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

Research Article

A Quantum Public-Key Cryptosystem Without Quantum Storage for Public-Keys

Xiaoyu Li[1*], Zhipeng Fang[2]

[1] School of Computer and Artificial Intelligence, Zhengzhou University, Zhengzhou, Henan, China
[2] School of Cyber Science and Engineering, Zhengzhou University, Zhengzhou, Henan, China
E-mail: iexyli@zzu.edu.cn

Received: 18 June 2025; **Revised:** 13 October 2025; **Accepted:** 16 October 2025

Abstract: A quantum public-key cryptosystem without quantum storage for public-keys is provided. In traditional quantum public-key cryptosystems the public key of a user is a set of quantum systems. There is a Key Mangement Center (KMC) which needs to keep the public keys of all users for a long time to satisfy communication requirments between users. But it's very difficult to keep quantum systems for a long time beacuse quantum system will undergo decoherence with time. This is a big obstacle for quantum public-key crytosystems when they are applied in practice. This quantum public-key cryptosystem can solve this problem. A user keeps a state sequence and a binary string in the key management center called the source key which is only a piece of classical information. If one user A wants to have another user B to get a secret message, KMC creates a sequence of quantum systems according to the latter one's source key, which is just the user's (public key, private key) pair. Then the two users can acomplish secure communications with KMC's assistance. On the otherhand users can also perform message authentication on the messages to guarantee that the messages can't be forged or distorted. In this cryptosystem KMC needs no quantum storage for public keys, which greatly reduces the technical difficulities of key management and secret communication. Moreover any two users needn't keep a quantum channel between them. Therefore to realize and apply this quantum public-key cryptosystem is much more easier than traditional quantum public-key cryptosystems.

***Keywords*:** quantum public-key cryptosystem, quantum storage, the source key, measurement, message authentication, security

MSC: 81P94, 94A60, 68P25

Abbreviation

KMC	Key Management Center
XOR	Exclusive OR
QKD	Quantum Key Distribution
QPK	Quantum Public-Key

DOI: https://doi.org/10.37256/cm.6620257498

1. Introduction

Quantum information technology is the integration of quantum physics and information technology. Quantum cryptography is a very active and important fields in quantum inforamtion technology. As known classical cryptosystems are based on the complexity of computation, which make them to be computationally secure. But quantum cryptosystems are based on the pricinples of quantum physics. So they can have unconditional security. In 1984 Bennett and Brassard issued a Quantum Key Distribution (QKD) protocol [1]. It's the first quantum cryptographic protocol which is also called BB84 protocol. After that researchers have developed many QKD protocols. For example, Ekert's scheme based on Bell theorem [2], the improved scheme for BB84 (named B92 scheme) [3], QKD scheme based on an unknown and untrusted source [4], QKD scheme over untrusted channels with zero quantum capacity [5], semi-quantum key distribution shemes [6–8], mediated semi-quantum key distribution schemes [9, 10], device independent QKD schemes [11, 12], continuous-variable QKD scheme [13], discrete-phase-randomized twin-field QKD scheme [14], high-dimensional QKD schemes [15] and noise-resilient QKD scheme [16]. The expermental work for QKD has also been fulfilled. The first experiment for BB84 protocol is performed by Bennett's research group [17]. Now people have finished QKD experiments in optical fibre over 400 kilometers [18]. Experimental experts have also completed QKD experiments in free space beyond 1 km [19]. QKD experiment between the satelite and earth station with a distantce more than 1,200 km were also realized [20].

In tranditional cryptosystems, key management is the most difficult and most complex problem. Public-key algorithm is a milestone in cryprography. It needs much lower key management expense. Rivest, Shamir and Adleman gave the first public-key algorithm named Rivest-Shamir-Adleman (RSA) algorithm [21]. Today people have developed many public-key algorithms which have become one of the foundation stones for information security in modern society. But Shore issued a quantum algorithm [22]. It's proved to be able to crack RSA algorithm in polynomial time. Since then most public-key algorithms have been found to be unsecure on future quantum computer, which forms a serous threat to information and network security. Gottesman is the first researcher trying to solve this problem. He gave a quantum one-way function [23] for quantum digital signature. At the same time he suggested people to dsign quantum public-key algorithms on possible quantum one-way functions. In 2008 Nikolopoulos first proposed a Quantum Public-Key (QPK) algorithm based on rotation of sigle-particle quantum state [24]. Thereafter many QPK cryptosystems were presented. Nikolopoulos et al. presented a deterministic quantum-public-key encryption in 2009 [25]. Ioannou issued a QPK cryptosystem based on bounded quantum reference frames [26]. Luo et al. gave a QPK cryptosystem which is based on one-parameter unitary groups [27]. In 2012 Seyfarth et al. studied symmetries and security of random QPK cryptosystem based on single-qubit rotations [28]. A quantum public-key cryptographic system based on quantum walk is given by Vlachou et al. [29]. Wu et al. provided a QPK cryptosystem based on the Bell States [30]. Yang et al. designed a QPK scheme based on conjugate coding [31]. Liu et al. presented a QPK cryptosystem with four states key [32]. Zhang et al. proposed a QPK cryptosystem based on quantum teleportation [33]. Li et al. put forward a QPK cryptosystem without quantum channels between any two users [34]. Wang gave a ternary QPK cryptosystem based on qubit rotation [35]. Barooti et al. developed a QPK cryptosystem with a group of quantum key [36]. Rencently research findings on QPK are still continuously brought forward [37–41].

