Quantum Public-Key Cryptosystem with Reusable (Public Key Privtate Key) Pair Using the Bell States

Xiaoyu Li * and Yue Zhou

Posted Date: 2 July 2025

doi: 10.20944/preprints202507.0137.v1

Keywords: quantum public key cryptosystem; entangled states; the Bell states; reusable (public key, private key) pair; management expenses; security

 doi:10.20944/preprints202507.0137.v1

Article

Quantum Public-Key Cryptosystem with Reusable (Public Key Privtate Key) Pair Using the Bell States

Xiaoyu Li * and Yue Zhou

School of Computer and Artificial Intelligence, Zhengzhou University, Kexue Road 100, Zhengzhou City, P. R. China
* Correspondence: iexyli@zzu.edu.cn

Abstract

In most of the traditional quantum public-key cryptosystems the public key held by the key management center (KMC) is a group of quantum systems. The public key will be destroyed after a secret communication process. So users must reconstruct the public key with KMC after every communication process or keep many copies of public key in the beginning. It's an obstacle for the quantum cryptosystem to apply in practice. A quantum public-key cryptosystem with reusable (public key privtate key) pair using the bell states is provided in this paper. Every user shares a set of entangled quantum systems in the Bell states with KMC as his or her (public key, private key) pair. Two users can acomplish secret comminications by the help of KMC. Moreover the states of the quantum systems turn back to their original states. The user's (public key, private key) pair is unchanged so that they are reusable. It's unnecessary for users to reconstruct the public key with KMC or save many copies of public key in KMC. So this public-key cryptosystem is of much lower management expenses. It's easier to realized in practice than most of traditional quantum public-key cryptosystems.

Keywords: quantum public key cryptosystem; entangled states; the Bell states; reusable; (public key, private key) pair; management expenses; security

1. Introduction

Quantum cryptography is a very active fields of quantum information science. As known classical cryptographic protocls are based on Computational Complexity. But quantum cryptographic protocols are based on the properties of quantum systems. Their securities are guaranteed by the principles of quantum mechanics. So quantum cryptographic protocols can show unconditionally security. It is a big advantage in relative to classical cryptographic protocls. In 1984 Bennett and Brassard provided the first quantum key distribution protocol [1] which is called BB84 protocol. Thereafter many QKD schemes were developed [2–12]. QKD schemes have also been realized in laboratory. Bennett et al first carried out BB84 procotol in 1992 [13]. Now people have completed QKD experiment in optical fibre over 400 kilometers [14] and QKD experiment over 1 kilometer in free space [15]. In 2017 researchers even finished QKD between Micius satellite and the earth station in which the transmission distance is beyond 1200 kilometers [16].

In tranditional cryptosystems any two users need to share a secret string named the key before they begin to communicate with each other. If there are a large number of users, it's very difficult and expensive for a user to build and manage all the keys with every other user. Rivest, Sharmir and Adleman provided the first public-key algorithm in 1978 which can solve this problem [17]. This public-key algorithm is called RSA algorithm on which people can establish a public-key cryptosystem. In public-key cryptosystems, every user has only a (public key, private key) pair. A user's public key can be open to everyone and his or her private key is kept absolutly secret. Obviously it greatly cut down the difficulty and management expense for key management. Today public-key cryptosystems are widely applied in modern society to safeguard information security and privacy. However Shore presented a quantum algorithm which can crack RSA algorithm on future quantum computers [18].

 doi:10.20944/preprints202507.0137.v1

Now people have found quantum algorithms to most of classical public-key algorithms so that they are all insecure once quantum computers come to being. Quantum public-key algorithms may be used to solve this problem. In 2001 Gottesman and Chuang constructed a quantum one-way function and proposed that a quantum public-key cryptosystem may be realized based on quantum one-way functions [19]. Nikolopoulos presented the first quantum public-key algorithm [20] in 2008. After that researchers issued many quantum public-key cryptosystem schemes [21–38].

It's known quantum public-key cryptosystems are based on the special properties of quantum systems. Usually a user's public key is a group of quantum systems. But these quantum systems will be consumped after a secret communication process finishes. Their states will irreversibly change. That is to say, the public key no longer exsist. So every user has to restruct their (public key, private key) after the communication process and keep the public key in KMC. Another solution is that every user keeps many copies of his or her public key in KMC. Obviously it brings huge management expense to the quantum public-key cryptosystems.

