(\|0>+\|1>)$	B_1	0
$\|\phi_3>$	1	$\frac{1}{\sqrt{2}}(\|0>-\|1>)$	B_1	1
$\|\phi_4>$	0	$\frac{1}{\sqrt{2}}(\|1>+\|2>)$	B_2	0
$\|\phi_5>$	1	$\frac{1}{\sqrt{2}}(\|1>-\|2>)$	B_2	1
$\|\phi_6>$	0	$\|0>$	B_0	0
$\|\phi_7>$	0	$\|0>$	B_0	0
$\|\phi_8>$	1	$\|2>$	B_0	1
$\|\phi_9>$	1	$\|2>$	B_0	1

So we have

$$AP' = PS \oplus S_A = AP \oplus S_B \oplus S_A = AP \tag{14}$$

It will be proved in Section 4 that eavesdroppers can't falsify the authentication token or distort the message. So we have showed users can realize the message authentication successfully.

4. Security of the quantum public-key cryptosystem

The communication process and the authentication process are secure. We prove it as follows.

4.1 *Secret communication process*

Tow users can exchage message secretly. No third party can acquire the message.

When Bob wants to send a secret message to Alice, an eavaedrooper, Eve, tries to obtain it. First Eve may catche the qutrits in e_j when they are being transfered from KMC to Bob in step 2 of the communication process in section 3.1. Eve may measures these qutrits to draw certain information which is helpful to her in getting Bob's message. But it's infeasible because the qutrits are in some non-orthogonal states at random. There are three base B_0, B_1, B_2. Eve doesn't know the correct measurement basis for any qutrit. If she chooses a wrong basis to measure a qutrit, the state of the qutrit will collapse to the basic vector of the basis. Obviously the probability for Eve to just select the correct basis for one qutrit is

$$p_1 = \frac{1}{3}. \tag{15}$$

In step 3 of the communication process, Bob and Alice do the first error-checking. To qutrit if Eve selects the right basis, her measurement doesn't change the state of the qutrit. So Alice and Bob will get the same results without finding anything wrong. In general, the probability which Alice and Bob obtains identical results is $\frac{1}{3}$. If Eve selects a wrong basis, the state of the qutrit will be changed. In general, the probability for them to obtain identical results is

$$p_2 = \frac{1}{9} \times \left(\frac{1}{3} \times \left(\frac{1}{2} \times \frac{1}{2} + \frac{1}{2} \times \frac{1}{2} \right) \times 2 \right) \times 9 = \frac{1}{3} \tag{16}$$

Then the whole probability which they obtain identical results is

$$p_s = p_1 + p_2 = \frac{2}{3} \tag{17}$$

For all the m qutrits in error-checking, the probability is

$$P_{error} = (p_s)^m = \left(\frac{2}{3} \right)^m \tag{18}$$

If $m = 100$,

$$P_{error} = \left(\frac{2}{3} \right)^{100} \approx (10)^{-18} \tag{19}$$

It's a very, very small number. As a result, Alice and Bob will get many disagreements in the first error-checking and abandon the communication process. At last Eve gets nothing. So Eve can't succeed in getting the message by measuring the qutrits from KMC to Bob.

Second in the step 4 of the communication process when Alice sends the qutrits of d_j to Bob, Eve may catches them trying to get some information about the message. She won't succeed because Alice and Bob perform the second error-checking in the step 5. If Eve measures the qutrits, she face the same situation discussed above. Obviously the probability which Alice and Bob don't detect Eve's existence is

$$P_{error} = \left(\frac{2}{3} \right)^{m1} \tag{20}$$

in which $m1$ is the number of two-qutrit systems which are used for error-checking in step 5 (the second error-checking) of the communication process in section 3.1. If $m1 = 100$,

$$P_{error} = \left(\frac{2}{3} \right)^{100} \approx (10)^{-18} \tag{21}$$

That is to say, Eve is destined to be detected. This attack method can't succeed.

Third in step 8 of the communication process Eve may obtain the string EP when Bob sends it to Alice. But Eve can't obtain the message P from EP. The reason is that $EP = P \oplus K_a$. Though Eve has EP, she can't obtain P because she has no chance of getting K_a or K_b which is equal to K_a at all.

