Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2015, Article ID 481824, 6 pages
http://dx.doi.org/10.1155/2015/481824

Research Article

A Realizable Quantum Three-Pass Protocol Authentication Based on Hill-Cipher Algorithm

Alharith A. Abdullah,[1] Rifaat Khalaf,[2] and Mustafa Riza[3]

[1] *Department of Computer Engineering, Eastern Mediterranean University, Northern Cyprus, Mersin 10, Turkey*
[2] *Department of Mathematics, Eastern Mediterranean University, Northern Cyprus, Mersin 10, Turkey*
[3] *Department of Physics, Eastern Mediterranean University, Northern Cyprus, Mersin 10, Turkey*

Correspondence should be addressed to Alharith A. Abdullah; alharith.khafaji@yahoo.com

Received 23 November 2014; Accepted 10 February 2015

Academic Editor: Kacem Chehdi

A realizable quantum three-pass protocol authentication based on Hill-cipher algorithm is presented by encoded and decoded plaintext using classical Hill-cipher algorithm. It is shown that the encoded message transferred to the particles called quantum state where we assumed that a photon is used as a qubit and after the encoded message is transferred into photons, the polarization of each photon is rotated by an angle θj, which is chosen randomly for each qubit. The sender and receiver agree over a Hill-cipher key, the encryption occurs by utilization of the quantum three-pass protocol (QTPP), the decryption will be illustrated, and an example shows how the algorithm will work. Finally, the security of this algorithm is analyzed in detail.

1. Introduction

Cryptography is the science of protection of private information from unauthorized access, ensuring data integrity, authentication, and other tasks. In order to obtain this goal, a cryptography algorithm is exploited to produce a cryptogram with some additional information, which is called the key. The classical cryptography is divided into two main types depending on the sender and receiver, where the first type is symmetrical system when sender and receiver use the same key and second type is asymmetrical system when sender and receiver use a different key. The one time pad algorithm also belongs to classical cryptography [1]. The quantum cryptography is an emerging technology based on quantum mechanics, the phenomena of light and the properties of light. The quantum cryptography was developed in 1984 by a physicist called Bennett where he proposed unconditionally secure quantum key distribution protocol BB84. This protocol allows secure communication between parties who do not share secret information initially [2], based on the uncertainty principle, and was proven scientifically in 1992 by [3], when it was shown that the processes of generating a key bit sequence in quantum key distribution protocol BB84 is nondeterministic. Lately [4] showed that the deterministic quantum key distribution is proposed where the quantum secure direct communication is implemented by exchanging single photons with classical channel. The Ping-Pong quantum secure direct communication uses the entanglement which is proposed in [5]. In [6, 7] the weakness of the Ping-Pong scheme was found and it was subsequently improved. A quantum secure direct communication protocol using single photons is proposed by [8, 9]. Quantum dense key distribution utilizes quantum key distribution and quantum dense coding [10] to prove the key distribution improvement on the capacity of transmission [11–13]. In 2002 it has been presented that a new kind of quantum cryptography protocol is based on Shamir's three-pass protocol of classical cryptography [14], and then the quantum three-pass protocol (QTPP) based on quantum superposition state is proposed [15] showing that there can be no key shared between the sender and receiver unlike the BB84 protocol. Throughout the subsequent years, the science began to evolve rapidly and significantly. Recently, quantum encryption algorithm is proposed and it is noticed that the quantum encryption algorithm is similar to the classical encryption algorithm except that the quantum algorithm is based on the quantum laws and the classical algorithms are based on the mathematical laws [16–20]. The development in the field of the quantum computation may become a threat to traditional encryption systems because of algorithms such as Shor's quantum factoring algorithms, discrete algorithms, and the quantum Grover's searching algorithms. Thus the researchers should look for designing new algorithms to resist the attacks of quantum algorithms because it is significantly important and necessary to protect the information with the progress made in this field. Because of the important characteristics which are characterized by quantum algorithms that distinguish them from classical algorithms where the opponent can be detected in the case of quantum easily, the nonorthogonal quantum states cannot be reliably distinguished [21]. Additionally, an unconditionally secure algorithm in practical is also significant to the classical information protection. Therefore the quantum algorithms are the best candidates to accommodate the current needs. This paper will address realizable quantum three-pass protocol authentication based on Hill-cipher algorithm. The planning of the paper is as follows. In Section 1 the classical cryptography and quantum cryptography is reviewed briefly. Section 2 discusses a quantum three-pass protocol and how it works. Section 3 presents the classical Hill-cipher algorithm. In Section 4 the proposed Hill-cipher algorithm based on quantum three-pass protocol (QTPP) is discussed and the proposed algorithm in simple example in Section 5 was applied. Finally, the paper is finished off with a security analysis and the conclusions in Sections 6 and 7, respectively.