A quantum public-key cryptosystem with resusable public key based on the Bell states is presented in this paper. Every user creates a group of two-particle quantum system as his or her (public key, private key) pair. The public-key is kept in KMC while the private key is hold by the user. Two users can accomplish secret communications by the help of KMC. No third party can get the secret message exchanged between the two users. After a communication process finishes, the state of the (public key, private key) pair keep unchanged. That is to say, the public key and private key can be reused. So this public-key cryptosystem needs much less management expenses for key management in relative to previous quantum publc-key cryptosystems. It's easier to carry out in practice.

2. Main Idea

A two-level quantum system is often used as the carrier of information. It's called a qubit whose state space is a 2-dimension Hilbert space. There are four states $|0>, |1>, |+>, |->$ of a qubit in which

$$\begin{aligned} |+> &= \frac{1}{\sqrt{2}}(|0> + |1>) \\ |-> &= \frac{1}{\sqrt{2}}(|0> - |1>). \end{aligned} \tag{1}$$

They form two complete orthogonal base

$$\begin{aligned} B_{01} &= \{|0>, |1>\} \\ B_{+-} &= \{|+>, |->\}. \end{aligned} \tag{2}$$

People can measure a qubit in B_{01} or B_{+-}. There are four basic quantum operations on a qubit

$$\begin{aligned} I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \ \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned} \tag{3}$$

 doi:10.20944/preprints202507.0137.v1

The Bell states are four states of a two-qubit quantum system.

$$
\begin{aligned}
|\Phi^+>&= \frac{1}{\sqrt{2}}(|00>+|11>) = \frac{1}{\sqrt{2}}(|+->+|-+>)\\
|\Phi^->&= \frac{1}{\sqrt{2}}(|00>-|11>) = \frac{1}{\sqrt{2}}(|+->-|-+>)\\
|\Psi^+>&= \frac{1}{\sqrt{2}}(|01>+|10>) = \frac{1}{\sqrt{2}}(|++>+|-->)\\
|\Psi^->&= \frac{1}{\sqrt{2}}(|01>-|10>) = \frac{1}{\sqrt{2}}(|++>-|-->).
\end{aligned} \tag{4}
$$

They form a complete orthogonal basis for a two-qubit system in which people can measure the two-qubit system. Such measurement is called the Bell measurement.

Let's assume that there is a key management center (KMC). Two users, for rexample, Alice and Bob want to communicate wtth each other by the help of KMC. There is a quantum channel and a classical channel through which everyone can use. The quantum channel is insecure which everyone can control. The classical channel is public so that everyone can listen to it. But at the same time it's authenticated so that no one can pretending to be someone else. First Alice creates n two-qubit systems in the state

$$
|\Phi^+>= \frac{1}{\sqrt{2}}(|0>_1|0>_2+|1>_1|1>_2) \tag{5}
$$

in which the subscript is used to discriminate the two qubits. Alice keeps qubit 2 of each two-qubit system in KMC while she holds qubit 1 of each two-qubit system at her hands. If Bob wants to sends a message denoted as a n-bit binary string P to Alice. He informs KMC through the classical channel. Then to qubit 2 of every two-qubit system KMC creates an auxilliary qubit denoted as qubit A in state $|0>$. To every two-qubit system KMC performs a CNOT operation on qubit 2 and the corresponding qubit A in which qubit 2 is the control qubit and qubit A is the target qubit. So the state of the whole three-qubit system turns into

$$
S = \frac{1}{\sqrt{2}}(|0>_1|0>_2|0>_A+|1>_1|1>_2|1>_A). \tag{6}
$$

Next KMC sends qubit A of every two-qubit system to Bob through the quantum channel. After receiving the qubits, Bob performs on qubit A of every two-qubit system according to the message P. To every bit P_i in P. He does in accordance with the following coding rule.

Coding rule: If P_i is "0", he perorms nothing; if the bit in P_i is "1", he performs σ_x on qubit A.

