Multi-Bits Transfer Based on the Quantum Three-Stage Protocol with Quantum Error Correction Codes

Duc Manh Nguyen & Sunghwan Kim

International Journal of Theoretical Physics

ISSN 0020-7748
Volume 58
Number 6

Int J Theor Phys (2019) 58:2043-2053
DOI 10.1007/s10773-019-04098-4

Volume 58 • Number 6 • June 2019

International Journal of Theoretical Physics

10773 · ISSN 0020-7748
58(6) 1711–2068 (2019)

Springer

International Journal of Theoretical Physics (2019) 58:2043–2053
https://doi.org/10.1007/s10773-019-04098-4

Multi-Bits Transfer Based on the Quantum Three-Stage Protocol with Quantum Error Correction Codes

Duc Manh Nguyen[1] · Sunghwan Kim[1]

Received: 29 August 2018 / Accepted: 18 March 2019 / Published online: 6 April 2019

Abstract
This paper presents a multi-bits transfer quantum protocol based on the three-stage quantum cryptography in which both parties use their own secret keys. In addition, a quantum three-stage protocol emerging with quantum error correction code is proposed. Finally, a cost comparison between the multi-bits transfer quantum protocol and the original three-stage quantum cryptography protocol is analyzed to show that our protocol has better performance.

Keywords Quantum cryptography · Quantum key distribution protocol · Quantum three-stage protocol · Quantum error correction code

1 Introduction

Quantum mechanics, which gives approximate and remarkably accurate predictions is successful in explaining and predicting many phenomena [1, 2]. The efficiency involved in quantum mechanics has often been demonstrated. One of the interesting applications of quantum principles is their application to information theory [3], which is a result of the effort to generalize classic information theory leading to the quantum computer. The field of quantum computing was first introduced by Richard Feynman in 1982 [4]. Digital computers are based on transistor gates that require data to be encoded into binary digits. In contrast, the quantum computer utilizes the properties of molecules to represent data, and subsequently, the quantum computer performs the operations on these data representations, wherein the superposition of quantum states and entanglement are involved. A theoretical model is the quantum Turing machine, also known as a universal quantum computer, which shares theoretical similarities with non-deterministic and probabilistic computers, including the ability to be in more than one state simultaneously.

✉ Sunghwan Kim
sungkim@ulsan.ac.kr

Duc Manh Nguyen
nguyenmanhduc18@gmail.com

[1] School of Electrical Engineering, University of Ulsan, 93 Daehak-ro, Nam-gu, Ulsan, 44610, Korea

An important milestone in quantum computing occurred in 1994 when Shor published a computationally efficient quantum algorithm for factoring integers and for evaluating discrete algorithms [5]. With these algorithms, the owner of the quantum computer could crack popular, highly utilized public key crypto-systems. In addition, Grover discovered a quantum algorithm for the important problem of searching unstructured databases, yielding a substantial speed-up over classic search algorithms [6, 7]. However, the effects of noise and imperfectly applied quantum gates would quash the performance advantages [8]. To deal with the problems, the theory of quantum error correction code (QECC) was developed to protect quantum states against noise. Discoveries of 9-qubit codes by Shor [9] and 7-qubit codes by Steane [10] showed how data could be protected by containing more redundancy after encoding by quantum systems; these were the first examples of QECC. The purpose of QECC is to encode a k-qubit state into a logical n-qubit state such that all 2^k complex coefficients are perfectly stored and used to correct errors [11].

Cryptography is the science of protecting private information from unauthorized access, ensuring data integrity, authentication, and other tasks. Quantum cryptography is an emerging technology based on the phenomena and properties of light. Quantum cryptography was developed by physicist Dr. Charles H. Bennett, who proposed the unconditionally secure quantum key distribution protocol BB84 [12]. In addition, ping-pong quantum secure direct communication uses the entanglement [13]. In 2002, a new kind of quantum cryptography protocol based on Shamir's three-stage protocol of classic cryptography was presented, and then, the quantum three-stage protocol (QTSP) based on quantum superposition states was proposed [14]. QTSP shows that there can be no key shared between the sender and receiver unlike the BB84 protocol. Throughout subsequent years, the science began to evolve rapidly and significantly. The basic idea behind QTSP is that of sending secrets (or valuables) through an unreliable courier by having both Alice and Bob place their locks on the box containing the secret, which is also called double-lock cryptography. The basic polarization rotation scheme was implemented in hardware where more than one photon can be used in the exchange between Alice and Bob. Therefore, it opens the possibility of multi-photons quantum cryptography [15]. The analysis of QTSP that can deal with the man-in-the-middle attack was also discussed [16]. Parakh analyzed the three-stage protocol under rotational quantum errors, and proposed a modified protocol based on the emerging QTSP and repetition code that can correct the errors [17]. In [18], the QTSP protocol was proven to work as a scheme for secure direct quantum communications. Then, a realizable quantum three-pass protocol based on Hill-cipher algorithm was discussed [19], wherein the message is first encrypted into a binary string by the Hill-cipher, then each bit is encrypted into a single quantum state and the QTSP is used to exchange each bit.