Fourth Eve may perform a collective attack. That is to say, she may catch both the qutrits in e_j which KMC sends Bob and the qutrits in d_j which Alice sends Bob. To every qutrit in e_j and the corresponding one in d_j Eve put them together to form a two-qutrit system. Then she does collective measurements on these two-qutrit systems. To do this Eve must catch the qutrits in e_j and keep them until she gets the qutrits in d_j to perform collective measurements. But once Eve does as above, Bob won't receive e_j in step 2. So Alice and Bob can't performs communication process any more. They terminate communication at once. As a result, Eve gets nothing. On the other hand Eve may try to make a copy of each qutrit in e_j and a copy of each qutrit in d_j. Then to ecah copy of qutrit in e_j and the corresponding copy of qutrit in d_j Alice puts them together to form acomposed system. So she can implement collective measurement on the two-qutrit systems with intention to get something about the message. But quantum non-cloning theorem forbids her to copy an unknown state. Eve isn't able to do such collective attack.

Finally can KMC obtain the secret message exchanged between Alice and Bob by its special position? In the quantum public-key cryptosystem, KMC knonw nothing about the state of any qutrit in e_j though it keeps e_j. As a result, KMC can do nothing more that Eve can do. That is to say, KMC can't obtain the secret message, too.

Now it has been proved that no third party can get the secret message which Bob want to give Alice. So the communication process is secure.

4.2 *Message authentication process*

It can be proved that the message authentication on Bob's message is secure. No one can fake the authentication token of Bob's message. If the message is distorted when it is transfered from Bob to Alice, the verification of message authentication is sure to fail. So Alice will find that the message is incredible. We give the proof as follows.

It's easy to notice that the verification passes if and only if $S_B = S_A$. If an eavesdropper Eve wants sends a faked message pretending to be from Bob, she has to make Alice to get a string S_A which is equal to a string S_E at her hands. According the step 3 and step 4 of the verification process, Alice gets S_A by measuring Bob' public key e_k in the correct measurement basis sequence B_V which Bob gives her. Bob can deduce Alice's measurement results because he has his private key $< d_k, \varphi_k >$ so that Bob can get S_B which is equal to S_A. But Bob keeps his private key absolutely secret. Eve has no way to get it. Moreover Eve has no way to get the correct measurement basis sequence B_V. What ever does Eve do, the probability that she make Alice to get a string S_A with $S_A = S_E$ is no more than

$$P_{Eve} = \left(\frac{1}{2}\right)^{n1}. \tag{22}$$

If $n1 = 100$,

$$P_{Eve} = \left(\frac{1}{2}\right)^{100} \approx 10^{-30}. \tag{23}$$

So any faked message produced by Eve can't pass the verification.

On the other hand we assume that the message is distorted when it is transfered from Bob to Alice. That is to say, in step 1 of the verification process P turns into another string Pe. Then Alice produces the abstract of Pe to get a string APe in step 6 of the verification process. On the other hand Alice get $AP' = PS \oplus S_A$ from the authentication token PS in step 5 of the verification process. Alice compares Ape and AP'. Obvious Alice will find $APe \neq AP'$. So Alice finds that the message has been distorted.

5. Feasibility and advantages

In the public-key cryptosystem users and KMC need to perform some operations as follows. They need creat a group of two-qutrit systems, perform single-particle measurement on one qutrit and do collective measurement on a composed system containing two qutrits. All these operations have been fulfilled in practice for decades of years. So there are no serious technical difficulities for this public-key cryptosystem. But there is still a problem left. As known quantum systems will occur decoherence inevitably over time. It may cause quantum states collapse and quantum cryptographical protocols fail. In QKD protocols the key distribution process is always excuted very fast so that it has been completed befor decoherence happens. But to a public key cryptosystem KMC need keep every user's the public key which consists of quantum particles for a long time waiting for a user to ask for it. This is an obstacle to all quantum public-key cryptographical systems. A possible solution is to rebuild users' public keys peroidicaly before decoherence occurs. But building a large-scale quantum cryptographic networks is still very difficult. Biham, Hunter and Tor a quantum cryptographical network based quantum memories [40]. It may be possible to construct wide-range quantum public key cryptosystems in practice using their method. We will discuss it in our future work.