Then the state of the whole three-qubit system turn into

$$
\begin{aligned}
SS_1 &= \frac{1}{\sqrt{2}}(|0>_1|0>_2|0>_A+|1>_1|1>_2|1>_A),\ \ if\ P_i=0;\\
SS_2 &= \frac{1}{\sqrt{2}}(|0>_1|0>_2|1>_A+|1>_1|1>_2|0>_A),\ \ if\ P_i=1.
\end{aligned} \tag{7}
$$

Then Bob sends the qubits to Alice through the quantum channel. When Alce receives them, she first performs CNOT operation on qubit 1 of the two-qubit system and the corresponding qubit A in which qubit 1 is the control qubit and qubt A is the target qubit. The state of the whole three-qubit system becomes

$$
\begin{aligned}
ST_1 &= \frac{1}{\sqrt{2}}(|0>_1|0>_2|0>_A+|1>_1|1>_2|0>_A),\ \ if\ P_i=0;\\
ST_2 &= \frac{1}{\sqrt{2}}(|0>_1|0>_2|1>_A+|1>_1|1>_2|1>_A),\ \ if\ P_i=1.
\end{aligned} \tag{8}
$$

 doi:10.20944/preprints202507.0137.v1

It can be rewritten as

$$ST_1 = \frac{1}{\sqrt{2}}(|0>_1 |0>_2)| + |1>_1 |1>_2)|0>_A, \ if \ P_i = 0;$$
$$ST_2 = \frac{1}{\sqrt{2}}(|0>_1 |0>_2 | + |1>_1 |1>_2)|1>_A, \ if \ P_i = 1. \quad (9)$$

Then Alice measures qubit A in B_{01} and records as the following decoding rule.

Decoding rule: If the measurement result is |0>, she records as "'0'; If the measurement result is |1>, she records as "1".

Finally Alice get a n-bit binary string P'. It's easy to find that $P'_i = P_i$ and the state of the two-qubit system compoed of qubit 1 qnd qubit 2 turns back into

$$|\Phi^+>= \frac{1}{\sqrt{2}}(|0>_1 |0>_2 + |1>_1 |1>_2). \quad (10)$$

The proof can be summarized by the Table 1.

Table 1. Correlation between P and P'.

$State_{12}$	$State_{12A}$	P_i	$State'_{12A}$	$State''_{12A}$	P'_i	$State'_{12}$
$\|\Phi^+>$	S	0	SS_1	ST_1	0	$\|\Phi^+>$
$\|\Phi^+>$	S	1	SS_2	ST_2	1	$\|\Phi^+>$

The notions in Table 1 are denoted as:

$State_{12}$: the oringinal state of the two-qubit system composed of qubit 1 and qubit 2;

$State_{12A}$: the state of the whole three-qubit system composed of qubit 1, qubit 2 and qubit A after KMC's CONT operation;

P_i: the i-th bit in P;

$State'_{12A}$: the state of the whole three-qubit system after Bob's operation;

$State''_{12A}$: the state of the whole three-qubit system after Alice's CNOT operation;

P'_i: the corresponding i-th bit in P';

$State'_{12}$: the final state of the two-qubit system.

In section 4 we will prove that no other one can get the secret message P which Bob send Alice. So Alice and Bob finish a secret communication process. Moreover Alice's (public key, prvate key) pair keeps unchanged after the communication process. That is to say, Alice's public key and private key are reusable just like those in classical public-key crytposytem. So we can build a quantum public-key cryptosystem with reusable (public key, private key) pair based on the idea above.

3. Quantum Public-Key Cryptosystem with Resuable (Public Key, Private Key) Pair

The quantum public-key cryptosystem with reusable key is given as follws.