The key result of this paper is to propose a modified QTSP to attach many bits into a single quantum state, and then use the QTSP protocol for the transfer between parties. The proposed protocol promises the advantages of a single qubit that can carry an unlimited amount of information. Moreover, the qubit needs to be protected from noise for the correct quantum state exchanged between parties. Therefore, we use the quantum error correction code emerging with QTSP to restore a quantum noise, the decoherence in a quantum state to a pure quantum state by removing the errors. The organization of this paper is as follows. In the next section, we review the theory of quantum information. In Section 3, we review the three-stage quantum cryptography protocol. Then, in Section 4, we propose the modified quantum three-stage protocol to attach the multi-bits in one qubit to exchange in the quantum system. Quantum error correction code using in the quantum three-stage protocol is discussed in Section 5. Finally, the conclusions are presented in the last section.

2 Quantum Information Theory

The *bit* is the fundamental unit of classical information. The fundamental unit of quantum information is the quantum bit (*qubit*). Just as the classic bit has a state of either 0 or 1, the state in the quantum system is instead a two-state physical system (0 and 1) on which the superposition principle applies. For the purpose of using mathematical model for quantum computing , we consider two-dimensional complex Hilbert space, H. The base state is denoted as

$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}, |1\rangle = \begin{bmatrix}0\\1\end{bmatrix},$$

and the general state is a linear combination of the two base states:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \begin{bmatrix}\alpha\\\beta\end{bmatrix},$$

where α and β are complex numbers and $|\alpha|^2 + |\beta|^2 = 1$. In general, quantum memory is a physical system composed of n qubits that can be considered as an element of the n times tensor-product of H. Quantum information processing requires unitary transformations operating on states. Linear operator $\mathbf{U}$ acting on single qubit fulfill normalization preserving condition if and only if $\mathbf{U}\mathbf{U}^{\dagger} = \mathbf{I}$, where $\mathbf{U}^{\dagger}$ is the adjoint of $\mathbf{U}$ (obtained by transposing and then complex conjugating $\mathbf{U}$). Some of the most important single-qubit operators are Pauli operators. So that any operation of one qubit can be decomposed as the linear combination of the Pauli matrices:

$$\mathbf{I} = \begin{bmatrix}10\\01\end{bmatrix}, \mathbf{X} = \begin{bmatrix}01\\10\end{bmatrix}, \mathbf{Z} = \begin{bmatrix}1\ 0\\0{-}1\end{bmatrix}, \mathbf{Y} = \mathbf{XZ}.$$

Pauli operators $\mathbf{X}$, $\mathbf{Z}$, and $\mathbf{Y}$ are regarded as a bit flip, a phase flip, and a combination of bit and phase flips, respectively. The single Pauli group, P_1, is a group formed by the Pauli operators, which is closed under multiplication. Therefore, the Pauli group consists of all the Pauli matrices. We have: $P_1 = \{\mathbf{I},\mathbf{X},\mathbf{Y},\mathbf{Z}\}$. The n-fold tensor product of single Pauli operators forms an n-qubit Pauli group, P_n. The main property of P_n is that any two elements, $\mathbf{A},\mathbf{B} \in P_n$, are either commutative or anti-commutative.

Let $H^{\otimes n}$ be the quantum state space of n qubits. A stabilizer group, S, closed under multiplication is an Abelian subgroup of P_n such that a non-trivial subspace, C_S of $H^{\otimes n}$, is fixed (or stabilized) by S. The stabilized C_S defines a quantum code space such that

$$C_S = \{|\psi\rangle \in H^{\otimes n} : \mathbf{g}|\psi\rangle = |\psi\rangle, \forall \mathbf{g} \in S\}.$$

If S is generated by $g = \{\mathbf{g}_1,\mathbf{g}_2,..,\mathbf{g}_m\}$ ($m = n - k$ independent stabilizer operators), the code space C_S encodes k logical qubits into n physical qubits and it can correct $\left\lfloor \frac{d_{\min}-1}{2} \right\rfloor$ errors and can detect $(d_{\min}-1)$ errors. This quantum stabilizer code C_S is denoted as $[[n, k, d_{\min}]]$. Then, it is enough to check the commutative property of generators of g, where two elements have to be commutative to each other.

