International Journal of Computer Networks and Communications Security

VOL. 3, NO. 7, JULY 2015, 283–290
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

Expand the Quantum Cipher-text Space by Using a Superposition Key

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

[1] Department of Computer Engineering, Eastern Mediterranean University, Gazimagusa, North Cyprus, Turkey

[2] Department of Mathematics, Eastern Mediterranean University, Gazimagusa, North Cyprus, Turkey

[3] Department of Pysics, Eastern Mediterranean University, Gazimagusa, North Cyprus, Turkey

E-mail: [1]alharith.khafaji@yahoo.com

ABSTRACT

In this paper an improvement of quantum encryption algorithm based on superposition state is proposed. The whole process including the encryption algorithm where the superposition state and bit-swapping are introduced, makes the quantum ciphertext space to expand broadly and allows the transmission of the necessary information and the decryption that is illustrated here. Finally, a short security analysis is given to show the difference between the proposed algorithm and its classical counterpart.

Keywords: *Quantum Cryptography, Quantum Computation, Quantum Encryption Algorithm, Superposition.*

1 INTRODUCTION

Advance in quantum computation is always considered as threat to the classical encryption systems. The most comprehensive summary in the field of quantum computation is given by [1]. Taking into account the block encryption algorithms; These algorithms are generally very easy to implement and they depend on long keys to ensure an appropriate level of security. Obviously, the length of the key is important to make a brute force attack very diffcult. So a review on the basics of a brute force or extensive search attack is provided. The diffculties of this attacking method are based on the combinatorics. The number of possible keys of a key with a length of n-bit can be easily calculated. So when it is intended to test all possible keys to decrypt a cypher text encrypted using a block cipher, the complexity for this attack is 2n, i.e. exponential. So the longer the key is, the lower the probability to find the key is. If a key of 128 bits length is taken, the number of possible keys becomes 2128 ≈1038. Assuming that testing one key takes 1 nanosecond, it will take 1029 years on a single processor machine. If it is assumed that there are currently 1020 processors available on the world and if all of them could be used, it still would take 109 years using all available processors in the world. So clearly the key length significantly determines the success of the brute force attack probability [2]. On the other hand, it increases also the number of operations for encryption and decryption. What is the difference in using a quantum bit using the same computational basis $\{|0\rangle, |1\rangle\}$? As any quantum bit can be written as superposition of the computational basis vectors, following equation 1 is obtained.

$$|\mathrm{A}\rangle = \alpha|0\rangle + \beta|1\rangle \qquad (1)$$

Where $\alpha, \beta \in \mathbb{C}$ and $|\alpha^2| + |\beta^2| = 1.$ If this infinite set is considered , it is easily observable that every point on the circle is an accumulation point, whereas the set of integers has no accumulation point, i.e. in an open interval around a point x of this set, there are infinite points, which is not the case in the case of integer numbers. So evidently one q-bit is sufficient to store a key that is combinatorially inaccessible. The only restriction in this case is that every transmission channel has a certain noise and therefore dependence on that noise and the error correction are the only limiting properties for the key and its transmission. If this is neglected, one q-bit is sufficient to prevent any combinatorially motivated brute force attack, as the number of possible keys is infinite. This is due to the fact that, every point in the set is an accumulation point. The mathematical theory states that the key space is infinite, but according to [3] there is an is an upper bound to the information in the universe contradicting with the mathematical claim that the quantum key space is infinite. Thus, despite of the mathematical reasons, it can be said that the quantum key space is considerably large but not infinite. From the birth of the idea quantum computation it has been clear that the nature of quantum measurement would play an important role in the secure transmission of information. So, it is self evident that one of the first significant contributions to quantum computation would be a way to prevent eavesdropping. The BB84 protocol proposed by [4] allows secure quantum key distribution over an insecure channel. There are many aspects of quantum computation related to security. One aspect is illuminated by Peter W. Shor by his groundbreaking works on polynomial time algorithms for prime number factorisation [5,6,7]. This work show how vulnerable classical public key encryption algorithms become if the prime number factorisation can be accomplished in polynomial time. Furthermore, there are many approaches for the establishment of quantum encryption algorithms based on the idea of superdense coding. At this point it is wise to refer to [8, 9, 10, 11,12,13]. All of them have something in common; applying self inverse unitary operations to a message to encrypt the message under certain circumstances. Other encryption algorithms like [14] rely on entanglement, where the entangled key is sent over an insecure quantum channel. A generalisation of [14] is given by [15]. Furthermore [10] encrypts a classical binary bit using keys in a non-orthogonal quantum state, extended by [8] to a new quantum encryption algorithm where it employing the bit-wise quantum computation by proposed a novel quantum encryption algorithm for classical binary information. [9] proposes standard one time pad encryption algorithm for classical messages without a pre-shared or stored key. [11] refines this algorithm to a probabilistic algorithm. In this paper the whole encryption process is presented as depicted in the figure 1.