There are N users and a key management center (KMC). An insecure quantum channel is public to everyone. At the same time there is authenticated public classical channel which everyone can listen to it but no one can impersonate other one. Every user creates M two-qubit systems in the state

$$|\Phi^+>= \frac{1}{\sqrt{2}}(|0>_1 |0>_2 + |1>_1 |1>_2). \quad (11)$$

as his or her (public key, private key) pair in which the subscripts are used to discriminate the two qubits. To each two-qubit system the user keeps qubit 1 and gives qubit 2 to KMC. So the user holds an M-qubit sequence Q^d which is his or her private key. KMC holds an M-qubit sequence Q^e which is

 doi:10.20944/preprints202507.0137.v1

the user's public key. if a user Bob wants to send a secret message which can be denoted as an n-bit binary string P to another user Alice. They perform the following process as follows.

step 1: Alice produce k=M-n checking bits at random. Then Alice randomly inserts these bits into P. Finally she gets new string PT which is just the plain text to be transmited to Bob. The inserted qubits are used for error-checking.

step 2: Bob informs KMC through the classical channel telling KMC that he wants to send a secret message to Alice.

step 3: To each qubit in Q^e KMC creates an auxilliary qubit denoted qubit A in state $|0>$. So KMC has a M-qubit sequence denoted as Q^A. Then KMC performs CNOT operation on qubit 2 in Q^e and qubit A in Q^A in which qubit 2 is the control qubit and qubit A is the target qubit. At last KMC send the qubit sequence Q^A to Bob through the quantum channel.

step 4: After receiving Q^A, Bob encodes PT on Q^A according to the coding rule. That is to say, when the bit in PT is 0, he performs nothing and when the bit in PT is 1, he performs σ_x on the corresponding qubit in Q^A.

step 5: Bob sends Q^A to Alice through the quantum channel.

step 6: When Alice gets Q^A, she puts it together with Q^d at her hands. Then to each qubit in Q^d Alice performs CNOT operation on qubit 1 in Q^d and qubit A in Q^A in which qubit 1 is the control qubit and qubit A is the target qubit.

step 7: Alice measures all qubits in Q^A and records her meaurement results accords to the decoding rule. Then she gets a binary string PT'.

step 8(error-checking): Alice asks Bob for error-chencking through the classical channel. After receiving Alice's requirement, Bob declares all the checking bits and their positions in PT through the classical channel. Then Alice extracts the correspongding bits in PT' and compares them with Bob's checking bits. If there are too many disagreements, Alice and Bob abandon the communication process. Or they go into next step.

step 9: Alice threw all the bits for error-checking from PT' to get a new binary string P'.

It's easy to find that $P' = P$. Now Alice has obtained the message which Bob sends her. In section 4 it's proved that no third party except Alice and Bob can get the message. So Alice and Bob complete a secret communication process. Moreover the state of every two-qubit system consisting of qubit 1 and qubit 2 turns back to $|\Phi^+>$. So Alice's (public key, private key) pair can be reusable.

4. Security of the Cryptosystem

This cryptosystem is secure. Any two users can exchange secret messages by the help of KMC. No third party can gets the secret message. Let's give the proof as follows.

If an eavesdropper Eve wants to get the secret message which Bob sends to Alice, she can listen to both the classical channel and the quantum channel. First Eve may catch the qubits in Q^A when they are sent from KMC to Bob. But Bob hasn't encode his mesaage in Q^A now. If Eve measures the qubits in Q^A, she can get nothing about the message. Moreover if Eve measures them, she will crash the communication process and will be found by Alice and Bob at last. When Eve gets Q^A, the state of the each three-qubit system is

$$S = \frac{1}{\sqrt{2}}(|0>_1 |0>_2 |0>_A + |1>_1 |1>_2 |1>_A). \tag{12}$$

If Eve measures it, the state turn to

$$S' = (|0>_1 |0>_2 |0>_A \tag{13}$$

or

$$S'' = (|1>_1 |1>_2 |1>_A . \tag{14}$$

 doi:10.20944/preprints202507.0137.v1

So the three-qubit system are no longer entangled. Then Eve sends Q^A to Bob. After Bob receives Q^A, he encodes his message PT on it according to the coding rule. Then the state of the each three-qubit system is

$$\begin{aligned} S_0' &= (|0>_1 |0>_2 |0>_A, \ if\ PT_i = 0; \\ S_1' &= (|0>_1 |0>_2 |1>_A, \ if\ PT_i = 1. \end{aligned} \tag{15}$$

or

$$\begin{aligned} S_0'' &= (|1>_1 |1>_2 |1>_A, \ if\ PT_i = 0; \\ S_1'' &= (|1>_1 |1>_2 |0>_A, \ if\ PT_i = 1. \end{aligned} \tag{16}$$