The quantum stabilizer operators help to construct the encoding and decoding circuits for quantum error correction. For example, in [21], the construction and error correcting circuit for quantum stabilizer [[7,1,3]] code was considered. The Shor code, or 9-qubit code, (the first full quantum code) was discussed in [23]. The shortest length of QECC [[5,1,3]] with an error correcting circuit was given in [8] and [22]. The single qubit, $\alpha\,|0\rangle + \beta\,|1\rangle$, is first extended to 5-qubits with the help of four ancilla qubits $|0000\rangle$. The combined 5-qubits go through the encoder to get the stabilizer state named the quantum logical state, where the stabilizer generators are given in Table 1. The errors that happen in a quantum

Table 1 Generators of [[5,1,3]]

Generators	Pauli operators
$\mathbf{g}_1$	**YZZY**
$\mathbf{g}_2$	**XZZX**
$\mathbf{g}_3$	**ZZXX**
$\mathbf{g}_4$	**ZZYY**

channel effect the quantum logical state. The errors are detected, and they are removed by quantum stabilizer operators, then the quantum logical state is corrected and the final output is $\alpha |0\rangle + \beta |1\rangle$. The simulation error correcting of [[5,1,3]] was discussed in [8].

3 Quantum Three-Stage Protocol

The three-stage quantum cryptography protocol is a method of data encryption that was proposed by Subhash Kak [14]. It is based on double-block cryptography with random polarization rotations by both parties. The secret rotations are so chosen that they commute with each other, i.e., $U(a)U(b) = U(b)U(a)$. Therefore, they are of following form:

$$U(\theta) = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \tag{1}$$

This operation can be considered in encryption, and θ represents the encryption key, while the rotation operation can be considered in decryption with the key $-\theta$.

Assume Alice wants to securely send an arbitrary quantum state, $|\psi\rangle$, to Bob. The protocol proceeds as follows.

1. Alice chooses secret random rotation transformation $U(\theta_A)$ and sends to Bob $U(\theta_A)|\psi\rangle$.
2. Bob chooses his secret random rotation transformation $U(\theta_B)$ and sends to Alice $U(\theta_B)U(\theta_A)|\psi\rangle$.
3. Alice applies the inverse of her transformation from step 1, $U(\theta_A)^{\dagger} = U(-\theta_A)$ and returns qubit $U(\theta_B)|\psi\rangle$ to Bob.
4. Bob applies his secret random rotation transformation, $U(\theta_B)^{\dagger} = U(-\theta_B)$, and retrieves the final quantum state, $|\psi\rangle$.

There are three transmissions in total, hence the name is three-stage protocol.

In the quantum three-pass protocol there is no shared key between the sender and the receiver; the sender generates its own secret $K_{\theta_{\mathbf{S}}}$ where $K_{\theta_{\mathbf{S}}} = \{\theta_{\mathbf{S}} | 0 \leq \theta_{\mathbf{S}} < \pi\}$ for each session. And the receiver generates its own secret key $K_{\theta_{\mathbf{R}}}$ where $K_{\theta_{\mathbf{R}}} = \{\theta_{\mathbf{R}} | 0 \leq \theta_{\mathbf{R}} < \pi\}$ for each session. Certainly, an opponent never discovers these keys. For n-qubits, the keys for the sender and the receiver are changed for each qubit, and each key is used only twice by the generator (once for encryption and once for decryption) which continues for other n-qubits of the key. Therefore the new key will prevent any information related to the key and data from being infiltrated. Now, if it is assumed that bit P is a single bit encrypted to the qubit $P = |1\rangle$, sender and receiver generate their own key, the key of the sender is $K_{\theta_{\mathbf{S}}}$, and the key of the receiver is $K_{\theta_{\mathbf{R}}}$. The sender encrypts bit P with the generation key, as follows.

$$E_{K_{\theta_{\mathbf{S}}}}[P]:$$

$$U(\theta_{\mathbf{S}})|1\rangle = \begin{bmatrix} \cos\theta_{\mathbf{S}} & \sin\theta_{\mathbf{S}} \\ -\sin\theta_{\mathbf{S}} & \cos\theta_{\mathbf{S}} \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \sin\theta_{\mathbf{S}}|0\rangle + \cos\theta_{\mathbf{S}}|1\rangle = |\theta_1\rangle$$

where E is encryption with the sender's key, $K_{\theta_{\mathbf{S}}}$, and the result is the superposition state, $|\theta_1\rangle$, which will be sent to the receiver. The receiver receives the qubit, $|\theta_1\rangle$, and encrypts it with its own key as follows.