As known in public-key cryptosystems the Key Management Center (KMC) must store the public key of every user. If one user wants to send a secret message to another user, he or she will ask KMC for the latter user's public key. Under normal circumstances KMC need store all users' public keys for long periods to satisfy communication requests which may arrive from time to time. It is not a problem in classical public-key cryptosystems because usually the public key is only one binary string or a group of binary strings. But in quantum public-key cryptosystems public keys are often a group of quantum systems. It's known that quantum systems will evitablely undergo decoherence over time, which may cause quantum systems to lose quantum coherence. So the quantum public-key cryptosystem is doomed to collapse. It's very difficult and expensive for KMC to store quantum systems which serve as users' public keys for a long period of time. It brings big difficulities for quantum public-key crytposystems to be applied in practice.

This paper presented a quantum public-key cryptosystem without quantum storage for public keys. KMC need only keep some classical information denoted as the source key for every user. Only when a communication request arrives, KMC temporarily creates a set of composed eantangled quantum systems as the (public key, private key) pair for the

user from his or her source key. So KMC needn't keep quantum systems for a long time any longer, which significantly reduces the technical difficulites and management expense of this cryptosystem. Furthermore any two users don't send qubits to each other so that they needn't a quantum channel conecting them. Thus this cryptosystem is much easier to be implemented in practical applications.

2. Main idea

In quantum information research a two-level particle or multiparticle system is defined as a 'qubit' on which people can encode inforamtion. Its state space is a two-dimension Hilbert space. People can measure a qubit in a complet orthogonal basis $\{|0>, |1>\}$ or in another complet orthogonal basis $\{|+>, |->\}$ in which

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

A composed system consisiting of two qubits can in one state of the four Bell states

$$|\Phi^+>=\frac{1}{\sqrt{2}}(|00>+|11>)=\frac{1}{\sqrt{2}}(|+->+|-+>)$$

$$|\Phi^->=\frac{1}{\sqrt{2}}(|00>-|11>)=\frac{1}{\sqrt{2}}(|+->-|-+>)$$

$$|\Psi^+>=\frac{1}{\sqrt{2}}(|01>+|10>)=\frac{1}{\sqrt{2}}(|++>+|-->)$$

$$|\Psi^->=\frac{1}{\sqrt{2}}(|01>-|10>)=\frac{1}{\sqrt{2}}(|++>-|-->). \tag{2}$$

We assume that a two-qubit quantum system is in one state of $\{|\Phi^+>, |\Phi^->, |\Psi^+>, |\Psi^->\}$. Two persons hold one qubit of the two-qubit system respectively, they can perform measurements on the qubit at his or her hands respectively. As known there are definite correlations between their measurement results. It is summarized in the following Table 1.

Table 1. Measurement results correlations

Two-qubit's state	Measurement basis	Results relations
$\|\Phi^+>$	$\{\|0>, \|1>\}$	Identical
$\|\Phi^+>$	$\{\|+>, \|->\}$	Contrary
$\|\Phi^->$	$\{\|0>, \|1>\}$	Identical
$\|\Phi^->$	$\{\|+>, \|->\}$	Contrary
$\|\Psi^+>$	$\{\|0>, \|1>\}$	Contrary
$\|\Psi^+>$	$\{\|+>, \|->\}$	Identical
$\|\Psi^->$	$\{\|0>, \|1>\}$	Contrary
$\|\Psi^->$	$\{\|+>, \|->\}$	Identical

Now two users, Alice and Bob, want to exchange secret messages. There is a KMC which servers for them to finish communications. There is an insecure quantum channel and an authenticated classical channel needed. The authenticated classical channel is public so that everyone can listen to it but no one can pretend to be other one. On the other hand the insecure quantum channel is open to everyone. First Alice creates a random state sequence

$$\varphi = (\varphi_1 \varphi_2 \ldots \varphi_N), \;\; \varphi_i \in \{|\Phi^+>, |\Psi^+>\}. \tag{3}$$

Alice creates a binary string R at random. Then Alice shares $< \varphi, R >$ with KMC. It is called Alice's source key. Both Alice and KMC must keep $< \varphi, R >$ absolutely secret so that no orthers can get it. When Bob wants to send a secret message to Alice, he asks for KMC's help. Then KMC produces N composed two-qubit quantum systems in which the state of each two-qubit system is

$$|\Phi^+>= \frac{1}{\sqrt{2}}(|0>_1 |0>_2 + |1>_1 |1>_2)$$

or

$$|\Psi^+>= \frac{1}{\sqrt{2}}(|0>_1 |1>_2 + |1>_1 |0>_2). \tag{4}$$

according to φ. The two-qubit sysyem sequence is just Allice's (public key, private key) pair. The subscript "1" and "2" mark the different two qubits. Furthermore the qubit sequence consisting of qubit 1of each quantum two-qubit system is denoted as d which is just Alice's private key. And the qubit sequence consisting of qubit 2 of each quantum two-qubit system is denoted as e which is just Alice's private key. KMC sends e to Bob while it keeps d by itself. After receiving e, Bob measures every qubit in meaurement basis $\{|0>, |1>\}$ while he writes down his measurement results as a state sequence

$$\xi = (\xi_1 \xi_2 \ldots \xi_N), \;\; \xi_i \in \{|0>, |1>\}. \tag{5}$$

Then Bob performs on ξ according to the Coding Rule.

Coding Rule:

When ξ_i is $|0>$, Bob gets "0"; when ξ_i is $|1>$, Bob gets "1".

At last Bob gets a binary string

$$m = (m_1 m_2 \ldots m_N), \;\; m_i \in \{0, 1\}. \tag{6}$$

If Bob wants to send a secret message P to Alice in which P is an N-bit string, he does an Exclusive OR (XOR) operation on P and m. Finally Bob obstains

$$S = P \oplus m. \tag{7}$$

Then Bob transfers S to Alice through the public classical channel. On the other hand KMC measures every qubit at his hands in meaurement basis $\{|0>, |1>\}$. The measurement results can be denoted as a state sequence

$$\phi = (\phi_1 \phi_2 \ldots \phi_N), \ \ \phi_i \in \{|0>, |1>\} \tag{8}$$

Next KMC produces a new state sequence ϕ^R from ϕ and R according the following rule.