Next Bob sends Q^A to Alice. After receiving Q^A, Alice performs CNOT operation the qubit A in Q^A and corresponding qubit 1 in Q^d in which the former is the target qubit and the latter is the control qubit. The state of the each three-qubit system is

$$\begin{aligned} S_0^T &= (|0>_1 |0>_2 |0>_A, \ if\ PT_i = 0; \\ S_1^T &= (|0>_1 |0>_2 |1>_A, \ if\ PT_i = 1. \end{aligned} \tag{17}$$

or

$$\begin{aligned} S_0^T &= (|1>_1 |1>_2 |0>_A, \ if\ PT_i = 0; \\ S_1^T &= (|1>_1 |1>_2 |1>_A, \ if\ PT_i = 1. \end{aligned} \tag{18}$$

Then Alice measures all the qubits in Q^A and records her measurement results according to the decoding rule. It's easy to find that Alice's measurement result is |0> or |1> with the same probability whatever $PT_i = 0$ or $PT_i = 1$. That is to say, finally the string PT' which Alice gets is a random string. So $PT' \neq PT$. Then Bob declares all the k checking bits in PT. Alice compares them with the corresponding bits in PT'. Obvious the average probability that Alice and Bob has the same value for a bit is $1/2$. So for all the k checking bits, the probability that Alice and Bob get the same value is

$$p_{error} = (\frac{1}{2})^k. \tag{19}$$

If k=100

$$p_{error} = (\frac{1}{2})^{100} \approx 10^{-30}. \tag{20}$$

It's a very small probability. So Alice and Bob are sure to found Eve's existence.

Second Eve may catch Q^A when Bob sends it to Alice. Now the state of each three-qubit system is

$$\begin{aligned} SS_0 &= \frac{1}{\sqrt{2}}(|0>_1 |0>_2 |0>_A + |1>_1 |1>_2 |1>_A), \ if\ PT_i = 0; \\ SS_1 &= \frac{1}{\sqrt{2}}(|0>_1 |0>_2 |1>_A + |1>_1 |1>_2 |0>_A), \ if\ PT_i = 1. \end{aligned} \tag{21}$$

Eve measures qubit A and records her measurement result according the decoding rule. Alice measurement result is recorded as $|\varphi>$. Then the state of the three-qubit system turns to

$$\begin{aligned} SS_{00} &= |0>_1 |0>_2 |0>_A, \ if\ PT_i = 0\ and\ |\varphi> = |0>; \\ SS_{01} &= |1>_1 |1>_2 |1>_A, \ if\ PT_i = 0\ and\ |\varphi> = |1>; \\ SS_{10} &= |1>_1 |1>_2 |0>_A, \ if\ PT_i = 1\ and\ |\varphi> = |0>; \\ SS_{10} &= |0>_1 |0>_2 |1>_A, \ if\ PT_i = 1\ and\ |\varphi> = |1>. \end{aligned} \tag{22}$$

 doi:10.20944/preprints202507.0137.v1

Obviously Eve will get measurement result $|0>$ and $|1>$ with the same probability $1/2$ whatever $PT_i = 0$ or $PT_i = 1$. So there are no correlations between PT and the string PE which Alice gets. Or in other words Eve can't get PT by such method.

Third let's consider a complex strategy of attack. Eve may implement entanglement attack. When Bob sends Q^A to Alice, Eve catches it. Then she creates an auxilliary qubit for each qubit in Q^A and performs CNOT operation on them with attention to get the message. When Eve gets Q^A, the state of the whole three-qubit system is

$$\begin{aligned} S1 &= \frac{1}{\sqrt{2}}(|0>_1 |0>_2 |0>_A + |1>_1 |1>_2 |1>_A), \ \ if\ PT_i = 0; \\ S2 &= \frac{1}{\sqrt{2}}(|0>_1 |0>_2 |1>_A + |1>_1 |1>_2 |0>_A), \ \ if\ PT_i = 1. \end{aligned} \tag{23}$$

