A quantum three pass protocol with phase estimation for many bits transfer

Duc Manh Nguyen
Coding & Information Theory Laboratory,
University of Ulsan, South Korea
nguyenmanhduc18@gmail.com

Sunghwan Kim
Coding & Information Theory Laboratory,
University of Ulsan, South Korea
sungkim@ulsan.ac.kr

***Abstract*—In this research, we propose a protocol for many bits transfer which is improved from quantum three pass protocol by using quantum phase estimation algorithm. In which, each party encrypt and decrypt the message by their own key. In addition, instead of attached in the carrier qubits, the key distribution is attached into the phase. Therefore, in the proposed protocol, the phase estimation is used to estimate the key distribution. Finally, the comparison between proposed protocol and original one is given to show the better performance.**

***Index Terms*—Quantum three pass protocol, quantum key sharing, quantum phase estimation**

I. Introduction

Quantum computation is proved to have possibility to solve the difficult problems that are hard to solve by the classical computation such as: factoring the number into primer factors [1], searching an item from un-ordered database [2], and the security of cryptography [3]. Most important phenomenon of quantum mechanism is quantum entanglement [4], [5], in which involved particles on a quantum state can not be represented independently even they are separated far from each other. Hence, quantum entanglement has been used as the key problems on such research as quantum algorithm, quantum communication, and quantum error correction code [6]. Since many quantum algorithms are proposed and they are proved to have better speed than classical one, the quantum cryptography based on quantum algorithms are discussed [7]. They promise new way in communication which is called quantum communication or quantum network [8]–[11].

Cryptography is the practical and study of techniques for secure communication. Quantum cryptography is a kind of cryptography of using the quantum mechanism advantages to perform cryptography tasks. Since the first quantum cryptography is BB84 which was invented by Mr. Bennett [12], others protocols are developed to use the advantages of quantum mechanism such as quantum ping pong algorithm which use quantum entanglement for secure a direct communication [13], quantum version of the Shamir's protocol called quantum three-passes (QTPP) [14]. The advantage of QTPP is that there is pre-shared keys between parities. The main idea of QTPP is that the secret message is locked by both the keys of Sender and Receiver, then we can called QTPP is double locked protocol. Many researches have improved the original QTPP such as the applications of quantum error correction codes for error correction of QTPP channel at [15], and proposed the multi-photons cryptography at [16].

Quantum phase estimation (QPE) is an advantage technique of quantum computation to approximate the real number to the binary presentation, which is based on the control-NOT transformation and Fourier transformation to find out each bit of binary transform from real number. Since its first application is in the Shor factoring algorithm to find out the period of an oracle function, there are many applications of QPE in quantum algorithms such as HHL algorithm to solve the linear equation in polynomial time at [17], quantum data compression based on principal component analysis [18]. In this research, we use the QPE to improve the QTPP algorithm. The proposed algorithm aims to attach many information bits into the phase part of quantum state, then QTPP is used to the transfer carrier state between parties. The research is organized as follows. In next section, we shortly explain the preliminaries of quantum information. In section 3, the three pass protocol and the quantum three pass protocol, and the quantum phase estimation algorithm are first reviewed. Then, the proposed protocol is explained.

II. Preliminaries

A classical bit is an elementary unit of information; it must be one of two states, conventionally ”0” or ”1”. Classical bits and classical gates are two basic elements that are used in classical computation. Quantum computation uses a quantum bit as the basis unit, and it is denoted as a qubit. Contrary to the classical bit, a qubit can take more than discrete values of ”0” or ”1”. It can also assume all possible linear combinations of them;this is called superposition, which is an important and fundamental property of quantum mechanics. Since the two basis states of quantum information are two column vectors, i.e.,

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ and } |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

A quantum superposition state is denoted as

$$|\varphi\rangle = \beta\,|0\rangle + \gamma\,|1\rangle = \begin{bmatrix} \beta \\ \gamma \end{bmatrix},$$

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

where β and γ are complex numbers that satisfy the equation: $|\beta|^2 + |\gamma|^2 = 1$. Quantum computation operates on its qubits using quantum gates, which are the unitary transformation of quantum states. Then, Pauli matrices, which include the identity matrix $\mathbf{I}$, and three non-identity matrices $\mathbf{X}$, $\mathbf{Z}$, and $\mathbf{Y}$, are considered as the basis generators of all unitary transformations. $P_1 = \{\mathbf{I}, \mathbf{X}, \mathbf{Y}, \mathbf{Z}\}$ is Pauli group for single qubit. Generally, Pauli group P_n for system of n-qubit is n-times tensor-product of single Pauli group P_1.