Transform Rule:

If $R_i = 0$, $\phi_i^R = \phi_i$; if R_i=1, $\phi_i^R = \sigma_x \phi_i$.

In the Transform Rule σ_x is the NOT operation on a sing-particle quantuam state and we have

$$\sigma_x|0>=|1>, \ \ \sigma_x|1>=|0>. \tag{9}$$

Then KMC sends ϕ^R through the public classical channel to Alice. So Alice gets both S and ϕ^R. Next Alice performs the same operation with ϕ^R and R according the Transform Rule to get a new state sequence ϕ^T. That is to say,

If $R_i = 0$, $\phi_i^T = \phi_i^R$; if R_i=1, $\phi_i^T = \sigma_x \phi_i^R$.

It's easy to find that

$$\phi^T = \phi. \tag{10}$$

Now Alice has KMC's measuremnets result sequence ϕ and the state sequence φ. She can deduce Bob's measurement result sequence ξ according Table 1.

Decoding Rule:

If KMC's measurement result ϕ_i is $|0>$ and the state φ_i is $|\Phi^+>$, Bob's measurement result ξ_i is $|0>$;
If KMC's measurement result ϕ_i is $|1>$ and the state φ_i is $|\Phi^+>$, Bob's measurement result ξ_i is $|1>$;
If KMC's measurement result ϕ_i is $|0>$ and the state φ_i is $|\Psi^+>$, Bob's measurement result ξ_i is $|1>$;
If KMC's measurement result ϕ_i is $|1>$ and the state φ_i is $|\Psi^+>$, Bob's measurement result ξ_i is $|0>$.

The reason process can be summarized as the following Table 2.

Table 2. Decoding rule

ϕ_i	φ_i	ξ_i
$\|0>$	$\|\Phi^+>$	$\|0>$
$\|1>$	$\|\Phi^+>$	$\|1>$
$\|0>$	$\|\Psi^+>$	$\|1>$
$\|1>$	$\|\Psi^+>$	$\|0>$

Next Alice gets Bob's string m from ξ according to the coding rule just as Bob. Finally Alice does an XOR operation on S and m. She have

$$P' = S \oplus m = P \oplus m \oplus m = P. \tag{11}$$

Therefore Alice acquires the secret message which Bob sends her. In section 4 it will be proved that any eavesdropper can't obtain the message. So Alice and Bob complete a secure communication process. On the contrary, when Alice wants to have Bob to receive a secret message, what they need to do is to swap places in the communication process.

We can design a quantum publc-key cryptosystem built on the basis of the idea above. The public key for a user isn't a group of quantum systems but only a piece of classical information. So KMC needn't quantum storage which can save quantum sytems for a long time to keep public keys. It greatly reduce the technical difficulty to establish the quantum public-key crytposystems. In the communication process every user need only receive qubits from KMC. Any two users doesn't need to send qubits to others or recive qubits from others so that they needn't quantum channel to connect with each other. The cryptosystem has lower resource consumption. Therefore it's much easier to be applied in reality.

3. Quantum public-key cryptosystem without quantum storage

Here let's introduce this quantum public-key cryptosystem. In the cryptosystem there are a number of users and a KMC. Like in classical public-key cryptosytems, such as Rivest-Shamir-Adleman (RSA) system or Elliptic Curve Cryptography (ECC) system, KMC serves as the core rule of this quantum public-key cryptosystem. It not only keeps users' keys but also joins in the communication processes. There is a public classical channel through which everyone can send and receive classical information. But it's authenticated so that everyone can't impersonate other one. At the same time there is an insecure quantum channel through which KMC can send qubits to every user. Every user creates a state sequence

$$\varphi = (\varphi_1 \varphi_2 \ldots \varphi_N), \;\; \varphi_i \in \{|\Phi^+>, |\Psi^+>\} \tag{12}$$

and a random binary string

$$R = (R_1 R_2 \ldots R_N), \;\; R_i \in \{0, 1\}. \tag{13}$$

$< \varphi, R >$ is clalled the source key of the user. Then the user and KMC share the resource key while they keep it absolute secret in order to prevent any third one from getting it. The source key can be produced and kept using the same produre like the private key in classical public-key cryptosystem, for example RSA cryptosystem.

Let's assume the two users are Alice and Bob. When Bob intends to transfer Alice a secret message, he first informs KMC. Then KMC creates N two-qubit systems according to φ. They are the (public key, private key) pair of Alice. All the first qubit of every two-qubit system consist of a qubit sequence d which is called Alice's privtae key. At the same time all the second qubit of every two-qubit systems consist of a qubit sequence e which is called Alice's public key. They will be used to encrypt and decrypt message. It must be pointed that Alice's (public key, private key) pair is created only when other user, for example Bob, wants to send her a secret message. Furthermore Alice's (public key, private key) pair is consumed after the secret communication process. So unlike most of the previous quantum public-key cryptosystems, our quantum public-key cryptosystem doesn't require KMC to maintain quantum storage for users' public keys for a relative long time.

3.1 *Secret communication process*

Without losing generality, the secret message which Bob wants to send Alice is denoted as n-bit binary string P. Alice and Bob perform the following process.

Step 1: Bob dispatches a notice to KMC through the classical channel declaring that he intends to transfer a secret n-bit string to Alice.

Step 2: KMC creates N two-qubit systems according to Alice's source key φ as Alice's (public key, private key) pair. KMC keeps the qubit sequence consistiong of the first qubit of every two-qubit system which is called Alice's public key e. The qubit sequence consistiong of the second qubit of every two-qubit system is called Alice's public key e. Next KMC sends e to Bob by the quantum channel.