Then Eve creats an auxilliary qubit (denoted as qubit E) in $|0>$ and performs CNOT operation on qubit A and qubit E in which the former is the target qubit and the latter is the control qubit. So the state of the four-qubit system is

$$\begin{aligned} SS1 &= \frac{1}{\sqrt{2}}(|0>_1 |0>_2 |0>_A |0>_E + |1>_1 |1>_2 |1>_A |1>_E), \ \ if\ PT_i = 0; \\ SS2 &= \frac{1}{\sqrt{2}}(|0>_1 |0>_2 |1>_A |1>_E + |1>_1 |1>_2 |0>_A |0>_E), \ \ if\ PT_i = 1. \end{aligned} \tag{24}$$

Then Eve sends Q^A to Alice. After receiving Q^A Alice performs CNOT operation on qubit A in Q^A and quabit 1 in Q^d in which qubit A is the target qubit and qubit 1 is the control qubit. The state of the four-qubit system turns into

$$\begin{aligned} SSS1 &= \frac{1}{\sqrt{2}}(|0>_1 |0>_2 |0>_A |0>_E + |1>_1 |1>_2 |0>_A |1>_E), \ \ if\ PT_i = 0; \\ SSS2 &= \frac{1}{\sqrt{2}}(|0>_1 |0>_2 |1>_A |1>_E + |1>_1 |1>_2 |1>_A |0>_E), \ \ if\ PT_i = 1. \end{aligned} \tag{25}$$

Finally Alice measures Q^A. At the same time Eve measures all her auxilliary qubits and record it accoding to the decoding rule. It's easy to find that Eve will get measurement result $|0>_E$ and $|1>_E$ with the same probability $1/2$ whatever Alice gets measurement result $|0>_1$ or $|1>_1$. So the string PE which Eve gets aren't equal to P_T. It can be summarized in the following Table 2.

Table 2. Result of Entanglement attack.

state of the four-qubit system	PT_i	Alice's result	Eve's result	PE_i
SSS1	0	$\|0>_A$	$\|0>_E$ or $\|1>_E$	0 or 1
SSS2	1	$\|1>_A$	$\|1>_E$ or $\|0>_E$	0 or 1

So Eve can't get the secret message by strategy of entangment attack.

Now we have showed that no eavesdroopers can get the secret message from Bob to Alice.

5. Discussion

In this quantum public-key cryptosystem to accomplish secret communications what people need to do are creating a group of two-qubit systems, performing CNOT operation on two qubits, exchanging qubits through a quantum channel and doing single-particle measurement on a qubit. All these have been carried out decades of years. So there are no fundamental obstacles for this public-key cryptosystem to be realized in practice by today's technology.

In most of previous quantum public-key cryptosystem, the quantum systems serving as user's (public key, private key) pair are consumed after a communication process because their states evitably

 doi:10.20944/preprints202507.0137.v1

changed so that they are no longer available for next communication process. To maintain the public-key cryptosystem to continue working, every user has to reconstruct his or her (public-key, private key) pair and give the public key to KMC. Obviously it is costly because reconstructing (public-key, private key) pairs and sharig public keys with KMC cause rather more resource consump and more time delay. Another solution is to create many copies of (public-key, private key) pairs for every user and keep all the public keys in KMC. But it need much more resource consumption. Moreover it also brings much more difficulties for both KMC and users to perform key management. This is a serious barrier for quantum public-key cryptosystems to be applied in practice. In this quantum public-key cryptosystem the two-qubit systems serving as a user's (public key, private key) pair keep unchanged after a communication process. Or in other words, all the public key and the private key of every user are reusable. So it is much easier to carry out in practice in relative to tranditional quantum public-key cryptosystem. This is a remarkable advantage of this public-key cryptosystem.