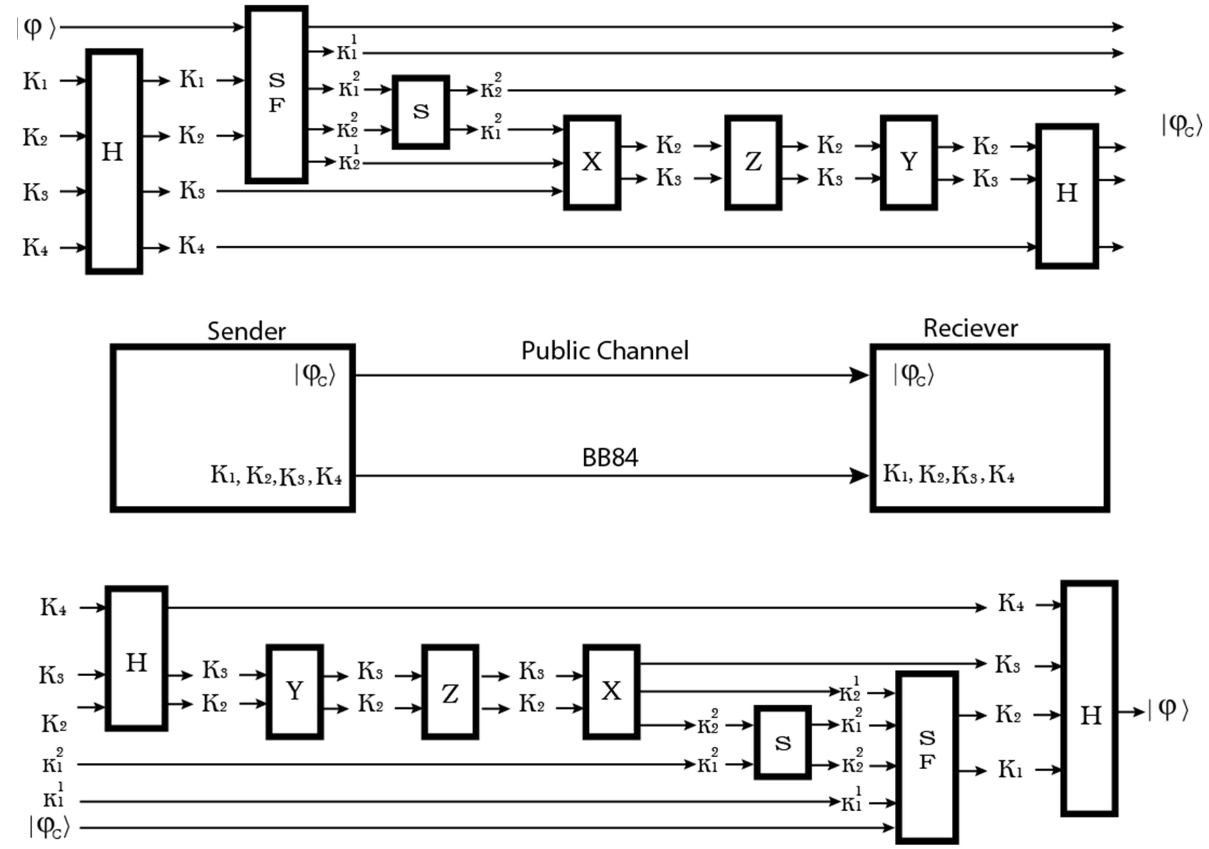

Fig. 1. Encryption,Transmission and Decryption Process. H: Hadmars Gate, SF:Switch Function, S:SWAP Gate, X: Pauli-X gate, Z: Pauli-Z gate, Y: Pauli-Y gate.

First, four groups of quantum keys are used in the process of encryption and decryption. The keys will be used as an input for the quantum encryption algorithm that is proposed here and will divided into four groups superposition, permutation, quantum error correction and hadamard transformation.

$$\begin{aligned}|\emptyset_{C1}\rangle &= |K_1^1K_1^2\rangle \otimes |\emptyset\rangle \\ &= |K_1^1K_1^2\rangle \otimes \alpha|0\rangle + \beta|1\rangle \\ &= \alpha|K_1^1K_1^2 0\rangle + \beta|K_1^1K_1^2 1\rangle\ , \end{aligned} \tag{2}$$

All of those, along with the algorithm encryption is discussed in section 2. The transmission of keys and the quantum ciphertext is introduced in section 3. Then the decryption in section 4 will be discussed as an inverse operation of the encryption. Furthermore, in section 5 the circuit of the proposed algorithms are presented.After that, analysis of the security of the algorithm is made in 6. Finally the paper ends with the concluding remarks in section 7.

2 QUANTUM ENCRYPTION ALGORITHM

The idea of the quantum encryption algorithm is very straightforward. It is based on the combination of four groups of quantum keys that are used in the process of encryption and decryption (K1, K2, K3 and K4) where K1 represent the superposition, K2 represent the permutation, K3 represent the quantum error correction and K4 represent the hadamard transformation. The operations of superposition, permutation and quantum error correction makes parasitization to the quantum state ∅ and the hadamard operation making the quantum cipheretext ∅_C non-orthogonal. The following steps explain the procedure of the proposal encryption algorithm.

2.1 *First Group:(Superposition)*

The superposition state is a newly proposed operation and it is considered as a basic issue both in cryptography and in real life physical system. The advantage of the superposition state

is that it expands ciphertext space. The quantum state is prepared by us as a superposition state $|\emptyset\rangle = \alpha|0\rangle + \beta|1\rangle$ according to the first group K1, where K_1^1, $K_1^2 \in$ K1 and the key is applied to the hadamard gate where the Hadamard gate acts on a single qubit. It maps the basis state $|0\rangle$ to $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ which represents $|+\rangle$ and $|1\rangle$ to $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ which represents $|-\rangle$, the hadamard gate represented as a matrix as follows:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix},$$

Finally, two images to the key can be obtained $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, then the first quantum cipheretext $|\emptyset_{C1}\rangle$ in equation 2, And all the cases for the |├ ∅_C1 ⟩┤ as shown in Table 1.

Table 1: Result of the first quantum ciphertext $|\emptyset_{C1}\rangle$.