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

The most important properties of Pauli group is that any two operators from this group are commutative or non-commutative to another. Hence, Pauli operators are used to be the basis for all unitary transformations. Since any classical logical gates can be built up from AND and NOT gate, the set of AND, NOT is called the universal logical gate. In quantum computation, the set of Hadarmard, Controlled-NOT, and Rotation gates are formed the universal quantum gates. All important quantum gates and these logical table are explained in Figure 1.

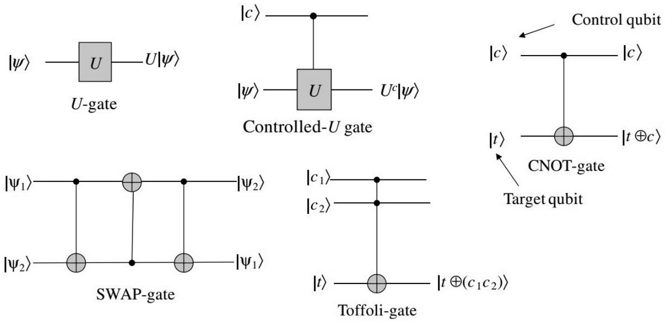

Fig. 1. The important quantum gates.

III. Three Pass Protocol

A. Classical three Pass Protocol

In cryptography, original three pass protocol for sending the messages allows a party to send securely a message to another party without the pre-shared encryption keys. Original three pass protocol was invented by A. Shamir as Figure 2. This classical protocol can be realized utilizing the XOR operator as follows, we assume that the binary message is denoted as M.

1) Sender chooses her secret key K_A and sends to Receiver $K_A \oplus M$.
2) Receiver chooses his secret key K_B and sends to Sender $K_B \oplus (K_A \oplus M)$.
3) Sender applies inversion to her secret from step 1, $K_A \oplus (K_B \oplus (K_A \oplus M)) = K_B \oplus M$ and returns the result to Receiver.
4) Receiver applies the inverse of his secret, $K_B \oplus (K_B \oplus M) = M$, and retrieves the final message M.

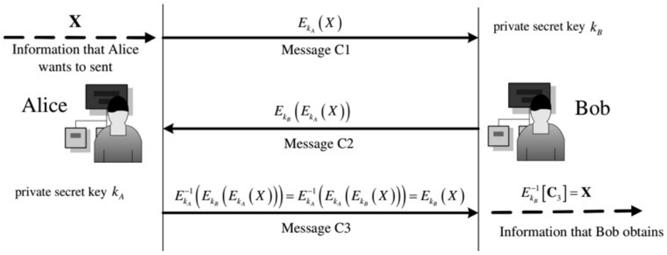
X
Information that Alice wants to sent
Alice
private secret key k_A
$E_{k_A}(X)$
Message C1
$E_{k_B}(E_{k_A}(X))$
Message C2
$E^{-1}_{k_A}(E_{k_B}(E_{k_A}(X))) = E^{-1}_{k_A}(E_{k_A}(E_{k_B}(X))) = E_{k_B}(X)$
Message C3
private secret key k_B
Bob
$E^{-1}_{k_B}[\mathbf{C}_3] = \mathbf{X}$
Information that Bob obtains

Fig. 2. Shamir's three-pass protocol for secrecy sharing.

For original three pass protocol above, it is easy for Eve to retrieve the message by copying of all message exchanged between Sender and Receiver.

$$(K_A \oplus M) \oplus (K_B \oplus (K_A \oplus M)) \oplus (K_B \oplus M) = M \quad (1)$$

In quantum channel, as the advantage of no-cloning in quantum state, we can avoid the above Eve's attack. The quantum three pass is considered in next section.