$$E_{K_{\theta_{\mathbf{R}}}}[E_{K_{\theta_{\mathbf{S}}}}[P]]:$$
$$U(\theta_{\mathbf{R}})\,|\theta_1\rangle = \sin(\theta_{\mathbf{R}}+\theta_{\mathbf{S}})\,|0\rangle + \cos(\theta_{\mathbf{R}}+\theta_{\mathbf{S}})\,|1\rangle = |\theta_2\rangle$$

where $|\theta_2\rangle$ is the superposition state. The receiver sends $|\theta_2\rangle$ back to the sender. The sender receives $|\theta_2\rangle$ and decrypts it by using the key, $\theta_{\mathbf{S}}$, but with a rotation of $-\,\theta_{\mathbf{S}}$ because there are decrypts in this case; then, the result, $|\theta_3\rangle$, goes back to the receiver as follows.

$$D_{K_{\theta_{\mathbf{S}}}}[E_{K_{\theta_{\mathbf{R}}}}[E_{K_{\theta_{\mathbf{S}}}}[P]]]:$$
$$U(-\theta_{\mathbf{S}})\,|\theta_2\rangle = \sin(\theta_{\mathbf{R}})\,|0\rangle + \cos(\theta_{\mathbf{R}})\,|1\rangle = |\theta_3\rangle\,,$$

where D is the decryption with sender's key $K_{\theta_{\mathbf{S}}}$. The receiver receives $|\theta_3\rangle$ and decrypts it by using $\theta_{\mathbf{R}}$, but with a rotation of $-\,\theta_{\mathbf{R}}$ because there are decryptions in this case; then, the receiver gets bit P that the sender sends, $|1\rangle$, as the follows.

$$D_{K_{\theta_{\mathbf{R}}}}[D_{K_{\theta_{\mathbf{S}}}}[E_{K_{\theta_{\mathbf{R}}}}[E_{K_{\theta_{\mathbf{S}}}}[P]]]]:$$
$$U(-\theta_{\mathbf{R}})\,|\theta_3\rangle = \begin{bmatrix}\cos(-\theta_{\mathbf{R}}) & \sin(-\theta_{\mathbf{R}})\\ -\sin(-\theta_{\mathbf{R}}) & \cos(-\theta_{\mathbf{R}})\end{bmatrix}\begin{bmatrix}\sin(\theta_{\mathbf{R}})\\ \cos(\theta_{\mathbf{R}})\end{bmatrix} = |1\rangle$$

Finally, the receiver has the bit, $|1\rangle$. The whole procedure of the protocol is in Fig. 1.

4 Multi-Bits Transfer Based on the Three-Stage Quantum Cryptography Protocol

Realizable quantum three-pass protocol authentication based on the Hill-cipher algorithm was presented in [19]. The plain-text is converted into binary string 01111011000111110011. The sender attaches each bit into a single qubit; for example first sending quantum bit $|1\rangle$ using the QTSP procedure. To send the whole binary string 01111011000111110011 requires using QTSP between Alice and Bob 20 times.

We propose a new algorithm to attach five information bits in one qubit, transferring it using the QTSP procedure. Alice and Bob can exchange the binary string as follows.

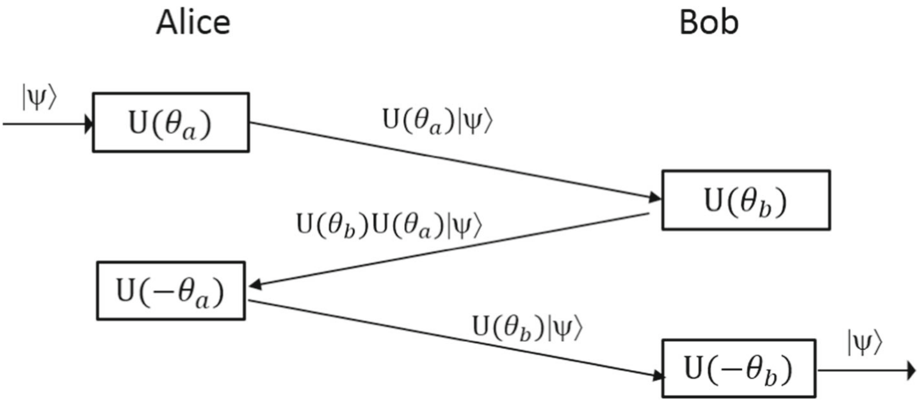

Fig. 1 Quantum three-stage protocol

1. Alice chooses five random binary digits, $a_1a_2a_3a_4a_5$ (where a_i is binary value {0,1}), and its decimal value is denoted as a (between 1 and 63). Alice and Bob use QTSP to exchange each bit. The length of that bit string is 5, so it requires using the QTSP procedure five times.
2. For the first five-bits string of key 01111, the decimal value is 15; Alice first attaches the five-digits string 01111 into a single qubit as follows.

$$|\theta_{01111}\rangle = \frac{15}{\sqrt{15^2+a^2}}|0\rangle + \frac{a}{\sqrt{15^2+a^2}}|1\rangle = \sin\theta_{01111}|0\rangle + \cos\theta_{01111}|1\rangle .$$