Step 3 (error-checking): After Bob receives the qubit sequence e, KMC and Bob mutually select k two-qubit systems at random in which $k = N - n$. To each two-qubit system of the k two-qubit systems KMC and Bob mutually choose a measure basis $\{|0>, |1>\}$ or $\{|+>, |->\}$ at random and measure the qubit at hands respectively. Afterwards Bob announces his measurement results through the classical channel. Now KMC have both its measurement results and Bob's measurement results. At the same time KMC also holds Alice's source key $<\varphi, R>$. If there are no errors in transmission or eavesdroppers exsting, KMC's measurement results, Bob's measurement results and φ must satify Table 1 in section 2. So KMC can compare its measurement results and Bob's measurement results with φ according to Table 1. If there are too many disagreements, KMC is sure that communication process is insecure. So KMC and Bob terminate the commucation process. They switch back to step 1. Or they continue to perform step 4.

Step 4: Bob measures the left n qubits of e in basis $\{|0>, |1>\}$ while KMC measures the left qubits of d in basis $\{|0>, |1>\}$. Bob writes down his measurement results as a state squence ξ and KMC records its measurement results as a state sequence ϕ. On the other hand KMC throws the corresponding k bits in R. Finally it gets a new n-bit string $R1$. It also throws the corresponding states which are used in error-cheking from φ to get a new state sequence $\varphi 1$. KMC also informs Alice asking she to do the same things. So Alice also gets the string $R1$ and the state squence $\varphi 1$.

Step 5: Bob performs on ξ according to Coding Rule. Then he has an n-bit string m. Then Bob performs an XOR operation on m and the message P. Next Bob has a n-binary string $S = P \oplus m$. Finally Bob transfers S to Alice by the classical channel.

Step 6: After getting S, Alice informs KMC through the classical channel and ask KMC's help.

Step 7: KMC performs on ϕ and $R1$ according to Transform Rule to get a new state sequence ϕ^{R1}. Then KMC declares ϕ^{R1} through the classical channel.

Step 8: Alice performs on ϕ^{R1} and $R1$ according to Transform Rule when she receives ϕ^{R1}. Then Alice gets a new string ϕ^T which is easy to prove that $\phi^T = \phi$. So Alice can deduce ξ from ϕ and $\varphi 1$ according to Table 2. Next Alice performs on ξ according to Coding Rule to gets m just as Bob. Finally Alice does an XOR operation on S and m. So she has $P' = S \oplus m = P \oplus m \oplus m = P$. Now Alice have acquired P. It's just the secret message that Bob transfers to Alice.

When Alice needs to transfer a secret message to Bob, Alice and Bob only need to switch roles in the communication process. So in this public-cryptosystem users can accomplish secret communication with KMC's assistance.

3.2 *Message authentication*

Except confidentiality of the message, people usually hope that the message is authenticated so that the receiver can affirm the veracity and integrity of the message. In this cryptoystem Bob is able to perform message authentication on the message which he sends Alice. When Alice receives the authenticated message, she can verify the authentication. If the authentication is verified, Alice is sure that the message is really from Bob. At the same time she also assures that the message hasn't been distorted in transmission.

3.2.1 *Authentication process*

Befor Bob transmits the secret message P to Alice, he creates an authenticator from the message by his private key and adds it to the message. Like in classical cryptosystems, the authenticator is not produced from P but from the abstract of P which is generated by a information-theoretic secure hash algotithm. In this crytosystem users use SHA256 algorithm which is widely applied in message authentication and digital signature. To accomplish message authentication, Bob and Alice perform the following process.

Step 1: Bob applies SHA256 algorithm to the message P and gets its abstract. Then Bob has an $n1$-bit string AP.

Step 2: Bob informs KMC asking it to help to perform message authentication through the classical channel.

Step 3: KMC creates N two-qubit systems accroding to Bob's source key $< \varphi, R >$. The qubit sequence which consists of the first qubit of each two-qubit system is denoted as Bob's private key d while the qubit sequence which consists of the second qubit of each two-qubit system is denoted as Bob's public key e. Then KMC sends d to Bob through the insecure quantum channel.

Step 4 (error-checking): After Bob receives the qubit sequence d, KMC and Bob mutually choose $k1$ two-qubit systems at random in which $k1 = N - n - n1$. To each two-qubit system KMC and Bob mutaully choose a measure basis $\{|0>, |1>\}$ or $\{|+>, |->\}$ at random and measure the qubit at hands respectively. Next Bob announces all the measurement results by the classical channel. Now KMC has its measurement results, Bob's measurement results. At the same time KMC also has Bob's source key $< \varphi, R >$. If there are no errors in transmission or eavesdroppers exsting, KMC's measurement results, φ and Bob's measurement results must satify Table 1 in section 2. So KMC can compare its results and Bob's results with φ according to Table 1. If there are too many disagreements, KMC is sure that communication process fails. So KMC and Bob stop the communication. They go back to step 1. Or they continue and perform step 5.

Step 5: Bob measures the left k qubits of d in basis $\{|0>, |1>\}$ while KMC measures the left k qubits of e in basis $\{|0>, |1>\}$. Bob writes down his measurement results as a state squence ξ and KMC records its measurement results as a state sequence χ. At the same time KMC and Bob also keeps the $n1$ corresponding states in φ. It's denoted as a new state sequence $\varphi 1$.

Step 6: Bob applies Coding Rule to ξ and obtains an $n1$-bit string m. Then Bob does an XOR opertion on AP and m. As a result he has $SAP = AP \oplus m$. It's just the authenticator of the message P. At the same time KMC can deduce ξ from χ and $\varphi 1$ according to Decoding Rule. So KMC also applies Coding Rule to ξ. Finally KMC obtains m, two.