2. Quantum Three-Pass Protocol (QTPP)

In recent years, three-pass protocol (TPP) has been widely used in many applications, for instance, cryptography. The quantum three-pass protocol is a new addition to the protocols of the quantum cryptography protocol and depends mainly on Shamir's three-pass protocol of classical cryptography. Featured in this protocol is that it uses only the quantum channel unlike the other quantum protocols that use the quantum channel and classical channel. The procedure of this protocol is using the photon as a qubit; therefore each classical bit is encrypted to the quantum bit. After the classical bit is encrypted to the photon, the polarization for the photon is rotated by an angle θj, which is chosen randomly for each qubit. The rotation operation is represented as

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

This operation can be considered in encryption and the angle θj represents the encryption key, while the rotation operation can be considered in decryption with the angle $-\theta j$. In the quantum three-pass protocol there is no shared key between the sender and receiver; the sender generates its own secret $K_{\theta S}$ where ($K_{\theta S} = \{\theta_S \mid 0 \le \theta_S < \pi\}$) for each session. And the receiver generates its own secret key $K_{\theta R}$ where ($K_{\theta R} = \{\theta_R \mid 0 \le \theta_R < \pi\}$) for each session. Certainly the opponent never discovered these keys. For n-qubits, the key for the sender and the receiver changed with each qubit and each key is used only twice by the generator (once for encryption and once for decryption) which continued 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 the plaintext P is single photon encrypted to the qubit as $P = |1\rangle$, the sender and receiver generate their own key, key of the sender = $K_{\theta S}$, and key of the receiver = $K_{\theta R}$. The sender encrypts the plaintext P with its generation key as the following:

$$\begin{aligned} & E_{K_{\theta S}}[P] : R(\theta_S)\,|1\rangle \\ & = \begin{bmatrix} \cos\theta_S & \sin\theta_S \\ -\sin\theta_S & \cos\theta_S \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \sin\theta_S\,|0\rangle + \cos\theta_S\,|1\rangle = |\emptyset_1\rangle, \end{aligned} \tag{2}$$

where E is the encryption with the sender key $K_{\theta S}$, and the resulting is the superposition state $|\emptyset_1\rangle$ where the sender will send it to the receiver. The receiver receives the photon in $|\emptyset_1\rangle$ and encrypts it with its own key as the following:

$$\begin{aligned} & E_{K_{\theta R}}\left[E_{K_{\theta S}}[P]\right] : R(\theta_R)\,|\emptyset_1\rangle \\ & \quad = \sin(\theta_R + \theta_S)\,|0\rangle + \cos(\theta_R + \theta_S)\,|1\rangle = |\emptyset_2\rangle, \end{aligned} \tag{3}$$

where $|\emptyset_2\rangle$ is the superposition state. The receiver sends $|\emptyset_2\rangle$ back to the sender. The sender receives $|\emptyset_2\rangle$ and decrypts it by using the angle θ_S but with rotation of $-\theta_S$ because there are decrypts in this case; then the results $|\emptyset_3\rangle$ send it back to the receiver as the following:

$$\begin{aligned} & D_{K_{\theta S}}\left[E_{K_{\theta R}}\left[E_{K_{\theta S}}[P]\right]\right] \\ & \quad = E_{K_{\theta R}}[P] : R(-\theta_S) = \sin\theta_R\,|0\rangle + \cos\theta_R\,|1\rangle = |\emptyset_3\rangle, \end{aligned} \tag{4}$$

where D is the decryption with the sender key $K_{\theta S}$. The receiver receives $|\emptyset_3\rangle$ and decrypts it by using the angle θ_R but with rotation of $-\theta_R$ because there are decryptions in this case; then the receiver gets the plaintext P that the sender sends it $|1\rangle$ as the following:

$$\begin{aligned} & D_{K_{\theta R}}\left[E_{K_{\theta S}}[P]\right] : R(-\theta_R)\,|\emptyset_3\rangle \\ & \quad = \begin{bmatrix} \cos -\theta_R & \sin -\theta_R \\ -\sin -\theta_R & \cos -\theta_R \end{bmatrix} \begin{bmatrix} \sin\theta_R \\ \cos\theta_R \end{bmatrix} = |1\rangle. \end{aligned} \tag{5}$$

Finally, the receiver has the plaintext $j1i$. The whole procedure of the protocol is in Figure 1 and all of the protocol is proposed, presented, and developed from [14, 15, 22].