   Alice and Bob exchange the quantum state $|\theta_{01111}\rangle$ using the QTSP procedure. Bob finally receives the correct state, $|\theta_{01111}\rangle$, and he uses the measurement with basis quantum state, $|0\rangle$, to get the probability value, $\frac{15}{\sqrt{15^2+a^2}}$, of the final state in the basic $|0\rangle$ state. Bob knows the value of a, and then, will know the exact decimal value, 15, and the corresponding binary string, 01111. Then, Alice and Bob have exchanged the binary string.
3. We use the procedure in step 2 for the remaining binary strings: 01100, 01111, 10011. Each string is encoded in a single quantum state

$$\begin{aligned} |\theta_{01100}\rangle &= \frac{12}{\sqrt{12^2+a^2}}|0\rangle + \frac{a}{\sqrt{12^2+a^2}}|1\rangle = \sin\theta_{01100}|0\rangle + \cos\theta_{01100}|1\rangle , \\ |\theta_{01111}\rangle &= \frac{15}{\sqrt{15^2+a^2}}|0\rangle + \frac{a}{\sqrt{15^2+a^2}}|1\rangle = \sin\theta_{01111}|0\rangle + \cos\theta_{01111}|1\rangle , \\ |\theta_{10011}\rangle &= \frac{19}{\sqrt{19^2+a^2}}|0\rangle + \frac{a}{\sqrt{19^2+a^2}}|1\rangle = \sin\theta_{10011}|0\rangle + \cos\theta_{10011}|1\rangle , \end{aligned}$$

   respectively.

In [19], each bit was transferred using the QTSP procedure, and we have 20-digits number, so it requires using QTSP procedure 20 times. In contrast, with the above procedure, Alice and Bob need qubit exchange by using QTSP nine times.

Generally, we sum up the proposed algorithm in Fig. 2 to attach multi-bits into one qubit and transfer it using the QTSP procedure. Assume that Alice and Bob wish to exchange binary string $\mathbf{b}_1\mathbf{b}_2...\mathbf{b}_n$, where $\mathbf{b}_i$ has length m, and the length of the total string is $l = n \times m$ (m,n and l are positive integers). The protocol proceeds as follows.

Multi-Bits Transfer Based on QTSP

1. Alice first chooses random binary string $a_1a_2...a_m$, and $\mathbf{a}$ is the corresponding decimal value, $\mathbf{a}\neq 0$. Alice will encode each bit, a_1,a_2,...,a_m, into quantum state $|a_1\rangle , |a_2\rangle , ..., |a_m\rangle$. Each quantum state is transferred to Bob by using the QTSP procedure as described in Section 2. It requires using QTSP m time to transfer them to Bob.
2. In this step, $b_1, b_2, ..., b_n$ is denoted as the decimal value of binary string $\mathbf{b}_1\mathbf{b}_2...\mathbf{b}_n$. Each string is attached to a single quantum state as follows.

$$\begin{aligned} |\theta_{b_1}\rangle &= \frac{b_1}{\sqrt{b_1^2+a^2}}|0\rangle + \frac{a}{\sqrt{b_1^2+a^2}}|1\rangle = \sin\theta_{b_1}|0\rangle + \cos\theta_{b_1}|1\rangle , \\ |\theta_{b_2}\rangle &= \frac{b_2}{\sqrt{b_2^2+a^2}}|0\rangle + \frac{a}{\sqrt{b_2^2+a^2}}|1\rangle = \sin\theta_{b_2}|0\rangle + \cos\theta_{b_2}|1\rangle , \end{aligned}$$