Step 7: Bob adds SAP to P to get a string PS. So PS is just the plain text which Bob sends Alice in the secret communication process of section 3.1.

Now Bob sends PS to Alice according to the secret communication process of section 3.1.

It is necessary to notice that the PS must be an n-bit string. So P must contain $n - n1$ bits. If P doesn't conform to it, what Bob need do is to divide P into a few pieces or add some bits to P to satisfy the requirement.

3.2.2 *Verification process*

After receiving PS, Alice and KMC performs the following process to acomplish verification.

Step 1: Alice draws P and SAP from PS. Then Alice asks KMC for m.

Step 2: KMC sends m to Alice through the classical channel.

Step 3: Alice applies SHA256 algorithm to P to get the abstract AP'.

Step 4: Alice does an XOR operation on AP' and m. Then Alice obtains $SAP' = AP' \oplus m$. If $SAP' = SAP$, the authencation is verified. Alice affirms that the message is surely from Bob. Moreover the message is undistorted. Or the verification is unsuccessful. Alice will refuse to accept the message.

4. Security of the communication process

In this public-key cryptosystem two users can realize secret communication and message authentication. The proof is given as follows.

4.1 *Confidentiality of the communication process*

An eavesdropper named Eve wants to get the secret message P when Bob sends it to Alice. Eve can listen to both the classical channel and the quantum channel, trying to obtain P.

First Eve can get the cipher text S when Bob sends it to Alice. Eve also can obtain the state sequence ϕ^{R1} which KMC declared it. But Eve doesn't hold $R1$. Therefore she is unable to deduce ϕ from ϕ^{R1}. Therefore Eve doesn't hold φ^{R1}, either. So Eve has no way to deduce Bob's measurement result sequence ξ just as Alice does. As a result Eve is

unable to get m from ξ. Whatever Eve may do, the probabilityfor her to obtain one bit in P by S and ϕ^{R1} is no more than $\frac{1}{2}$. So the probablity for her to get P is at most

$$p\_E = \left(\frac{1}{2}\right)^n. \tag{14}$$

If n is equal to 1,000,

$$p\_E = \left(\frac{1}{2}\right)^{1,000} \approx (10)^{-300}. \tag{15}$$

It's an extremely small probablity. In fact Eve is unable to get P.

Second Eve can catch e when KMC sends it to Bob. But she can't measure the qubits in e because they contain no information about P. Moreover if Eve measures the qubits in e, they will collapse into state $|0>$ or $|1>$ at random. The entangled two-qubit systems lose entanglement. Bob and KMC will perform error-checking in step 3 of section 3.1. They choose out k two-qubit systems at random. Next KMC and Bob measure the qubits respectively in basis $\{|0>, |1>\}$ or $\{|+>, |->\}$ at random. Both KMC and Bob will get measurement results $|0>, |1>, |+>$ or $|->$ at random. As known no correlations exsit between KMC's and Bob's measurement results. Then KMC compares its measurement result and Bob's measurement results with φ according to Table 1. Therefore to one two-qubit sysytem the probability for KMC and Bob to get the same results is no more than $\frac{1}{2}$. So the probability for Bob and KMC to obtain the same results to all the two-qubit sysytems for error-checking is

$$p_1\_E = \left(\frac{1}{2}\right)^k. \tag{16}$$

If $k = 100$,

$$p_1\_E = \left(\frac{1}{2}\right)^{100} \approx (10)^{-30}. \tag{17}$$

The probability can be negligible in practice. So Eve will be undoubtedly found. Her attack is invalid.

Third Eve may perform entangment attack on the qubits from KMC to Bob. As known the two-qubit system in the (public key, private) pair is in the state

$$|\Phi^+> = \frac{1}{\sqrt{2}}(|0>_1 |0>_2 + |1>_1 |1>_2) \tag{18}$$

or

$$|\Psi^+> = \frac{1}{\sqrt{2}}(|0>_1 |1>_2 + |1>_1 |0>_2). \tag{19}$$

When KMC sends the qubit sequence e which consists of qubit 2 of each two-qubit system to Bob, Eve catches e. To each qubit in e, Eve creates an auxiliary qubit. It is denoted as qubit E. Then Eve does a controlled-NOT (CNOT) operation on qubit 2 and qubit E in which the former is the control qubit and the latter is the target qubit. Now the whole three-qubit system's state is

$$\begin{aligned} |S>&=\frac{1}{\sqrt{2}}(|0>_1|0>_2|0>_E+|1>_1|1>_2|1>_E)\\ &=\frac{1}{2\sqrt{2}}[|+>_1(|+>_2|+>_E+|->_2|->_E)+|->_1(|+>_2|->_E+|->_2|+>_E)] \end{aligned} \tag{20}$$

or

$$\begin{aligned} |SS>&=\frac{1}{\sqrt{2}}(|0>_1|1>_2|1>_E+|1>_1|0>_2|0>_E)\\ &=\frac{1}{2\sqrt{2}}[|+>_1(|+>_2|+>_E+|->_2|->_E)-|->_1(|+>_2|->_2+|->_1|+>_E)]. \end{aligned} \tag{21}$$

When KMC and Bob performs error-checking, they choose k two-qubit systems at random. Then KMC and Bob respectively measure the qubits at his hands in basis $\{|0>,|1>\}$ or $\{|+>,|->\}$ at random. To each two-qubit systems the measurement results are summarized as the following Table 3.