B. Quantum Three Pass Protocol

In quantum three pass protocol (QTPP), the secret encryption are the unitary transformation which are commutative to each others. Here, we consider the basic rotation gates as follows,

$$\mathbf{U}(\delta) = \begin{bmatrix} \cos\delta & \sin\delta \\ -\sin\delta & \cos\delta \end{bmatrix}. \quad (2)$$

The above unitary matrix is considered as encryption part, δ is called encryption key. As the properties of Rotation gate, the unitary matrix for decryption part can be considered with key $-\delta$. We assume that Sender aims to send a quantum state denoted as $|\varphi\rangle$ to Receiver. The protocol is explained as following steps:

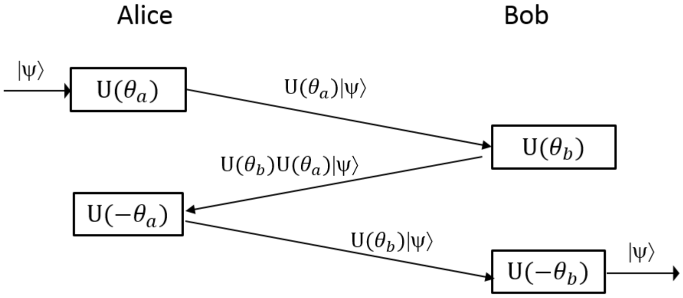

Fig. 3. Quantum three pass protocol.

1) Sender randomly uses encryption key, configures to unitary transformation $\mathbf{U}(\delta_A)$, and teleport quantum state $\mathbf{U}(\delta_A)\,|\varphi\rangle$ to Receiver.
2) Receiver randomly uses encryption key, configures to unitary transformation $\mathbf{U}(\delta_B)$, and teleport quantum state $\mathbf{U}(\delta_B)\mathbf{U}(\delta_A)\,|\varphi\rangle$ back to Sender.
3) Sender decrypts her lock key by applying the minus of key, configures to unitary transformation $\mathbf{U}(\delta_A)^\dagger = \mathbf{U}(-\delta_A)$, and teleport qubit $\mathbf{U}(\delta_B)\,|\varphi\rangle$ back to Receiver.

4) Receiver decrypts his lock key by applying the minus of key, configures to unitary transformation $\mathbf{U}(\delta_B)^\dagger = \mathbf{U}(-\delta_B)$, and receive quantum state $|\varphi\rangle$, which is sent by Sender.

Since, we use three teleportation in total, this protocol is called three pass. In QTPP, no KEY is sent between Sender, Receiver. Sender randomly chooses her own secret key $K_\mathbf{S}$ where $K_\mathbf{S} = \{\delta_\mathbf{S} \mid 0 < \delta_\mathbf{S} \leq \pi\}$ for each teleportation time. And Receiver uses his own secret $K_\mathbf{R}$ where $K_\mathbf{R} = \{\delta_\mathbf{R} \mid 0 < \delta_\mathbf{R} \leq \pi\}$ for each teleportation time. Surely, Eve has small successful of finding out correct keys. Since the keys of Sender and Receiver are different for each round, and each key is used only twice; once for encryption and once for decryption, new key prevents any information which related to original information.

Now, let us assume the bit *b* is a information bit which encrypted into qubit $|b\rangle = |1\rangle$, Sender and Receiver randomly choose their own key where key of Sender is denoted as $K_\mathbf{S}$ and key of Receiver is denoted as $K_\mathbf{R}$. Sender encrypts bit *b* by his own key as following.

$$\begin{aligned} &E_{K_\mathbf{S}}[b] : \\ &\quad U(\delta_\mathbf{S})\,|1\rangle = \begin{bmatrix} \cos\delta_\mathbf{S} & \sin\delta_\mathbf{S} \\ -\sin\delta_\mathbf{S} & \cos\delta_\mathbf{S} \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} \\ &\qquad = \sin\delta_\mathbf{S}\,|0\rangle + \cos\delta_\mathbf{S}\,|1\rangle = |\delta_1\rangle \end{aligned}$$

where *E* denotes encryption part, and output a quantum state, $|\delta_1\rangle$. Sender will be teleported the output to Receiver, and Receiver receives qubit, $|\delta_1\rangle$, encrypts the system by his own key as following.