6. Conclusions

This paper provided a quantum public-key cryptosystem with reusable (public key, private key) pair using the Bell states. Every user shares a group of two-qubit systems in the Bell state with KMC as his or her (public key, private key) pair. If a user Bob wants to send a secret message to another user Alice, he ask for KMC's help. Then KMC creates a group of auxilliary qubits and engtangles them with Alice's (public key, private key) pair by performing CNOT operations. Next KMC sends the auxilliary qubits to Bob. After receiving the auxlilliary qubits, Bob encodes his message on them and sends them to Alice. When Alice receives the auxilliary qubits, Alice also performs CNOT operations on them and her (public key, private key) pair. Then she measures the auxilliary qubits and get the message at last. At the same time the two-qubit systems turn back to their original states. Alice's (public key, private key) pair keeps unchanged after the communication process so that it can be reused. In this public-key cryptosystem, users doesn't need to save many copies of (public key, private key) pair or reconstruct (public key, private key) pair after a communication process. It greatly reduces the expense for key management. So this quantum public-key cryptosystem is easier to realize in relative to previous quantum public-key cryptosystems.

Author Contributions: Conceptualization, Xiaoyu Li; Analyzation and reasoning, Xiaoyu Li; investigation, Yue Zhou; writing, Xiaoyu Li; error-checking and modifying, Yue Zhou. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Natural Science Foundation of China Grant number 62371423.

Acknowledgments: We would thank Ruqian Lu for directing us into this field.

Conflicts of Interest: The authors declare no conflicts of interest

References

1. Bennett, C.H.; Brassard, G. Quantum cryptography: Public-key distribution and tossing. In Proceedings of IEEE International conference on Computers, Systems and Signal Processing, Bangalore, India, December 1984; pp. 175–179.
2. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Physical Review Letters* **1991**, *67(6)*, 661–663.
3. Bennett, C.H.; Brassard, G.; Mermin, N.D. Quantum cryptography without Bell's theorem. *Physical Review Letters* **1991**, *68(5)*, 557–559.
4. Zhao, Y.; Qi, B.; Lo, H.K. Quantum key distribution with an unknown and untrusted source. *Physical Review A* **2008**, *77(5)*, 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.
6. Aguilar, E.A.; Ramanathan, R.; Kofler, J.; Pawlowski, M. Completely Device Independent Quantum Key Distribution. *Physical Review A* **2015**, *94(2)*, 022305.