3. Classical Hill-Cipher Algorithm

It is known that the substitution ciphers which use letter-by-letter are nonresistant and insecure at the attack and in the case of frequency analysis. The block cipher plaintext on the other hand is divided into groups of adjacent letters, which are fixed-length m; then each group turns or encrypts to the other groups of letters m depending on the key used in each group. It is considered as the best use of the letters

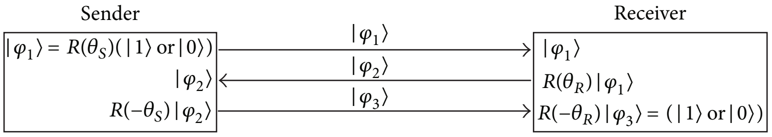

Sender
$|\varphi_1\rangle = R(\theta_S)(|1\rangle \text{ or } |0\rangle)$
$|\varphi_2\rangle$
$R(-\theta_S)|\varphi_2\rangle$
$|\varphi_1\rangle$
$|\varphi_2\rangle$
$|\varphi_3\rangle$
Receiver
$|\varphi_1\rangle$
$R(\theta_R)|\varphi_1\rangle$
$R(-\theta_R)|\varphi_3\rangle = (|1\rangle \text{ or } |0\rangle)$

Figure 1: Quantum three-pass protocol procedure.

as compensatory and individually for each character, similar to substitution ciphers. If the length of m is large enough, then the block cipher will be resistant and it would become extremely difficult to attacker and to carry out the frequency analysis. The first encryption system based on a simple block cipher using more than two letters in the same group is Hill-cipher. Hill-cipher was invented by the mathematician Lester Hill [23, 24]. The Hill-cipher is an example of symmetric encryption. Hill-cipher relies heavily on the operation of matrices, where it multiplies a plaintext vector by a key matrix to get the ciphertext. It is very attractive due to its simplicity and high throughput [25, 26]. The basic idea of the Hill-cipher is that the letter of the text explicit in the blocks of length m is supposed that the matrix key $(m\times m)$, after that each block of plaintext letters are converted to the integer matrix depending on the alphabet of selected then multiplied by the $(m\times m)$ key matrix. The results are then converted back to letters and the ciphertext message is produced. The key of the Hill-cipher must be a square matrix $(m \times m)$ and must have invertible matrix key. In order to guarantee that the key matrix has the invertible key, the determinant of key must be relatively prime to the modulus N where N is alphabet cardinality to satisfy this; it is required that

$$\gcd(\det(K) \bmod N, M) = 1. \tag{6}$$

In the formula M is block size and N is alphabet cardinality being selected as positive integers; $\det(K)$ is the determinant of key and gcd is the greatest common divisor. The Hill-cipher has the property of diffusion where a change in a single letter in the plaintext leads to several changes in the letters of the ciphertext and this feature makes it much more difficult and complicated when using frequency analysis. And also the Hill-cipher has the confusion property and with this property each letter of the ciphertext depends on several parts of the key. In addition to that, the key cannot be computed part by part. When it is supposed that the sender wants to exchange information with the receiver using the Hill-cipher encryption algorithm, sender shares securely a nonsingular invertible key matrix K. If A wants to encrypt a plaintext vector P, the receiver gets the ciphertext vector C as follows:

$$C = K \cdot P \bmod N. \tag{7}$$

The receiver decrypts the ciphertext vector C by

$$P = K^{-1} \cdot C \bmod N, \tag{8}$$

where K^{-1} is the key inverse and N is the alphabet cardinality. For existence of K^{-1}, conditions that were stated before should be satisfied.

4. Hill-Cipher Algorithm Based on Quantum Three-Pass Protocol

For instance, the distinctive feature in the quantum three-pass protocol (QTPP) is that there is no need for the classical channel like the BB84 but there is a need for only quantum channel, so that all the information and data that deals with this protocol is quantum information. It is known that the exchange, storage, and processing of information are carried out by using elementary entities called bits, where these bits are represented by discrete values 0 and 1. Recently with the tremendous development in the field of information, communication, and cryptography, these classical bits are carried by light pulses, corresponding to macroscopic packets of photons, allowing a classical description of their behavior and propagation. Physicists have realized that individual quantum objects, for instance, photons, could also be employed to deal with another kind of information. Here information is no longer encoded on the number of involved photons, but individual photons merely serve as carriers and quantum information and photons are encoded on their quantum properties, like polarization or time-bins of arrival. Indeed, by selecting two orthogonal states spanning the Hilbert space, $|0\rangle$ and $|1\rangle$ now encode the 0 and 1 values of the quantum bit (qubit), and quantum superposition makes it possible to create states of the form:

$$|\emptyset\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\ , \tag{9}$$

where $\alpha, \beta \in C$ and $|\alpha^2| + |\beta^2| = 1$.