Table 3. Measurement results with Eve's existence

φ_i	Three-qubit system's state	Measurement basis	KMC's result	Bob's result	Results relations
$\|\Phi^+>$	S	$\{\|0>,\|1>\}$	$\|0>$	$\|0>$	Identical
$\|\Phi^+>$	S	$\{\|0>,\|1>\}$	$\|1>$	$\|1>$	Identical
$\|\Phi^+>$	S	$\{\|+>,\|->\}$	$\|+>$	$\|+>$ or $\|->$	Uncertain
$\|\Phi^+>$	S	$\{\|+>,\|->\}$	$\|->$	$\|+>$ or $\|->$	Uncertain
$\|\Psi^+>$	SS	$\{\|0>,\|1>\}$	$\|0>$	$\|1>$	Contrary
$\|\Psi^+>$	SS	$\{\|0>,\|1>\}$	$\|1>$	$\|0>$	Contrary
$\|\Psi^+>$	SS	$\{\|+>,\|->\}$	$\|+>$	$\|+>$ or $\|->$	Unsertain
$\|\Psi^+>$	SS	$\{\|+>,\|->\}$	$\|->$	$\|+>$ or $\|->$	Uncertain

So KMC will find that Bob's measurement results aren't always consistent with what he deduces by φ and its measurement results according to Table 1. From Table 3 we can get that to one two-qubit sysytem the average probability for KMC and Bob to get consistent results is $\frac{3}{4}$. To all k two-qubit systems for error-checking the average probability is no more than

$$p_{2\_}E=\left(\frac{3}{4}\right)^k. \tag{22}$$

If $k=100$,

$$p_2\_E = \left(\frac{3}{4}\right)^{100} \approx (10)^{-13}. \tag{23}$$

Therefore entangmemt attack is also impossible to succeed.

At lat Bob may find ways and means to obtain some information (named leaked information) about Alice's source key in the communication process. Moreover he may hope to get Alice's source key by communicating with Alice for many times by accumulating the leaked information. If Bob can succeed, this quantum public-key cryptosystem is insecure. We prove that it's impossible as follows. When Bob gets e from KMC, he and KMC perform error-checking. Finally Bob gets measurement result sequence ξ. As known the measurement result of a qubit which is part in a entangled two-qubit system is random. So ξ is a random state quence which contains no inforamtion about φ of Alice's source key. In fact Bob can deduce $\varphi 1$ accroding Table 1 if he gets KMC's measurem result sequence ϕ. But KMC keeps ϕ secret. Bob can't get it. Next KMC declares ϕ^{R1} through the channel and Bob gets it. But ϕ^{R1} is produced by KMC in step 7 of the secret communication process, in which KMC performs Transform Rule on ϕ and $R1$. If Bob has $R1$, he can deduce ϕ by $R1$ and ϕ^{R1} just as Alice does. But $R1$ is also kept absolutely secret by KMC and Alice. So Bob can get nothing from ξ and ϕ^{R1}. That is to say, Bob is unable to get any information about Alice's source key in a secret communicaton process. Alice's source key is secure.

Now the security of the communication process is proved.

4.2 *Security of the message authentication*

Bob can accomplish message authentication on the message which he sends to Alice. No one can forge the message. On the other hand, if there is somthing wrong with the meaasge in transmission, Alice can find it at once.

In the message authentication process, Bob gets his string m by measuring the qubits which KMC sends him. Bob can affirm that these qubits are really from Alice and they haven't be tampered with after the error-checking process of the step 4 in section 3.2.1. Since Bob's qubits are entangled with KMC's qubits, there are correlations between Bob's measurement results and KMC's measurement results. So KMC can decuce Bob's measurement results by its measurement results and $\varphi 1$. If Eve intends to have Alice to receive a message pretending to be from Bob, she has to produce an authenticator of his message acccording to the authentication process in section 3.2.1. Then she informs KMC through the classical channel asking for Bob's private key d. But as this quantum public-key cryptosystem requires, the classical channel is authenticated. Therefore KMC will find that the one on the other side isn't Bob at once. Then KMC declines to begin the comunication process. So Eve fails.

Second Eve may forge a signed message. Next she transfers the fake message to Alice directly. When Alice gets it, Alice needs to verify the authentication. So she asks KMC for help her to finish the verification process in section 3.2.2. But KMC hasn't received Bob's requirement for perform message authentication. That is to say, KMC finds that Alice gets a fake message. So KMC tells Alice right away. Finally Alice declines to accept the fake message. Eve's attack fails.

Third let's assume that the message which Bob sends Alice is changed by channel noises or some eavedroopers in transmission. Without losing generality, the distorted message is denoted as P_e. According to the verification process in section 3.2.2, when Alice receives PS, she extracts P_e and SAP. Then Alice ask KMC and gets m. Next Alice applies SHA256 algorithm to P_e. So she obtains the abstract AP_e. Alice does an XOR operation on AP_e and m. Finaly Alice gets

$$SAP_e = AP_e \oplus m. \tag{24}$$

Since $Pe \neq P$, according to the property of SHA256 algorithm, it's obvious that

$$AP_e \neq AP. \tag{25}$$

Then from

$$SAP = AP \oplus m, \;\; SAP_e = AP_e \oplus m \tag{26}$$

we have

$$SAP_e \neq SAP. \tag{27}$$

When Alice compares SAP_e and SAP according to the step 4 of scetion 3.2.2, she will find that they are unequal. So the verification fails. Alice is sure to find that the message is distorted by noises or possible eavesdroppers.

5. Analysis for the public-key cryptosystem

5.1 *Feasibility and advantages*

To finish secret communication, all that users and KMC have to do is producing entangled two-qubit systems, performing single-particle measurement, exchaging classical information through a classical channel and exchanging qubit through a quantum channel. These technologies were carried out in practice tens of year ago. So no big obstacles prevent this cryptosystem from being carried out. It can be fulfill by today's technology.