$$\begin{aligned} &E_{K_\mathbf{R}}[E_{K_\mathbf{S}}[b]] : \\ &\quad U(\delta_\mathbf{R})\,|\delta_1\rangle = \sin(\delta_\mathbf{R}+\delta_\mathbf{S})\,|0\rangle + \cos(\delta_\mathbf{R}+\delta_\mathbf{S})\,|1\rangle = |\delta_2\rangle \end{aligned},$$

where $|\delta_2\rangle$ is a quantum state.

Receiver teleports $|\delta_2\rangle$ to Sender. Sender decrypts $|\delta_2\rangle$ by using his inversion rotation $-\delta_\mathbf{S}$; then, it results $|\delta_3\rangle$, and teleport back to Receiver as following.

$$\begin{aligned} &D_{K_\mathbf{S}}[E_{K_\mathbf{R}}[E_{K_\mathbf{S}}[b]]] : \\ &\quad U(-\delta_\mathbf{S})\,|\delta_2\rangle = \sin(\delta_\mathbf{R})\,|0\rangle + \cos(\delta_\mathbf{R})\,|1\rangle = |\delta_3\rangle \end{aligned}$$

where *D* denoted decryption with key $K_\mathbf{S}$.

Receiver receives $|\delta_3\rangle$ and decrypts it by using $\delta_\mathbf{R}$ with inversion rotation $-\delta_\mathbf{R}$; then, Receiver gets bit *b* which Sender sent, $|1\rangle$, as the following.

$$\begin{aligned} &D_{K_\mathbf{R}}[D_{K_\mathbf{S}}[E_{K_\mathbf{R}}[E_{K_\mathbf{S}}[b]]]] : \\ &U(-\delta_\mathbf{R})\,|\delta_3\rangle = \begin{bmatrix} \cos(-\delta_\mathbf{R}) & \sin(-\delta_\mathbf{R}) \\ -\sin(-\delta_\mathbf{R}) & \cos(-\delta_\mathbf{R}) \end{bmatrix} \begin{bmatrix} \sin(\delta_\mathbf{R}) \\ \cos(\delta_\mathbf{R}) \end{bmatrix} \\ &\qquad = |1\rangle \end{aligned}$$

Finally, Receiver has original bit, $|1\rangle$. Whole protocol is explained in Figure 3.

C. Quantum Phase Approximation Algorithm

The purpose of phase estimation is to estimate the phase of a unitary matrix that apply into the quantum states. In detail, we assume that a unitary matrix and quantum state is given such that

$$\mathbf{U}\,|\varphi\rangle = e^{2\pi i\delta}\,|\varphi\rangle\,. \tag{3}$$

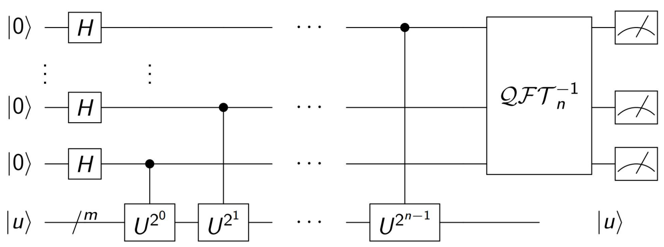

Fig. 4. The quantum circuit for phase estimation.

Then, the algorithm estimates the value of δ with high probability. Phase estimation is frequently used as a subroutine in the most important quantum algorithm, Shor's algorithm, to factor the number into the prime factors [1].

The circuit for phase estimation is given as Figure 4 where the unitary operation $\mathbf{U}$ on *m* qubits, along with a black box(oracle) that can perform $\wedge\mathbf{U}^j$ for any integer j. We obtain the achieved phase by measuring the first registers. In this paper, we use QPE algorithm to receive the *n*-bits approximation to the fraction.