$\lvert\emptyset\rangle$	$\boldsymbol{K_1^1K_1^2} = \lvert + +\rangle$	$\boldsymbol{K_1^1K_1^2} = \lvert + -\rangle$	$\boldsymbol{K_1^1K_1^2} = \lvert - +\rangle$	$\boldsymbol{K_1^1K_1^2} = \lvert - -\rangle$
$\lvert 0\rangle + \lvert 1\rangle$	$\alpha\lvert + + 0\rangle + \beta\lvert + + 1\rangle$	$\alpha\lvert + - 0\rangle + \beta\lvert + - 1\rangle$	$\alpha\lvert - + 0\rangle + \beta\lvert - + 1\rangle$	$\alpha\lvert - - 0\rangle + \beta\lvert - - 1\rangle$

2.2 *Second group:(Permutation)*

The permutation is a basic operation in classical cryptography and it shows up frequently in quantum computation and can be realized easily.This operation extends the ciphertext space and confuses the opponent.The second group of key K2, permuting two qubits can be implemented by the bit swapping gate where the definition of the SWAP function representation is as:

$$\text{SWAP} = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\end{bmatrix},$$

Here, if the K2 =$|+\rangle$ the SWAP do not work and if K2 =$|-\rangle$ the SWAP works between state 1 and state 3.Then the second ciphertext state $|\emptyset_{C2}\rangle$ is written as in equation 3, and all the cases for the $|\emptyset_{C2}\rangle$ as shown in table 2.

$$\begin{aligned}|\emptyset_{C2}\rangle &= \left[\delta_{+,K2}(\alpha|K_1^1K_1^2 0\rangle + \beta|K_1^1K_1^2 1\rangle) + \delta_{-,K2}(\alpha|0K_1^2K_1^1\rangle + \beta|1K_1^2K_1^1\rangle)\right] \otimes |\emptyset_{C1}\rangle \\ &= U_{SWAP}^{K2} \otimes |\emptyset_{C1}\rangle\end{aligned}$$

Table 2: Result of the second quantum ciphertext $|\emptyset_{C2}\rangle$.

$|\emptyset_{C1}\rangle$	$\boldsymbol{K_2} = |+\rangle$	$\boldsymbol{K_2} = |-\rangle$
$\alpha|+ + 0\rangle + \beta|+ + 1\rangle$	$\alpha|+ + 0\rangle + \beta|+ + 1\rangle$	$\alpha|0 + +\rangle + \beta|+ + 1\rangle$
$\alpha|+ - 0\rangle + \beta|+ - 1\rangle$	$\alpha|+ - 0\rangle + \beta|+ - 1\rangle$	$\alpha|0 - +\rangle + \beta|1 - +\rangle$
$\alpha|- + 0\rangle + \beta|- + 1\rangle$	$\alpha|- + 0\rangle + \beta|- + 1\rangle$	$\alpha|0 + -\rangle + \beta|1 + -\rangle$
$\alpha|- - 0\rangle + \beta|- - 1\rangle$	$\alpha|- - 0\rangle + \beta|- - 1\rangle$	$\alpha|0 - -\rangle + \beta|1 - -\rangle$

2.3 Third group:(Quantum Error Correction)

This operation confuses the quantum information where the sender padding several errors into it. All errors can fall into four types of gates I, X, Z and Y gates1, where gate I represents no error where the definition of the gate I is represented as:

$$\mathrm{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

The X gate acts on a single qubit and it is the quantum equivalent of a NOT gate where it maps to $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$. It is represented by the matrix,

$$\mathrm{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

The Z gate is a special case of a phase shift gate in which it leaves the basis state $|0\rangle$ unchanged and maps $|1\rangle$ to $-|1\rangle$. It is represented by the Z matrix,

$$\mathrm{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

The Y gate represents both bit flip and phase flip and it is represented by the matrix,

$$\mathrm{Y} = \begin{bmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{bmatrix},$$