Quantum superposition is very important for quantum communication protocols. In our study, it is assumed that a photon is used as a qubit. A photon is used as a qubit and one polarization base set horizontal or vertical to represent a classical two-level system. A horizontally polarized photon represents logic zero, $|0\rangle = \begin{pmatrix}1 & 0\end{pmatrix}^T$, and a vertically polarized photon represents logic one, $|1\rangle = \begin{pmatrix}0 & 1\end{pmatrix}^T$. Now, after the sender implements the classical Hill-cipher algorithm and encodes the plaintext, each letter in encoded plaintext is converted to the binary code. After the conversion of the letters to the binary code, all the information binary bit is encrypted into a single particle called quantum bit or encoded plaintext qubits $|E\rangle$ and then sends all the quantum bits to the receiver by using the quantum three-pass protocol (QTPP) as follows. First, sender and receiver generate their session keys $K_{\theta S}$ and $K_{\theta R}$. Sender encrypts the encoded plaintext qubits $|E\rangle$ with its encryption key $K_{\theta S}$:

$$|\emptyset_1\rangle = |E\rangle \cdot K_{\theta S}. \tag{10}$$

Sender sends the resulting state to receiver. Receiver receives the photon and encrypts it with its key $K_{\theta R}$. The

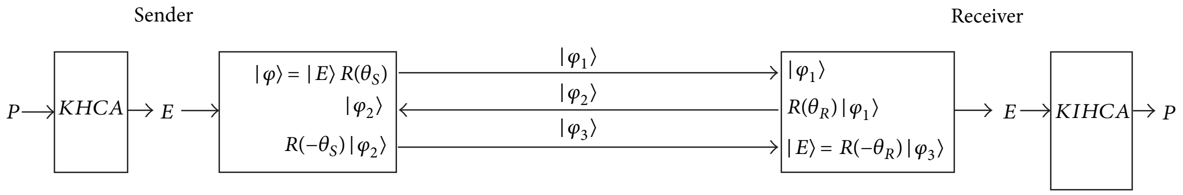

Sender
Receiver
P
$KHCA$
E
$|\varphi\rangle = |E\rangle\, R(\theta_S)$
$|\varphi_2\rangle$
$R(-\theta_S)\,|\varphi_2\rangle$
$|\varphi_1\rangle$
$|\varphi_2\rangle$
$|\varphi_3\rangle$
$|\varphi_1\rangle$
$R(\theta_R)\,|\varphi_1\rangle$
$|E\rangle = R(-\theta_R)\,|\varphi_3\rangle$
E
$KIHCA$
P

Figure 2: Quantum three-pass protocol authentication based on hill-cipher algorithm.

Table 1: Correspondence table for encoding.

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*
0	1	2	3	4	5	6	7	8	9	10	11	12
N	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
13	14	15	16	17	18	19	20	21	22	23	24	25

resulting state is still a superposition state and the receiver sends it back to sender:

$$\left|\emptyset_2\right\rangle = \left|\emptyset_1\right\rangle \cdot K_{\theta R}. \tag{11}$$

The sender receives and decrypts it by rotating it back with the angle $K_{-\theta S}$ and sends the resulting superposition state to receiver again:

$$\left|\emptyset_3\right\rangle = \left|\emptyset_2\right\rangle \cdot K_{-\theta S}. \tag{12}$$

Receiver receives and decrypts it by rotating it back with the angle $K_{-\theta R}$:

$$\left|E\right\rangle = \left|\emptyset_3\right\rangle \cdot K_{-\theta R}. \tag{13}$$

This procedure continues with all the quantum bits of the encoded plaintext qubits $|E\rangle$ until the receiver gets whole encoded plaintext qubits $|E\rangle$, after that convert all of the binary code to letters which are then decoded to the plaintext by using the key inverse of Hill-cipher algorithm (KIHCA) where the sender and receiver agree on the key of Hill-cipher algorithm (KHCA). Now the receiver has the original plaintext. The whole procedure shown in Figure 2.

5. Example

"HELP" is encoded for this example. The first step includes the choice of an invertible modulo 26 $n \times n$ matrix, for a hill 2-cipher 2 × 2 matrix is used:

$$K = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}. \tag{14}$$

The next step; plaintext are grouped into pairs and replaced with the corresponding numerical value from Table 1.

Now the corresponding numerical values are

$$\begin{bmatrix} H \\ E \end{bmatrix} = \begin{bmatrix} 7 \\ 4 \end{bmatrix}, \qquad \begin{bmatrix} L \\ P \end{bmatrix} = \begin{bmatrix} 11 \\ 15 \end{bmatrix}. \tag{15}$$

Table 2: Correspondence table for the binary code.