In this cryptosystem the (public key, private key) pair is build from two-qutrit system. No entangled states are needed. As known manipulating and keeping entangled states are much more difficult than manipulating and keeping unentangled states. Moreover both users and KMC needn't perform complex quantum operations. As a result realizing this quantum public-key cryptosystem has less technical difficulties. Obviously this is an advantage over many other schemes.

Another advantage is that in this cryptosystem one two-qutrit system can produce three bits of K_a which is used to do an XOR operation with the plaint text. It means that users can use a smaller amount of two-qutrit systems to encrypt a longer plain text. So this cryptosystem can gain a high channel capacity.

6. Conclusion

This paper provides a quantum public-key cryptosystem using orthogonal product states with high channel capacity. Every uses a group of two-qutrit systems as his or her (public key, private key) pair. The private key is kept by user himself while the public key is kept by KMC. Users can accomplish secure communications with the help of KMC. Moreover user can apply message authentication to the secret message. No entangled states are needed. Meanwhile people needn't perform complex quantum operations except quantum measurements. So it's easier for people to realize this cryptosystem than many previous schemes. One two-qutrit quantum system can contribute three bits to the string which is actually used to encrypt the message. So the cryptosystem can gain a high capacity.

Acknowledgement

This research is supported by Natural Science Foundation of China (Grants 61876016). The authors would thank Ruqian Lu for directing them into the study of quantum cryptography and quantum computing.

Conflict of interest

The authors declare no competing financial interest.

References

[1] Bennett CH, Brassard G. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science-TCS*. 1984; 560: 175-179.

[2] Ekert AK. Quantum cryptography based on Bell's theorem. *Physical Review Letters*. 1991; 67(6): 661-663.

[3] Bennett CH, Brassard G, Mermin ND. Quantum cryptography without Bell's theorem. *Physical Review Letters*. 1992; 68(5): 557-559.

[4] Lo HK, Chau HF. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*. 1999; 283(5410): 2050-2056.

[5] Qi B, Zhao Y, Ma XF, Lo HK, Qian L. Quantum key distribution with dual detectors. *Physical Review A*. 2007; 75(5): 052304.

[6] Matsumoto R. Multiparty quantum-key-distribution protocol without use of entanglement. *Physical Review A*. 2007; 76(6): 062316.

[7] Zhao Y, Qi B, Lo HK. Quantum key distribution with an unknown and untrusted source. *Physical Review A*. 2008; 77(5): 052327.

[8] Horodecki K, Horodecki M, Horodecki P, Leung D, Oppenheim J. Quantum key distribution based on private states: Unconditional security over untrusted channels with zero quantum capacity. *IEEE Transactions on Information Theory*. 2008; 54(6): 2604-2620.

[9] Aguilar EA, Ramanathan R, Kofler J, Pawłowski M. Completely device independent quantum key distribution. *Physical Review A*. 2016; 94(2): 022305.

[10] Hatakeyama Y, Mizutani A, Kato G, Imoto N, Tamaki K. Differential-phase-shift quantum key distribution protocol with small number of random delay. *Physical Review A*. 2017; 95(4): 042301.

[11] Bennett CH, Bessette F, Brassard G, Salvail L, Smolin J. Experimental quantum cryptography. *Journal of Cryptology*. 1992; 5(1): 3-28.

[12] Yin HL, Chen TY, Yu ZW, Liu H, You LX, Zhou YH, et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Physical Review Letters*. 2016; 117(19): 190501.

[13] Buttler WT, Hughes RJ, Kwiat PG, Lamoreaux SK, Luther GG, Morgan GL, et al. Practical free-space quantum key distribution over 1 km. *Physical Review Letters*. 1998; 81(15): 3283-3286.

[14] Liao SK, Cai WQ, Liu WY, Zhang L, Li Y, G RJ, et al. Satellite-to-ground quantum key distribution. *Nature*. 2017; 549(7670): 43-47.

[15] Rivest R, Sharmir A, Adleman L. A method for obstaining digital signature and public-key cryptosystem. *Communications of ACM*. 1978; 21(2): 120-126.

[16] Shor PW. Algorithms for quantum computation: Discrete logarithm and factoring. In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. USA: IEEE Computer Society; 1994. p.124-134.

[17] Gottesman D, Chuang I. Quantum digital signatures. *arXiv:quant-ph/0105032*. 2001. Available from: https://doi.org/10.48550/arXiv.quant-ph/0105032.