According to quantum mechanics quantum systems is doomed to undergo decoherence with time, which makes quantum systems to degenerate to classical system. Or in other words all quantum cryptographic protocols will lose effectiveness after decoherence occurs. In tranditional quantum public-key cryptosystems, KMC has to keep users' public keys for a relative long time. It's very difficult and expensive. In this quantum public-key cryptosystem, KMC only needs to storage the source key for every user which consists of some classical information. Only when a user wants to send a secret message to another user, KMC creats the latter one's (public key, private key) pair which consists of a group of two-qubit system. So both KMC and the user needn't keep the public key and private key for a relative long time to wait for another user's commnication request like that in most previous quantum public-key cryptosystems. That is to say, both KMC and the user needn't have to keep quantum systems in a quantum storage for a relative long time. So the technical difficulties and management cost of this quantum public-key cryptosystem are much less than the quantum public-key cryptosystems before. It's a big advantage of this cryptosystem.

There is another advantage of our cryptosystem. Every user doesn't need to send qubits to other users or receive qubits from other users. So any two users needn't keep a quantum channel connecting them. Only a communal quantum channel is needed through which any user can exchange qubit with KMC. To sustain this communal quantum channel requires much lower expense than to sustain $N(N-1)/2$ quantum channels connecting any two users, which makes this cryptosystem easier to be applied in business and military affairs.

5.2 *Comparasion with existing quantum public-key cryptosystems*

Now a comparision between this public-key crytposystem and exisisting quantum public-key cryptosystems is given as follows. It's in the Table 4.

Table 4. Comparasion with main existing quantum public-key cryptosystems

Cryptosystem	Based on	Using entanggled states	Security	Quantum storage for public keys
Nikolopoulos [24]	Single-particle rotation	No	Secure	Required
Vlachou [29]	Quantum walk	No	Secure	Required
Yang [31]	Quantum conjugate coding	No	Secure	Required
Zhang [33]	Quantum teleportation	Yes	Secure	Required
Fu [40]	Correlations in entangled state	Yes	Secure	Required
This cryptosystem	Correlations in entangled state	Yes	Secure	Not required

It's easy to find that this public-key cryptosystem has the same security as quantum public-key cryptosystems before. But it's superior to the latter ones because it doesn't need quantum storage for public keys so that the key management cost and technical difficulites are significantly reduced.

6. Conclusion

In this paper a quantum public-key cryptosystem without storage for public keys is provided. Uers and KMC share some classical information as the source key. KMC will creates a user's (public key, private key) pair when another other wants to send him or her a secret message. Then any two users can realize secret communication with the assistance of KMC. KMC needn't maintain a long-term quantum storage to store quantum systems which serve as the public key. It greatly reduces the technical difficulties and management costs. Moreover any two users needn't maintain a quantum channel between them. Therefore it's easier for this quantum public-key cryptosystem to be carreid out in laboratory and be applied in reality than thoese previous ones.

Acknowledgement

This research is supported by Natural Science Foundation of China (Grants 62371423). 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 tossing. In: *Proceedings of IEEE International conference on Computers, Systems and Signal Processing*. Bangalore, India: IEEE; 1984. p.175-179.

[2] Ekert AK. Quantum cryptography based on Bell's theorem. *Physical Review Letters*. 1991; 67(6): 661-663. Available from: https://doi.org/10.1103/PhysRevLett.67.661.

[3] Bennett CH, Brassard G, Mermin ND. Quantum cryptography without Bell's theorem. *Physical Review Letters*. 1992; 68(5): 557-559. Available from: https://doi.org/10.1103/PhysRevLett.68.557.

[4] Zhao Y, Qi B, Lo HK. Quantum key distribution with an unknown and untrusted source. *Physical Review A*. 2008; 77(5): 052327. Available from: https://doi.org/10.1103/PhysRevA.77.052327.

[5] 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 Transaction on Information Theory*. 2008; 54(6): 2604-2620. Available from: https://doi.org/10.1109/TIT.2008.921870.

[6] Boyer M, Gelles R, Kenigsberg D, Mor T. Semi-qantum key distribution. *Physical Review A*. 2009; 79(3): 032341. Available from: https://doi.org/10.1103/PhysRevA.79.032341.

[7] Ye TY, LI HK, Hu JL. Semi-quantum key distribution with single photons in both polarization and spatial-mode degrees of freedom. *International Journal of Theoretical Physics*. 2020; 59(9): 2807-2815. Available from: https://doi.org/10.1007/s10773-020-04540-y.

[8] Hajji H, Baz ME. Mutually unbiased bases in 3 and 4 dimensions semi-quantum key distribution protocol. *Physics Letters A*. 2022; 426: 127884. Available from: https://doi.org/10.1016/j.physleta.2021.127884.

[9] Krawec WO. Mediated semi-quantum key distribution. *Physical Review A*. 2015; 91: 032323. Available from: https://doi.org/10.1103/PhysRevA.91.032323.

[10] Tsai CW, Yang CW. Lightweight mediated semi-quantum key distribution protocol with a dishonest third party based on Bell states. *Scientific Reports*. 2021; 11: 23222. Available from: https://doi.org/10.1038/s41598-021-02614-3.

[11] Aguilar EA, Ramanathan R, Kofler J, Pawlowski M. Completely device independent quantum key distribution. *Physical Review A*. 2016; 94(2): 022305. Available from: https://doi.org/10.1103/PhysRevA.94.022305.

[12] Zhen YZ, Mao Y, Zhang YZ, Xu F, Sanders BC. Device-independent quantum key distribution based on the Mermin-Peres magic square game. *Physical Review Letters*. 2023; 131: 080801. Available from: https://doi.org/10.1103/PhysRevLett.131.080801.