D. A Proposed Protocol for Many Bits Transfer

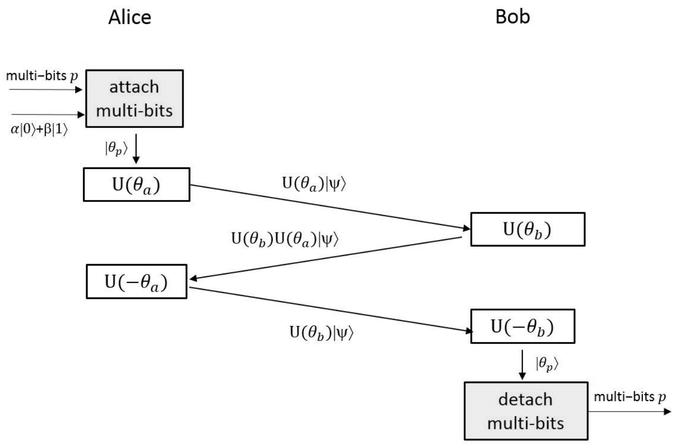

Fig. 5. Many bits transfer based on QTPP

In paper [19], realization of QTPP for authentication from Hill-cipher algorithm is explained. Original information is firstly presented in binary string 1000010011100000011001111. In this protocol, Sender divided information into single bit, and attached it to a single qubit; for example in above strings, $|0\rangle$ will be the second qubit. Then, using the QTPP procedure to exchange each qubit. To send all bit of string 1000010011100000011001111, we need 25 times by using this protocol.

In this research, a new protocol is proposed to attach many bits in the phase part of a carrier qubit, then exchange carrier qubit by using the QTPP procedure. The detail of proposed protocol is as following.

1) Sender chooses five random binary digits, $b_1b_2b_3b_4b_5$ (where b_i is a value from $\{0,1\}$), its decimal value is

denoted as b (a integer number from one to sixty three). Sender, Receiver use QTPP to exchange each bit. This string has the length five, so we need to use QTPP protocol 5 times.

2) In this example, five bits of string is 10000, its decimal value is 16. Then, Sender attaches firstly five digits string 10000 into a carrier qubit as following.

$$\begin{aligned} |\delta_{10000}\rangle &= \tfrac{16}{\sqrt{16^2+b^2}}|0\rangle + \tfrac{b}{\sqrt{16^2+b^2}}|1\rangle \\ &= \sin\delta_{10000}|0\rangle + \cos\delta_{10000}|1\rangle . \end{aligned}$$

Sender, Receiver exchange quantum state $|\delta_{10000}\rangle$ by using QTPP protocol. Receiver finally got correct state, $|\delta_{10000}\rangle$, and Receiver uses basis quantum state $|0\rangle$ for measurement to get probability value, $\frac{16}{\sqrt{16^2+b^2}}$, which tell the probability of seeing final state as basic state $|0\rangle$. By using quantum phase estimation algorithm for the probability, the phase is estimated correctly. Since, Receiver knows value of b, the exact decimal value, 16, will be calculated. Finally, corresponding binary string, 10000 is determined. We conclude that Sender and Receiver have exchanged binary string 10000 successfully.

3) Same procedure of step 2 is used for remaining binary strings 10011, 10000, 01100, 11111. Each of them is encoded into its carrier quantum state as following.

$$\begin{aligned} |\delta_{10011}\rangle &= \tfrac{19}{\sqrt{19^2+b^2}}|0\rangle + \tfrac{b}{\sqrt{19^2+b^2}}|1\rangle \\ &= \sin\delta_{10011}|0\rangle + \cos\delta_{10011}|1\rangle , \\ |\delta_{10000}\rangle &= \tfrac{16}{\sqrt{16^2+b^2}}|0\rangle + \tfrac{b}{\sqrt{16^2+b^2}}|1\rangle \\ &= \sin\delta_{10000}|0\rangle + \cos\delta_{10000}|1\rangle , \\ |\delta_{01100}\rangle &= \tfrac{12}{\sqrt{12^2+b^2}}|0\rangle + \tfrac{b}{\sqrt{12^2+b^2}}|1\rangle \\ &= \sin\delta_{01100}|0\rangle + \cos\delta_{01100}|1\rangle , \\ |\delta_{11111}\rangle &= \tfrac{31}{\sqrt{31^2+b^2}}|0\rangle + \tfrac{b}{\sqrt{31^2+b^2}}|1\rangle \\ &= \sin\delta_{11111}|0\rangle + \cos\delta_{11111}|1\rangle , \end{aligned}$$

respectively.