The quantum state was applied if their respective quantum control bits are $|+ +\rangle$, $|+ -\rangle$, $|- +\rangle$ and $|- -\rangle$ according to the key element K3. The third ciphertext state $|\emptyset_{\mathrm{C3}}\rangle$ is written as two cases when $\left|\emptyset_{\mathrm{C}_2^+}\right\rangle$ and $|\emptyset_{\mathrm{C}_2^-}\rangle$ hence,

$$|\emptyset_{\mathrm{C3}}\rangle = \left|\emptyset_{\mathrm{C}_2^+}\right\rangle \otimes \big(\delta_{++,\mathrm{K3}}\mathrm{I} + \delta_{+-,\mathrm{K3}}\mathrm{X} + \delta_{-+,\mathrm{K3}}\mathrm{Z} + \delta_{--,\mathrm{K3}}\mathrm{Y}\big)\,, \qquad (4)$$

$$|\emptyset_{\mathrm{C3}}\rangle = |\emptyset_{\mathrm{C}_2^-}\rangle \otimes \big(\delta_{++,\mathrm{K3}}\mathrm{I} + \delta_{+-,\mathrm{K3}}\mathrm{X} + \delta_{-+,\mathrm{K3}}\mathrm{Z} + \delta_{--,\mathrm{K3}}\mathrm{Y}\big)\,, \qquad (5)$$

Therefore 32 different states for one qubit can be obtained according to different keys as shown in table 3 and table 4.

Table 3: Result of the third quantum ciphertext $|\emptyset_{C3}\rangle$ when $K_2 = |+\rangle$.

$\left|\emptyset_{C_2^+}\right\rangle$	$\boldsymbol{K_3} = |+ +\rangle$	$\boldsymbol{K_3} = |+ -\rangle$	$\boldsymbol{K_3} = |- +\rangle$	$\boldsymbol{K_3} = |- -\rangle$
$\alpha|+ + 0\rangle + \beta|+ + 1\rangle$	$\alpha|+ + 0\rangle + \beta|+ + 1\rangle$	$\alpha|+ + 0\rangle + \beta|+ + 1\rangle$	$\alpha|- + 0\rangle + \beta|- + 1\rangle$	$\alpha|- + 0\rangle + \beta|- + 1\rangle$
$\alpha|+ - 0\rangle + \beta|+ - 1\rangle$	$\alpha|+ - 0\rangle + \beta|+ - 1\rangle$	$\alpha|+ - 0\rangle + \beta|+ + 1\rangle$	$\alpha|- - 0\rangle + \beta|- - 1\rangle$	$\alpha|- - 0\rangle + \beta|- - 1\rangle$
$\alpha|- + 0\rangle + \beta|- + 1\rangle$	$\alpha|- + 0\rangle + \beta|- + 1\rangle$	$-\alpha|- + 0\rangle - \beta|- + 1\rangle$	$\alpha|+ + 0\rangle + \beta|+ + 1\rangle$	$\alpha|+ + 0\rangle + \beta|+ + 1\rangle$
$\alpha|- - 0\rangle + \beta|- - 1\rangle$	$\alpha|- - 0\rangle + \beta|- - 1\rangle$	$-\alpha|- - 0\rangle - \beta|- + 1\rangle$	$\alpha|+ - 0\rangle + \beta|+ - 1\rangle$	$\alpha|+ - 0\rangle + \beta|+ - 1\rangle$

Table 4. Result of the third quantum ciphertext $|\emptyset_{C3}\rangle$ when $K_2 = |-\rangle$.