P	*M*	*P*	*T*
01111	01100	01111	10011

And by using the equation $C = K \cdot P \bmod N$ we get

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \cdot \begin{bmatrix} 7 & 11 \\ 4 & 15 \end{bmatrix} = \begin{bmatrix} 15 & 41 \\ 12 & 45 \end{bmatrix} \bmod 26 \Longrightarrow C = \begin{bmatrix} 15 & 15 \\ 12 & 19 \end{bmatrix}. \tag{16}$$

So the ciphertext C is

$$C_1 = \begin{bmatrix} 15 \\ 12 \end{bmatrix} = \begin{bmatrix} P \\ M \end{bmatrix}, \qquad C_2 = \begin{bmatrix} 15 \\ 19 \end{bmatrix} = \begin{bmatrix} P \\ T \end{bmatrix}. \tag{17}$$

So the encoded plaintext is "PMPT", and then each letter in encoded plaintext is converted to the binary code as in Table 2.

After converting the letters to the binary code we encrypt all the information binary bit into a single particle called quantum bit and then send all the quantum bits to the receiver by using the QTPP as follows. The sender first sends quantum bit which is $|1\rangle$. After that it encrypts it to the photons by using the angle for the sender; for instance, in this example we will use $\theta_S = 30$; then $\emptyset_1$ is

$$\begin{aligned} \emptyset_1 &= \begin{bmatrix} \cos 30 & \sin 30 \\ -\sin 30 & \cos 30 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} \\ &= \begin{bmatrix} 0.5 \\ 0.866 \end{bmatrix} = 0.5\,|0\rangle + 0.866\,|1\rangle . \end{aligned} \tag{18}$$

The receiver receives $\emptyset_1$ and generates its session angle; for instance, in this example we will use $\theta_R = 45$; then $\emptyset_2$ is

$$\begin{aligned}\emptyset_2 &= \begin{bmatrix} \cos 45 & \sin 45 \\ -\sin 45 & \cos 45 \end{bmatrix} \cdot \begin{bmatrix} 0.5 \\ 0.866 \end{bmatrix} \\ &= \begin{bmatrix} 0.97 \\ 0.26 \end{bmatrix} = 0.97\,|\,0\rangle \; + 0.26\,|\,1\rangle \; .\end{aligned} \tag{19}$$

The resulting state $\emptyset_2$ is sent it back to the sender. The sender receives and decrypts it by rotating it back with the angle $-\emptyset_S = -30$ and sends the resulting superposition state $\emptyset_3$ to the receiver as follows:

$$\begin{aligned}\emptyset_3 &= \begin{bmatrix} \cos -30 & \sin -30 \\ -\sin -30 & \cos -30 \end{bmatrix} \cdot \begin{bmatrix} 0.97 \\ 0.26 \end{bmatrix} \\ &= \begin{bmatrix} 0.71 \\ 0.71 \end{bmatrix} = 0.71\,|\,0\rangle \; + 0.71\,|\,1\rangle \; .\end{aligned} \tag{20}$$

The receiver gets $\emptyset_3$ and decrypts it by rotating it back with the angle $-\theta_R = -45$; then the receiver has the original ciphertext "PM" as follows:

$$\begin{bmatrix} \cos -45 & \sin -45 \\ -\sin -45 & \cos -45 \end{bmatrix} \cdot \begin{bmatrix} 0.71 \\ 0.71 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{21}$$

And this represent state $|1\rangle$ that the sender sends it, and then continues with the second quantum bit, which is $|0\rangle$ by using same procedure:

$$\begin{aligned}\emptyset_1 &= \begin{bmatrix} \cos 30 & \sin 30 \\ -\sin 30 & \cos 30 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ &= \begin{bmatrix} 0.866 \\ -0.5 \end{bmatrix} = 0.866\,|\,0\rangle \; - 0.5\,|\,1\rangle \; , \\ \emptyset_2 &= \begin{bmatrix} \cos 45 & \sin 45 \\ -\sin 45 & \cos 45 \end{bmatrix} \cdot \begin{bmatrix} 0.866 \\ -0.5 \end{bmatrix} \\ &= \begin{bmatrix} 0.26 \\ -0.97 \end{bmatrix} = 0.26\,|\,0\rangle \; - 0.97\,|\,1\rangle \; , \\ \emptyset_3 &= \begin{bmatrix} \cos -30 & \sin -30 \\ -\sin -30 & \cos -30 \end{bmatrix} \cdot \begin{bmatrix} 0.26 \\ -0.97 \end{bmatrix} \\ &= \begin{bmatrix} 0.71 \\ -0.71 \end{bmatrix} = 0.71\,|\,0\rangle \; - 0.71\,|\,1\rangle \; , \\ &\begin{bmatrix} \cos -45 & \sin -45 \\ -\sin -45 & \cos -45 \end{bmatrix} \cdot \begin{bmatrix} 0.71 \\ -0.71 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}.\end{aligned} \tag{22}$$

And this represent state $|0\rangle$ that the sender sends it, and so on so forth same way the sender sends the rest of quantum bits. Finally, the receiver decodes the whole quantum bits and converts it back to the binary to get the ciphertext. Eventually, the plaintext is obtained by using the equation $P = K^{-1} \cdot C \bmod N$.