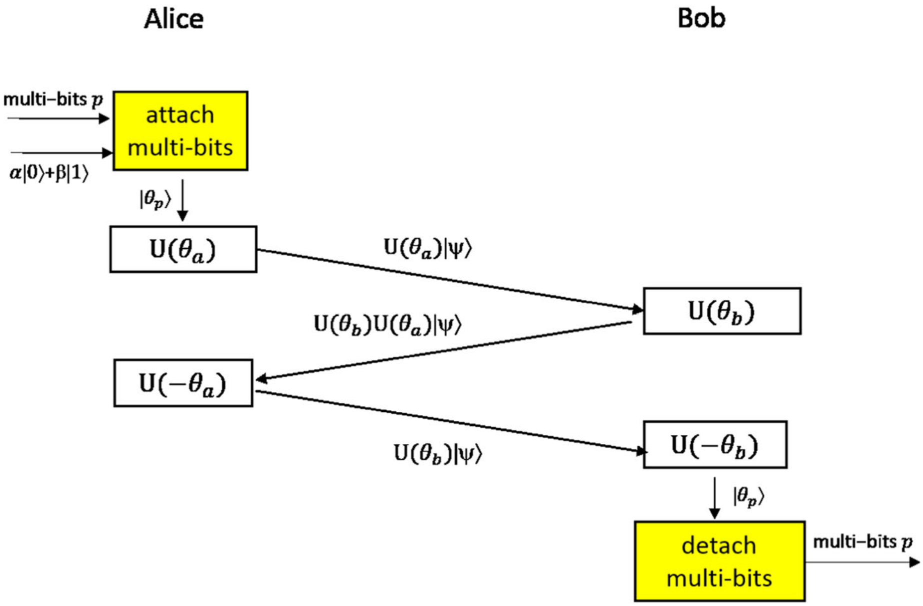

Fig. 2 Multi-bits transfer based on QTSP

...

$$\left|\theta_{b_n}\right\rangle = \frac{b_1}{\sqrt{b_n^2+a^2}}\,|0\rangle + \frac{a}{\sqrt{b_n^2+a^2}}\,|1\rangle = \sin\theta_{b_n}\,|0\rangle + \cos\theta_{b_n}\,|1\rangle\,.$$

Alice transfers each single qubit, $\left|\theta_{b_1}\right\rangle$, $\left|\theta_{b_2}\right\rangle$, ..., $\left|\theta_{b_n}\right\rangle$, to Bob by using the QTSP procedure. Bob receives the exact the qubit, uses the measurement with basis quantum state $|0\rangle$ to get the probability value, $\frac{b_i}{\sqrt{b_i^2+a^2}}$ $(i = 1,2,...,n)$ of the final state in the basic $|0\rangle$ state. Bob knows the value of a, and then, he will know the exact decimal value, $b_1, b_2, ..., b_n$, and the corresponding binary string, $\mathbf{b}_1, \mathbf{b}_2, ..., \mathbf{b}_n$. Then, Alice and Bob have exchanged binary string $\mathbf{b}_1\mathbf{b}_2...\mathbf{b}_n$. Step 2 requires using the QTSP procedure n times.

Using multi-bits transfer based on the QTSP procedure, for binary string length $l = n \times m$, we need use the QTSP procedure $cost = m + n$, where n is the length of the multi-bits, and the constant number length n has to be transferred one-by-one by using the QTSP protocol; therefore, it should be a small number. In contrast, if we use only the QTSP protocol, it requires using QTSP $cost = n \times m$ times. For more details, in Fig. 3, we consider the cost as a function of the binary string length; the red line is the graph of function $y = 5n$, and the blue line is the graph of function $y = 5 + n$. This shows that our procedure reduces the complexity of the quantum system needed to transfer a long binary string.

5 Quantum Three-Stage Protocol with Error Correction Codes

We saw that unwanted interactions with the environment changes quantum states. In the QSTP protocol, the quantum state has to be transmitted three times, if there are errors from

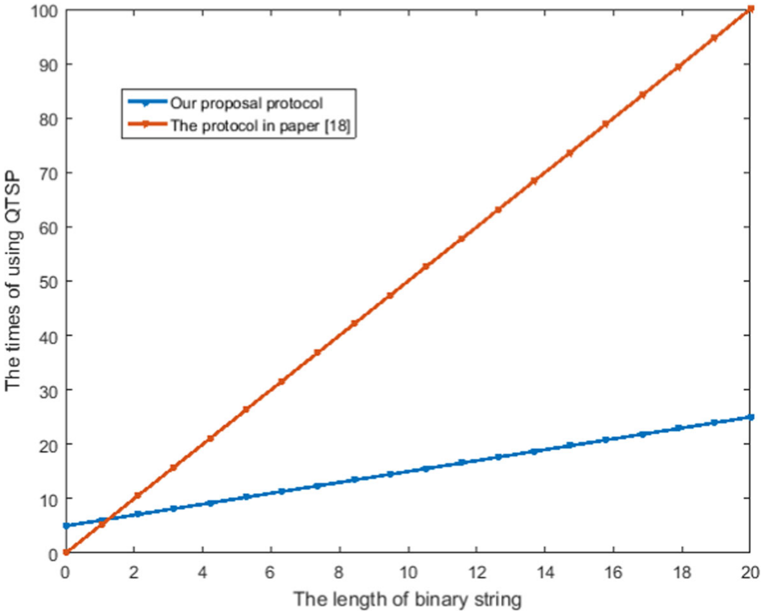

Fig. 3 Comparison between our proposal protocol without QECC and the protocol in [19]

the environment, it will change the quantum state; so the key sharing between Alice and Bob is incorrect. We need a way to detect, or even correct, these errors. We use quantum stabilizer code [[5,1,3]] that can correct one error, can detect two errors and required the length five logical quantum state, the shortest code. If the errors are detected, Bob can correct them by decoder or require Alice to re-transmit the quantum state. Figure 4 shows a modified QTSP protocol with QECC. Since Kak's protocol requires three transmissions, the quantum error correction code would have to be executed after every transmission by Alice and Bob. The modified quantum three-stage protocol with quantum error correction is as follows.