$|\emptyset_{C_2^-}\rangle$	$\boldsymbol{K_3} = |+ +\rangle$	$\boldsymbol{K_3} = |+ -\rangle$	$\boldsymbol{K_3} = |- +\rangle$	$\boldsymbol{K_3} = |- -\rangle$
$\alpha|0+ +\rangle + \beta|1 + +\rangle$	$\alpha|0+ +\rangle + \beta|1+ +\rangle$	$\alpha|1+ +\rangle + \beta|0 - -\rangle$	$\alpha|0+ +\rangle - \beta|1 + +\rangle$	$i\alpha|1+ +\rangle - i\beta|0 + +\rangle$
$\alpha|0 - +\rangle + \beta|1- +\rangle$	$\alpha|0 - +\rangle + \beta|1 - +\rangle$	$\alpha|1 - +\rangle + \beta|0 - +\rangle$	$\alpha|0 - +\rangle - \beta|1- +\rangle$	$i\alpha|1- +\rangle - i\beta|0 - +\rangle$
$\alpha|0 + -\rangle + \beta|1 + -\rangle$	$\alpha|0+ -\rangle + \beta|1+ -\rangle$	$\alpha|1 + -\rangle - \beta|0 + -\rangle$	$\alpha|0 + -\rangle - \beta|1 + -\rangle$	$i\alpha|1+ -\rangle - i\beta|0 + -\rangle$
$\alpha|0 - -\rangle + \beta|1 - -\rangle$	$\alpha|0- -\rangle + \beta|1 - -\rangle$	$\alpha|1- -\rangle + \beta|0 - -\rangle$	$\alpha|0 - -\rangle - \beta|1 - -\rangle$	$i\alpha|1- -\rangle - i\beta|0 - -\rangle$

2.4 Fourth group:(H Transformation)

At the end of the algorithm, the sender applies the H gate to the state that is coming from the third group under the control of the key element K4 where the quantum ciphertext here becomes non-orthogonal.The forth quantum ciphertext state $|\emptyset_{C4}\rangle$ is,

$$|\emptyset_{C4}\rangle = |\emptyset_{C3}\rangle \otimes \mathrm{H}^{\delta-,\mathrm{K}4} \quad (6)$$

Based on equation 3 and 4 it was noticed that there were two cases to the$|\emptyset_{C3}\rangle$ therefore the quantum ciphertext $|\emptyset_{C4}\rangle$ includes 64 different cases according to different keys as shown in the following table 5.

Table 5: Result of the fourth quantum ciphertext $|\emptyset_{C4}\rangle$.