Where

$$\begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix} \cdot \begin{bmatrix} 15 & 15 \\ 12 & 19 \end{bmatrix} = \begin{bmatrix} 111 & 167 \\ 108 & 171 \end{bmatrix} \bmod 26 \Longrightarrow P = \begin{bmatrix} 7 & 11 \\ 4 & 15 \end{bmatrix} \tag{23}$$

which is "HELP."

6. Security Analysis

The security of the proposal is directly based on QTPP. We now give a brief argument provided for the security of the proposal. Given a ciphertext $|\emptyset_1\rangle = |E\rangle \cdot K_{\theta S}$, an opponent cannot drive $|E\rangle$ without the information of $K_{\theta S}$. Given a ciphertext $|\emptyset_2\rangle = |E\rangle \cdot K_{\theta S} \cdot K_{\theta R}$, an opponent cannot drive $|E\rangle$ without information of $K_{\theta S}$ and $K_{\theta R}$. Given a ciphertext $|\emptyset_3\rangle = |E\rangle \cdot K_{\theta S} \cdot K_{\theta R} \cdot K_{-\theta S}$, an opponent cannot drive $|E\rangle$ without the information of $K_{\theta S}, K_{\theta R}$, and $K_{-\theta S}$. Furthermore, if the opponent manages to obtain the multiple duplications of the superposition state and measure them, opponent also cannot determine the qubit $|E\rangle$. For example, if the opponent obtains $\cos\theta_S|0\rangle - \sin\theta_S|1\rangle$ and knows each qubit, he/she can still not determine $|E\rangle$ because there are different sender angles. If we assumed that an opponent can drive the qubit $|E\rangle$, he/she still cannot find the plaintext without the information of the Hill-cipher key matrix.

Another possible attempt to get information from the transmitted data is that opponent may entangle the intercepted data with opponent's qubit, which is called individual particle attack [27]. However, opponent will still observe 0 or 1 randomly. For example, opponent can apply controlled-NOT (C-NOT) operation to the transmitted data as the control bit and its qubits 0 and 1 as the target bit. In this case, sender and receiver cannot detect the eavesdropping since this operation does not change the state of the transmitted qubit. Using this technique, opponent can entangle its three qubits with three transmitted data qubits (i.e., Sender → Receiver, Receiver → Sender, and Sender → Receiver) and apply unitary operations with its three qubits in order to try to get the plaintext. However, opponent cannot retrieve the plaintext data bit, because opponent does not know the states of entangled particles and the angles of sender and receiver.

7. Conclusion

The quantum technology is new and being improved, specifically in the field of quantum cryptography. At the same time, the most of the world is challenging the fact that science and technology is advancing and sooner or later the quantum computers will take their part in this world. So it is not possible to treat or transfer all of the existing information in the form of classical form, which is more familiar to the people in quantum information, and preshared classical since the security cannot be guaranteed. Therefore a realizable quantum three-pass protocol authentication based on Hill-cipher algorithm is proposed. The classical encryption algorithm is represented by Hill-cipher algorithm and presented new protocol where this protocol work relies on the principle of the classical three-pass protocol and the properties of quantum mechanism. This protocol has many distinctive properties which are characterized by the rest of the quantum protocols where it can be used to determine quantum key distribution and used to data transmission utilizing classical existing error correcting codes. Also with this protocol there is no need for a classical channel like the BB84 protocol, which is more common in this area. Therefore the protocol can detect an opponent when under any attack. Furthermore, as long as the measurement base stays still during the session, the protocol does not require precise base alignments. The security and the physical implementation of the proposed algorithm are analyzed in detail and it is concluded that the new proposed algorithm can prevent the quantum attacks as well as classical attacks. Managing to prevent two kinds of attacks and protecting the information from new prying manner is the goal. It should be mentioned that improvements can be made to the algorithm by the users in order to make it more powerful and secure.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] W. Stallings, *Cryptography and Network Security: Principles and Practice*, Pearson Custom Computer Science Series, Prentice Hall, 5th edition, 2010.

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, vol. 175, New York, NY, USA, 1984.

[3] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of Cryptology*, vol. 5, no. 1, pp. 3–28, 1992.

[4] A. Beige, B.-G. Englert, C. Kurtsiefer, and H. Weinfurter, "Secure communication with a publicly known key," *Acta Physica Polonica A*, vol. 101, no. 3, pp. 357–368, 2002.