 doi:10.20944/preprints202507.0137.v1

7. Zhen, Y.Z.; Mao, Y.; Sanders, X.B.C. Device-Independent Quantum Key Distribution Based on the Mermin-Peres Magic Square Game. *Physical Review Letters* **2023**, *131*, 090801.
8. 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(1)*, 012604.
9. Zhang, C.M.; Wang, Z.; Wu. Y.D.; Zhu, J.R.; Wang, R.; Li, H.W. Discrete-phase-randomized twin-field quantum key distribution with advantage distillation. *Physical Review A* **2024**, *109(5)*, 052432.
10. 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.
11. Sixto, X.; Navaerrete, A.; Pereira, M.; Curras-Lorenzo, G.; Tamaki, k.; Curty, M. Quantum key distribution with imperfectly isolated devices. *Quantum Science and Technology* **2025**, *10(3)*, 035034.
12. Rivera-Dean, J.; Steffinlongo, A.; Parker-Sánchez, N.; Acín, A.; Tamaki, k.; Curty, M.; Oudot, E. Device-independent quantum key distribution beyond qubits. *New Journal of Physics* **2025**, *27(5)*, 054512.
13. Bennett, C.H.; Bessette, F.; Brassard, G.; Salvail, L.; Smolin, J. Experimental quantum cryptography. *Journal of Cryptology* **1992**, *5(1)*, 3-28.
14. Yin, H.L.; Chen, T.Y.; Yu, Z.W.; Liu, H.; You, L.X.; Zhou, H.Y,; et al. Measurement device independent quantum key distribution over 404 km optical fibre. *Physical Review Letters* **2016**, *117*, 190501.
15. Buttler, W.T.; Hughes, R.J.; Kwiat, P.G.; Lamoreaux, S.K.; Luther, G.G.; Morgan, G.L.; Nordholt, J.E.; et al. Practical Free-Space Quantum Key Distribution over 1 km. *Physical Review Letters* **1998**, *81(15)*, 3283.
16. Liao, S.K.; Cai, W.Q.; Liu, W.Y.; Liang, Z.; Yang, L.; Ren, J.G.; et al. Satellite-to-ground quantum key distribution. *Nature* **2017**, *549(7670)*, 43-47.
17. Rivest, R.; Sharmir, A.; Adleman, L. A Method for Obstaining Digital signature and Public-Key Cryptosystem. *Communications of ACM* **1978**, *21(2)*, 120-126.
18. Shor, P.W. Algorithms for quantum computation: Discrete logarithm and Factoring. In Proceedings of 35th Annual IEEE Symposium on Foundations of Computer Science, Santa Fe, US. 1994; pp. 124-134.
19. Gottesman D, Chuang I. A Method for Obstaining Digital signature and Public-Key Cryptosystem. *arXiv:quant-ph*, 2001, 0105032.
20. Nikolopoulos, G. Applications of single-qubit rotations in quantum public-key cryptography. *Physical Review A* **2008**, *77(3)*, 032348.
21. Nikolopoulos, G.; Ioannou, L. Deterministic quantum-public-key encryption: forward search attack and randomization. *Physical Review A* **2008**, *77(3)*, 032348.
22. Ioannou, L.; Mosca, M. Public-key cryptography based on bounded quantum reference frames. In Proceedings of 6th Conference on the Theory of Quantum Computation, Communication and Cryptography, Madrid, Spain 2011; pp. 121-142.
23. Luo, M.X.; Chen, X.B.; Yun, D.; Yang, Y.X. Quantum Public-Key Cryptosystem. *International Journal of Theoretical Physics* **2012**, *51(3)*, 912-924.
24. 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.
25. Vlachou, C.; Rodrigues, J, Mateus, P. Quantum walk public-key cryptographic system. *International Journal of Quantum Information* **2015**, *13(7)*, 1550050.
26. Wu, W.Q.; Cai, Q.Y.; Zhang, H.G.; Liang, X.Y. Quantum Public Key Cryptosystem Based on Bell States. *International Journal of Theoretical Physics* **2017**, *56(11)*, 3431-3440.
27. Yang, L.; Yang, B.Y.; Xiang, C. Quantum public-key encryption schemes based on conjugate coding. *Quantum Information Processing* **2020**, *19(11)*, 415.
28. Liu, Z.X.; Xie, Q.L.; Zha, Y.F.; Dong, F.M. Quantum public key encryption scheme with four states key. *Physica Scripta* **2022**, *97*, 045102.
29. Zhang, D.X.; Li, X.Y. 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.
30. Li, X.Y.; Chen, L.J. QUANTUM PUBLIC-KEY CRYPTOSYSTEM WITHOUT QUANTUM. *Romanian Journal of Physics* **2022**, *67*, 118.
31. Wang Y, Chen G, Jian L. Ternary quantum public-key cryptography based on qubit rotation. *Quantum Information Processing* **2022**, *21(6)*, 197.
32. Barooti K, Grilo AB, Huguenin-Dumittan L, Malavolta G, Sattath O, Vu Q, M Walter M. Public-Key Encryption with Quantum Keys. In 21st International Conference on Theory of Cryptography, Taipei, Taiwan, November, 2023; 198-227.

 doi:10.20944/preprints202507.0137.v1

33. Zhang, D.X.; Li, X.Y.; Zhao, Q.Y. Quantum Public-Key Cryptosystem Based on the Non-Locality in Unentangled Quantum System. *Brazilian Journal of Physics* **2024**, *54(5)*, 158.
34. 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, August, Santa Barbara, US, 2024; 93-125.
35. 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, August, Santa Barbara, US, 2024; 126-151.
36. Fu, X.Q.; Li, H.W.; Shi, J.H.; Li, T.; Bao, W.S. Quantum public-key crypto via EPR pairs. *Science China-Physics Mechanics & Astronomy* **2025**, *68(1)*, 210314.
37. Li, X.Y.; Chen, Y.L. Quantum Public-Key Cryptosystem Using Orthogonal Product States with High Channel Capacity. *Contemporary Mathematics* **2025**, *6(2)*, 1455-1467.
38. Hussain, S.M.S.; Aftab, M.A.; Farooq, S.M.; Latif, A. ; Konstantinou, C.; Abido, M.A. A Public key Based Quantum Secure Digital Signature Scheme for Securing IEC 61850 R-GOOSE and R-SV Messages. *IEEE Transactions on Industrial Applications* **2025**, *61(3)*, 5135-5147.