In paper [19], each bit is attached into a qubit, if string length is 25, so we is required to use QTPP procedure 25 times. In contrast, by using proposed protocol, Sender and Receiver need qubit exchange only ten times. It promises the efficiency of reduction the complexity of quantum system.

IV. Conclusion

The research has improved quantum three-stage protocol from quantum phase estimation algorithm. The proposed protocol not only has the security of the original three pass protocol on own secret keys of each parities, but also has the security of the non cloning theorem of quantum mechanism. In addition, the quantum phase approximation algorithm is used to attach the key in the phase instead of qubit to improve the performance.

References

[1] Shor, P. W. “Algorithms for quantum computation discrete logarithms and factoring.” IEEE Computer Society Press. 124-134 (1994)

[2] Grover, L. “Quantum mechanics helps in searching for a needle in a haystack.” Phys. Rev. Lett. 79, 325 (1997)

[3] Nguyen,D.M., Kim,S. “Multi-Bits Transfer Based on the Quantum Three-Stage Protocol with Quantum Error Correction Codes.” Int. J. Theor. Phys. 58(6) (2019)

[4] M. Zidan et. al. “A Novel Algorithm based on Entanglement Measurement for Improving Speed of Quantum Algorithms.” Appl. Math. Inf. Sci. 12(1), 265-269, (2018).

[5] M. Zidan et. al. “A Quantum Algorithm Based on Entanglement Measure for Classifying Boolean Multivariate function into Novel Hidden Classes.” Results in Physics (2019).

[6] Nguyen, D.M., Kim,S. “Minimal-Entanglement Entanglement-Assisted Quantum Error Correction Codes from Modified Circulant Matrices.” Symmetry vol. 9(7), pp. 122, (2017)

[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] Nguyen,D.M., Kim,S. “Quantum stabilizer codes construction from Hermitian self-orthogonal codes over GF(4).” Journal of Communications and Networks 20 (3), 309-315 (2019)

[9] Nguyen,D.M., Kim,S. “Construction and complement circuit of a quantum stabilizer code with length 7.” in proc. Eighth International Conference on Ubiquitous and Future Networks (ICUFN) (2016)

[10] Nguyen,D.M., Kim,S. “The fog on: Generalized teleportation by means of discrete-time quantum walks on N-lines and N-cycles.” Modern Physics Letters B. 33(23), 1950270 (2019)

[11] Nguyen,D.M., Kim,S. “New Constructions of Quantum Stabilizer Codes Based on Difference Sets.” Symmetry 10 (11), 655 (2018)

[12] Bennett, C.H., Bessette,F., Brassard,G., Salvail, L. and Smolin, J. “Experimental quantum cryptography.” Journal of Cryptology, 5(1), 328, (1992)

[13] Cai, Q. Y. “The ping-pong protocol can be attacked without eavesdropping.” Physical Review Letters, 91, (2003)

[14] Kak, S. “A Three-Stage Quantum Cryptography Protocol.” Found Phys Lett, 19, 293, (2006)

[15] Parakh. A., vanBrandwijk, J. “Correcting Rotational Errors in Three Stage QKD.” 23rd International Conference on Telecommunications (ICT), (2016)

[16] Mandal, S. et al. “Multi-photon implementation of three-stage quantum cryptography protocol.” The International Conference on Information Networking (ICOIN), (2013)

[17] Yonghae, L., Jaewoo, J., and Soojoon, L. “ Hybrid quantum linear equation algorithm and its experimental test on IBM Quantum experience.” Scientific Reports, 9, 4778 (2019)

[18] Yu,C-H., Gao,F., Lin,S., Wang,J. “Quantum data compression by principal component analysis.” Quantum Information Processing, 18(249) (2019).

[19] Abdullah, A.A., Khalaf,R., and Riza,M. “A Realizable Quantum Three-Pass Protocol Authentication Based on Hill-Cipher Algorithm.” Mathematical Problems in Engineering, 2015, (2015)