[5] K. Boström and T. Felbinger, "Deterministic secure direct communication using entanglement," *Physical Review Letters*, vol. 89, no. 18, pp. 187902–187905, 2002.

[6] A. Wójcik, "Eavesdropping on the 'ping-pong' quantum communication protocol," *Physical Review Letters*, vol. 90, no. 15, Article ID 157901, 2003.

[7] Q.-Y. Cai, "The ping-pong protocol can be attacked without eavesdropping," *Physical Review Letters*, vol. 91, 2003.

[8] F.-G. Deng and G. L. Long, "Secure direct communication with a quantum one-time pad," *Physical Review A: Atomic, Molecular, and Optical Physics*, vol. 69, no. 5, Article ID 052319, 2004.

[9] H. Hoffmann, K. Bostroem, T. Felbinger, F.-G. Deng, and G. L. Long, "Comment on 'Secure direct communication with a quantum one-time pad,'" *Physical Review A—Atomic, Molecular, and Optical Physics*, vol. 72, no. 1, Article ID 016301, 2005.

[10] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, "Dense coding in experimental quantum communication," *Physical Review Letters*, vol. 76, no. 25, pp. 4656–4659, 1996.

[11] I. P. Degiovanni, I. R. Berchera, S. Castelletto et al., "Quantum dense key distribution," *Physical Review A: Atomic, Molecular, and Optical Physics*, vol. 69, no. 3, 2004.

[12] Y. Xia and H.-S. Song, "Controlled quantum secure direct communication using a non-symmetric quantum channel with quantum superdense coding," *Physics Letters A*, vol. 364, no. 2, pp. 117–122, 2007.

[13] J. Liu, Y.-M. Liu, Y. Xia, and Z.-J. Zhang, "Revisiting controlled quantum secure direct communication using a non-symmetric quantum channel with quantum superdense coding," *Communications in Theoretical Physics*, vol. 49, no. 4, pp. 887–890, 2008.

[14] L. Yang, L.-A. Wu, and S. Liu, "Quantum three-pass cryptography protocol," in *Quantum Optics in Computing and Communications*, vol. 4917 of *Proceedings of the SPIE*, pp. 106–111, Shanghai, China, October 2002.

[15] Y. Kanamori and S. Moo-Yoo, "Quantum three-pass protocol: key distribution using quantum superposition states," *International Journal of Network Security & Its Applications*, vol. 1, no. 2, 2009.

[16] N.-R. Zhou and G.-H. Zeng, "A realizable quantum encryption algorithm for qubits," *Chinese Physics*, vol. 14, no. 11, pp. 2164–2169, 2005.

[17] N. R. Zhou, Y. Liu, G. H. Zeng, J. Xiong, and F. Zhu, "Novel qubit block encryption algorithm with hybrid keys," *Physica A: Statistical Mechanics and its Applications*, vol. 375, no. 2, pp. 693–698, 2007.

[18] T. Hua, J. Chen, D. Pei, W. Zhang, and N. Zhou, "Quantum image encryption algorithm based on image correlation decomposition," *International Journal of Theoretical Physics*, vol. 54, no. 2, pp. 526–537, 2015.

[19] N. Sandip and A. Kumar, "Network security based on quantum cryptography & multiqubit hadamard matrices," *Global Journal of Computer Science and Technology*, vol. 11, no. 12, 2011.

[20] Z. Cao and L. Liu, "Improvement of one quantum encryption scheme," in *Proceedings of the IEEE International Conference on Intelligent Computing and Intelligent Systems (ICIS '10)*, vol. 1, pp. 335–339, Xiamen, China, 2010.

[21] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2010.

[22] Y. Kanamori, S.-M. Yoo, and M. Al-Shurman, "A quantum no-key protocol for secure data communication," in *Proceedings of the 43rd Annual Association for Computing Machinery Southeast Conference (ACM-SE '05)*, vol. 2, pp. 292–293, ACM, New York, NY, USA, March 2005.

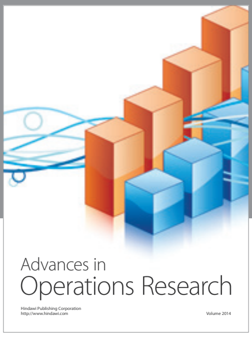
[23] L. S. Hill, "Cryptography in an algebraic alphabet," *The American Mathematical Monthly*, vol. 36, no. 6, pp. 306–312, 1929.

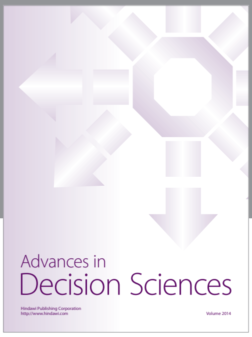
[24] L. S. Hill, "Concerning certain linear transformation apparatus of cryptography," *The American Mathematical Monthly*, vol. 38, no. 3, pp. 135–154, 1931.