[18] Nikolopoulos GM. Applications of single-qubit rotations in quantum public-key cryptography. *Physical Review A*. 2008; 77: 032348.

[19] Nikolopoulos GM, Ioannou LM. Deterministic quantum-public-key encryption: Forward search attack and randomization. *Physical Review A*. 2009; 79: 042327.

[20] Ioannou L, Mosca M. Public-key cryptography based on bounded quantum reference frames. *Theoretical Computer Science*. 2014; 560(1): 33-45.

[21] Luo MX, Chen XB, Yun D, Yang YX. Quantum Public-Key Cryptosystem. *International Journal of Theoretical Physics*. 2012; 51(3): 912-924.

[22] Seyfarth U, Nikolopoulos G, Alber G. Symmetries and security of a quantum-public-key encryption based on single-qubit rotations. *Physical Review A*. 2012; 85(2): 022342.

[23] Li XY, Chen YW. Quantum public-key cryptosystem without quantum channels between any two users using non-orthogonal states. *International Journal of Security and Its Applications*. 2015; 9(9): 253-264.

[24] Vlachou C, Rodrigues J, Mateus P, Paunković N, Souto A. Quantum walk public-key cryptographic system. *International Journal of Quantum Information*. 2015; 13(7): 1550050.

[25] Wu W, Cai QY, Zhang HG, Liang XY. Quantum public key cryptosystem based on bell states. *International Journal of Theoretical Physics*. 2017; 56(11): 3431-3440.

[26] Liu ZX, Xie QL, Zha YF, Dong YM. Quantum public key encryption scheme with four states key. *Physica Scripta*. 2022; 97(4): 045102.

[27] Zhang D, Li X. A quantum public-key cryptosystem without quantum channels between any two users based on quantum teleportation. *International Journal of Theoretical Physics*. 2022; 61(4): 101.

[28] Li XY, Chen LJ. Quantum public-key cryptosystem without quantum. *Romanian Journal of Physics*. 2022; 67: 118.

[29] Wang Y, Chen G, Jian L, Zhou Y, Liu S. Ternary quantum public-key cryptography based on qubit rotation. *Quantum Information Processing*. 2022; 21(6): 197.

[30] Bennett CH, DiVincenzo DP, Fuchs CA, Mor T, Rains E, Shor PW, et al. Quantum nonlocality without entanglement. *Physical Review A*. 1999; 59(2): 1070-1091.

[31] Guo GP, Li CF, Shi BS, Li J, Guo GC. Quantum key distribution scheme with orthogonal product states. *Physical Review A*. 2001; 64(4): 042301.

[32] Yang Y, Wen Q, Zhu F. An efficient quantum secret sharing protocol with orthogonal product states. *Science in China Series G: Physics, Mechanics and Astronomy*. 2007; 50(3): 331-338.

[33] Yang YG, Wen QY. An efficient quantum key distribution protocol with orthogonal product states. *Chinese Physics*. 2007; 16(8): 2215-2218.

[34] Xu J, Chen H, Liu Z. An efficient quantum key distribution protocol with orthogonal product states. *International Journal of Quantum Information*. 2012; 10(3): 1250031.

[35] Jiang DH, Xu GB. Multiparty quantum key agreement protocol based on locally indistinguishable orthogonal product states. *Quantum Information Processing*. 2018; 17(7): 180.

[36] Jiang DH, Hu QZ, Liang XQ, Xu GB. A novel quantum multi-signature protocol based on locally indistinguishable orthogonal product states. *Quantum Information Processing*. 2019; 18(9): 268.

[37] Jiang DH, Wang J, Liang XQ, Xu GB, Qi HF. Quantum voting scheme based on locally indistinguishable orthogonal product states. *International Journal of Theoretical Physics*. 2020; 59(2): 436-444.

[38] Du G, Zhou BM, Ma CG, Zhang S, Li JY. A secure quantum voting scheme based on orthogonal product states. *International Journal of Theoretical Physics*. 2021; 60(4): 1374-1383.

[39] Zhang DX, Li XY, Zhao QY. Quantum public-key cryptosystem based on the non-locality in unentangled quantum system. *Brazilian Journal of Physics*. 2024; 54(5): 158.

[40] Biham E, Huttner B, Mor T. Quantum cryptographic network based on quantum memories. *Physical Review A*. 1996; 54(4): 2651-2658.