[13] Yang H, Liu S, Yang S, Lu Z, Li Y, Li Y. High-efficiency rate-adaptive reconciliation in continuous-variable quantum key distribution. *Physical Review A*. 2024; 109: 012604. Available from: https://doi.org/10.1103/PhysRevA.109.012604.

[14] Zhang CM, Wang Z, Wu YD, Zhu JR, Wang R, Li HW. Discrete-phase-randomized twin-field quantum key distribution with advantage distillation. *Physical Review A*. 2024; 109(5): 052432. Available from: https://doi.org/10.1103/PhysRevA.109.052432.

[15] Zhang Y, Zhao H, Wu T, Gao Z, Ge L, Feng L. High-dimensional quantum key distribution by a spin-orbit microlaser. *Physical Review X*. 2025; 15: 011024. Available from: https://doi.org/10.1103/PhysRevX.15.011024.

[16] Zhang H, Li W, He R, Zhang Y, Xu F, Gao W. Noise-reducing quantum key distribution. *Reports on Progress in Physics*. 2025; 88: 016001. Available from: https://doi.org/10.1088/1361-6633/ad9505.

[17] Bennett CH, Bessette F, Brassard G, Salvail L, Smolin J. Experimental quantum cryptography. *Journal of Cryptology*. 1992; 5(1): 3-28. Available from: https://doi.org/10.1007/BF00191318.

[18] Yin HL, Chen TY, Yu ZW, Liu H, You LX, Zhou YH, et al. Measurement device independent quantum key distribution over 404 km optical fibre. *Physical Review Letters*. 2016; 117: 190501. Available from: https://doi.org/10.1103/PhysRevLett.117.190501.

[19] 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. Available from: https://doi.org/10.1103/PhysRevLett.81.3283.

[20] Liao SK, Cai WQ, Liu WY, Zhang L, Li Y, Ren JG, et al. Satellite-to-ground quantum key distribution. *Nature*. 2017; 549: 43-47. Available from: https://doi.org/10.1038/nature23655.

[21] Rivest R, Sharmir A, Adleman L. A method for obstaining digital signature and public-key cryptosystem. *Communications of ACM*. 1978; 21(2): 120-126. Available from: https://doi.org/10.1145/359340.359342.

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

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

[24] Nikolopoulos G. Applications of single-qubit rotations in quantum public-key cryptography. *Physical Review A*. 2008; 77(3): 032348. Available from: https://doi.org/10.1103/PhysRevA.77.032348.

[25] Nikolopoulos G, Ioannou L. Deterministic quantum-public-key encryption: Forward search attack and randomization. *Physical Review A*. 2009; 79(4): 042327. Available from: https://doi.org/10.1103/PhysRevA.79.042327.

[26] Ioannou L, Mosca M. Public-key cryptography based on bounded quantum reference frames. *Theoretical Computer Science*. 2014; 560: 33-45. Available from: https://doi.org/10.1016/j.tcs.2014.09.016.

[27] Luo MX, Chen XB, Yun D, Yang YX. Quantum public-key cryptosystem. *International Journal of Theoretical Physics*. 2012; 51(3): 912-924.

[28] 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. Available from: https://doi.org/10.1103/PhysRevA.85.022342.

[29] Vlachou C, Rodrigues J, Mateus P. Quantum walk public-key cryptographic system. *International Journal of Quantum Information*. 2015; 13(7): 1550050. Available from: https://doi.org/10.1142/S0219749915500501.

[30] Wu WQ, Cai QY, Zhang HG, Liang XY. Quantum public key cryptosystem based on Bell states. *International Journal of Theoretical Physics*. 2017; 56: 3431-3440. Available from: https://doi.org/10.1007/s10773-017-3506-4.

[31] Yang L, Yang BY, Xiang C. Quantum public-key encryption schemes based on conjugate coding. *Quantum Information Processing*. 2020; 19: 415. Available from: https://doi.org/10.1007/s11128-020-02912-1.

[32] Liu ZX, Xie QL, Zha YF, Dong FM. Quantum public key encryption scheme with four states key. *Physica Scripta*. 2022; 97: 045102. Available from: https://doi.org/10.1088/1402-4896/ac576c.

[33] Zhang DX, Li XY. 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. Available from: https://doi.org/10.1007/s10773-022-05093-y.

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

[35] Wang Y, Chen G, Jian L. Ternary quantum public-key cryptography based on qubit rotation. *Quantum Information Processing*. 2022; 21(6): 197. Available from: https://doi.org/10.1007/s11128-022-03541-6.

[36] Barooti K, Grilo AB, Huguenin-Dumittan L, Malavolta G, Sattath O, Vu Q, et al. Public-key encryption with quantum keys. In: *21st International Conference on Theory of Cryptography*. Taipei, Taiwan; 2023. p.198-227.

[37] 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. Available from: https://doi.org/10.1007/s13538-024-01537-4.

[38] Kitagawa F, Morimae T, Nishimaki R, Yamakawa T. Quantum public-key encryption with tamper-resilient public keys from one-way functions. In: *44th Annual International Cryptology Conference on Advances in Cryptology*. Santa Barbara, US; 2024. p.93-125.

[39] Malavolta G, Walter M. Robust quantum public-key encryption with applications to quantum key distribution. In: *44th Annual International Cryptology Conference on Advances in Cryptology*. Santa Barbara, US; 2024. p.126-151.

[40] Fu XQ, Li HW, Shi JH, Li T, Bao WS. Quantum public-key crypto via EPR pairs. *Science China-Physics Mechanics & Astronomy*. 2025; 68(1): 210314. Available from: https://doi.org/10.1007/s11433-024-2510-x.

[41] Li XY, Chen YL. Quantum public-key cryptosystem using orthogonal product states with high channel capacity. *Contemporary Mathematics*. 2025; 6(2): 1455-1467. Available from: https://doi.org/10.37256/cm.6220256333.