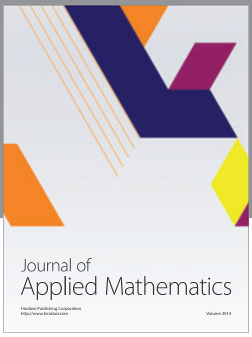
[25] S. Saeednia, "How to make the hill cipher secure," *Cryptologia*, vol. 24, no. 4, pp. 353–360, 2000.

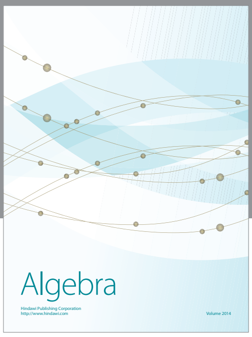
[26] J. Overbey, W. Traves, and J. Wojdylo, "On the keyspace of the hill cipher," *Cryptologia*, vol. 29, no. 1, pp. 59–72, 2005.

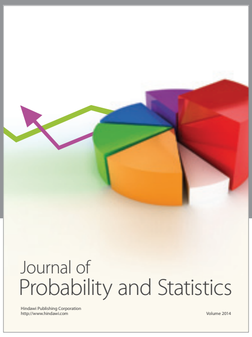
[27] D. Bouwmeester, A. Ekert, and A. Zeilinger, *The Physics of Quantum Information*, Springer, New York, NY, USA, 2000.


Advances in
Operations Research

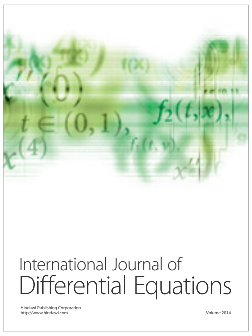

Advances in
Decision Sciences


Journal of
Applied Mathematics

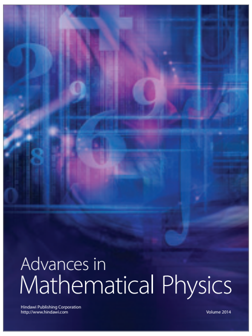

Algebra

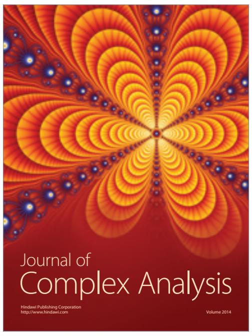

Journal of
Probability and Statistics

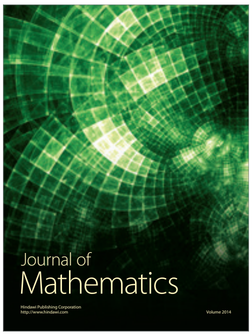
The Scientific
World Journal

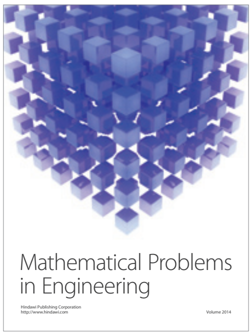

International Journal of
Differential Equations

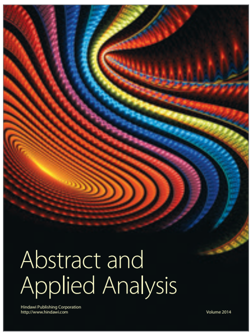
International Journal of
Combinatorics

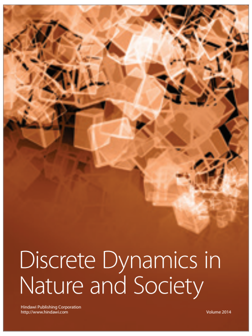

Advances in
Mathematical Physics

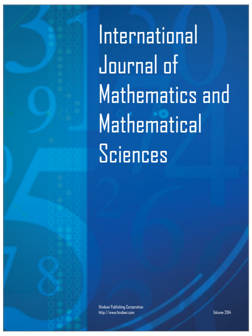

Journal of
Complex Analysis


Journal of
Mathematics


Mathematical Problems
in Engineering

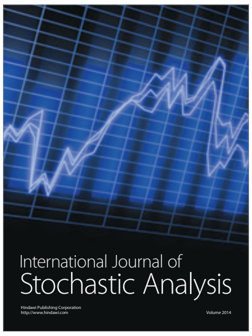

Abstract and
Applied Analysis


Discrete Dynamics in
Nature and Society


International
Journal of
Mathematics and
Mathematical
Sciences

Journal of
Discrete Mathematics

Journal of
Function Spaces


International Journal of
Stochastic Analysis

Journal of
Optimization