1. Alice prepares the multi-bits string p to attach in a single qubit, as described in Section 4, to get the single qubit $\left|\alpha_p\right\rangle$.
2. Alice chooses a secret random rotation transformation, U_a, and maps $U_a\left|\alpha_p\right\rangle$ into logical qubit $|\Psi_{\mathrm{aL}}\rangle$, and then, sends it to Bob.
3. Bob executes the error detection and correction algorithm, returning the received quantum state from $\left|\Psi'_{\mathrm{aL}}\right\rangle$ to $U_a\left|\alpha_p\right\rangle$.
4. Bob then chooses his secret random rotation transformation, U_b, and maps qubit $U_bU_a\left|\alpha_p\right\rangle$ into the logical qubit $|\Psi_{\mathrm{abL}}\rangle$, and returns it to Alice.
5. Alice executes error detection and correction, retrieving the quantum state, $U_bU_a\left|\alpha_p\right\rangle$.
6. Alice then applies the inverse of her transformation from step 1, $U_a^{\dagger}$, and maps $U_b\left|\alpha_p\right\rangle$ into logical qubit $|\Psi_{\mathrm{bL}}\rangle$. Then, Alice returns the logical qubit to Bob.

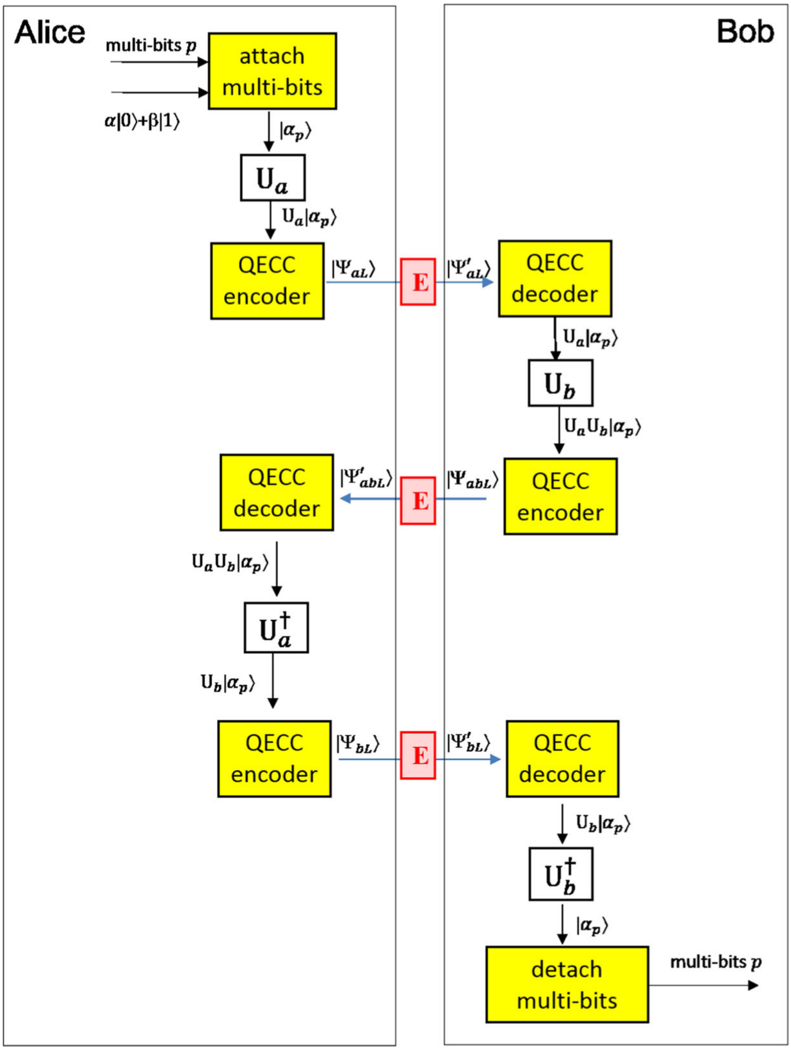

Fig. 4 Multi-bits transfer QTSP protocol with QECC

7. Bob, upon receiving the qubit, applies error detection and correction one final time, thereby converting the state to $|\Psi_{\mathrm{bL}}\rangle$. Bob applies his secret random rotation transformation, $U_b^{\dagger}$, and retrieves $|\alpha_p\rangle$ without errors.
8. The multi-bits p is finally detached from the qubit via measurement, and then, Bob gets the string, p. In the original QTSP, Alice and Bob need to teleport a single qubit. But errors are very serious in a quantum system; it affects the existence of the qubits. Therefore, the modified QTSP protocol with QECC aims to protect single qubits from errors with quantum stabilizer codes $[[n,1,d]]$, where the smallest n is 5, and d is bigger

than 3. Hence, at least the single qubit has to be encoded into five qubits. Therefore, Alice needs the complex system to teleport five qubits to Bob.

6 Conclusion

In this paper, a new protocol based on a three-stage quantum cryptography protocol to transfer multi-bits has been proposed. This protocol has the security of the original three-stage quantum cryptography protocol. In addition, it shows the advantages of quantum information bits, *qubits*, that can attach infinite information in a single *qubit*. In addition, quantum stabilizer code was used together with QTSP to protect the quantum state under the noise of the environment.

Acknowledgements This work was supported by the Research Program through the National Research Foundation of Korea (NRF-2016R1D1A1B03934653, NRF-2019R1A2C1005920).

References

1. Von Neumann, J.: Mathematical foundations of quantum mechanics. Princeton University Press, Princeton (1955)
2. Feynman, R.P., Leighton, R.B., Sands, M.: Lectures on Physics, vol. III. Quantum mechanics. Addison-Wesley, Reading (1965)
3. Nielsen, M.A., Chuang, I.L.: Quantum computation and quantum information. Cambridge University Press, Cambridge (2000)
4. Feynman, R.P.: Simulating physics with computers. Int. J. Theor. Phys. **21**, 6 (1982)
5. Shor, P.W.: Algorithms for quantum computation discrete logarithms and factoring, pp 124–134. IEEE Computer Society Press, Washington (1994)
6. Grover, L.: Quantum mechanics helps in searching for a needle in a haystack. Phys. Rev. Lett. **79**, 325 (1997)
7. Nguyen, D.M., Kim, S.: Quantum key distribution protocol based on modified generalization of Deutsch-Jozsa algorithm in *d*-level quantum system. Int. J. Theor. Phys. **58**, 1 (2019)
8. Gaitan, F.: Quantum error correction and fault tolerant quantum computing. CRC Press, Boca Raton (2007)
9. Shor, P.W.: Scheme for reducing decoherence in quantum computer memory. Phys. Rev. A **52**, 2493 (1995)
10. Steane, A.M.: Error correcting codes in quantum theory. Phys. Rev. Lett. **77**, 793 (1996)
11. Gottesman, D.: Stabilizer codes and quantum error correction. Ph.D. thesis, California Institute of Technology, Pasadena, CA (1997)
12. Bennett, C.H., Bessette, F., Brassard, G., Salvail, L., Smolin, J.: Experimental quantum cryptography. J Cryptol **5**(1), 3–28 (1992)
13. Cai, Q.Y.: The ping-pong protocol can be attacked without eavesdropping. Phys. Rev. Lett., 91 (2003)
14. Kak, S.: A three-stage quantum cryptography protocol. Found Phys Lett **19**, 293 (2006)
15. Mandal, S., et al.: Multi-photon implementation of three-stage quantum cryptography protocol. The International Conference on Information Networking (ICOIN) (2013)
16. Chan, K.W.C., Rifai, M.El., Verma, P.K., Kak, S.C., Chen, Y.: Security analysis of the multi-photon three-stage quantum key distribution. International Journal on Cryptography and Information Security (IJCIS), 5(3/4) (2015)
17. Parakh. A., van Brandwijk, J.: Correcting rotational errors in three stage QKD. In: 23rd International Conference on Telecommunications (ICT) (2016)
18. Thapliyal, K., Pathak, A.: Kak's three-stage protocol of secure quantum communication revisited: hitherto unknown strengths and weaknesses of the protocol. Quantum Inf Process **17**, 229 (2018)
19. Abdullah, A.A., Khalaf, R., Riza, M.: A realizable quantum Three-Pass protocol authentication based on Hill-Cipher algorithm. Math. Probl. Eng., 2015 (2015)
20. Nguyen, D.M., Kim, S.: Minimal-entanglement entanglement-assisted quantum error correction codes from modified circulant matrices. Symmetry **9**(7), 122 (2017)

21. Nguyen, D.M., Kim, S.: Construction and complement circuit of a quantum stabilizer code with length 7. In: Proceedings of 8th International Conference on Ubiquitous and Future Networks (2016)
22. Nguyen, D.M., Kim, S.: Quantum stabilizer codes construction from hermitian Self-Orthogonal codes over GF(4). J. Commun. Netw. **20**(3), 209–315 (2017)
23. Devitt, S.J., Munro, W.J., Nemoto, K.: Quantum error correction for beginners. Reports on Progress in Physics. 76(7) (2013)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.