$\vert\emptyset_{C3}\rangle$	$\boldsymbol{K_4} = \vert+\rangle$	$\boldsymbol{K_4} = \vert-\rangle$
$\alpha\vert++0\rangle+\beta\vert++1\rangle$	$\alpha\vert++0\rangle+\beta\vert++1\rangle$	$\alpha\vert0+0\rangle+\beta\vert0+1\rangle$
$\alpha\vert+-0\rangle+\beta\vert+-1\rangle$	$\alpha\vert+-0\rangle+\beta\vert+-1\rangle$	$\alpha\vert0-0\rangle+\beta\vert0-1\rangle$
$\alpha\vert-+0\rangle+\beta\vert-+1\rangle$	$\alpha\vert-+0\rangle+\beta\vert-+1\rangle$	$\alpha\vert1+0\rangle+\beta\vert1+0\rangle$
$\alpha\vert--0\rangle+\beta\vert--1\rangle$	$\alpha\vert--0\rangle+\beta\vert--1\rangle$	$\alpha\vert1-0\rangle+\beta\vert1-0\rangle$
$\alpha\vert++0\rangle+\beta\vert++1\rangle$	$\alpha\vert++0\rangle+\beta\vert++1\rangle$	$\alpha\vert0+0\rangle+\beta\vert0+1\rangle$
$\alpha\vert+-0\rangle+\beta\vert++1\rangle$	$\alpha\vert+-0\rangle+\beta\vert++1\rangle$	$\alpha\vert0-0\rangle+\beta\vert0+1\rangle$
$-\alpha\vert-+0\rangle-\beta\vert-+1\rangle$	$-\alpha\vert-+0\rangle-\beta\vert-+1\rangle$	$-\alpha\vert1+0\rangle-\beta\vert1+1\rangle$
$-\alpha\vert--0\rangle-\beta\vert-+1\rangle$	$-\alpha\vert--0\rangle-\beta\vert-+1\rangle$	$-\alpha\vert1-0\rangle-\beta\vert1+1\rangle$
$\alpha\vert-+0\rangle+\beta\vert-+1\rangle$	$\alpha\vert-+0\rangle+\beta\vert-+1\rangle$	$\alpha\vert1+0\rangle+\beta\vert1+1\rangle$
$\alpha\vert--0\rangle+\beta\vert--1\rangle$	$\alpha\vert--0\rangle+\beta\vert--1\rangle$	$\alpha\vert1-0\rangle+\beta\vert1-1\rangle$
$\alpha\vert++0\rangle+\beta\vert++1\rangle$	$\alpha\vert++0\rangle+\beta\vert++1\rangle$	$\alpha\vert0+0\rangle+\beta\vert0+1\rangle$
$\alpha\vert+-0\rangle+\beta\vert+-1\rangle$	$\alpha\vert+-0\rangle+\beta\vert+-1\rangle$	$\alpha\vert0-0\rangle+\beta\vert0-1\rangle$
$\alpha\vert-+0\rangle+\beta\vert-+1\rangle$	$\alpha\vert-+0\rangle+\beta\vert-+1\rangle$	$\alpha\vert1+0\rangle+\beta\vert1+1\rangle$
$\alpha\vert--0\rangle+\beta\vert--1\rangle$	$\alpha\vert--0\rangle+\beta\vert--1\rangle$	$\alpha\vert1-0\rangle+\beta\vert1-1\rangle$
$\alpha\vert++0\rangle+\beta\vert++1\rangle$	$\alpha\vert++0\rangle+\beta\vert++1\rangle$	$\alpha\vert0+0\rangle+\beta\vert0+1\rangle$
$\alpha\vert+-0\rangle+\beta\vert+-1\rangle$	$\alpha\vert+-0\rangle+\beta\vert+-1\rangle$	$\alpha\vert0-0\rangle+\beta\vert0-1\rangle$
$\alpha\vert0++\rangle+\beta\vert1++\rangle$	$\alpha\vert0++\rangle+\beta\vert1++\rangle$	$\alpha\vert+++\rangle+\beta\vert-++\rangle$
$\alpha\vert0-+\rangle+\beta\vert1-+\rangle$	$\alpha\vert0-+\rangle+\beta\vert1-+\rangle$	$\alpha\vert+-+\rangle+\beta\vert--+\rangle$
$\alpha\vert0+-\rangle+\beta\vert1+-\rangle$	$\alpha\vert0+-\rangle+\beta\vert1+-\rangle$	$\alpha\vert++-\rangle+\beta\vert-+-\rangle$
$\alpha\vert0--\rangle+\beta\vert1--\rangle$	$\alpha\vert0--\rangle+\beta\vert1--\rangle$	$\alpha\vert+--\rangle+\beta\vert---\rangle$
$\alpha\vert1++\rangle+\beta\vert0--\rangle$	$\alpha\vert1++\rangle+\beta\vert0--\rangle$	$\alpha\vert-++\rangle+\beta\vert+--\rangle$
$\alpha\vert1-+\rangle+\beta\vert0-+\rangle$	$\alpha\vert1-+\rangle+\beta\vert0-+\rangle$	$\alpha\vert--+\rangle+\beta\vert+-+\rangle$
$\alpha\vert1+-\rangle-\beta\vert0+-\rangle$	$\alpha\vert1+-\rangle-\beta\vert0+-\rangle$	$\alpha\vert-+-\rangle-\beta\vert++-\rangle$
$\alpha\vert1--\rangle+\beta\vert0--\rangle$	$\alpha\vert1--\rangle+\beta\vert0--\rangle$	$\alpha\vert---\rangle+\beta\vert+--\rangle$
$\alpha\vert0++\rangle-\beta\vert1++\rangle$	$\alpha\vert0++\rangle-\beta\vert1++\rangle$	$\alpha\vert+++\rangle-\beta\vert-++\rangle$
$\alpha\vert0-+\rangle-\beta\vert1-+\rangle$	$\alpha\vert0-+\rangle-\beta\vert1-+\rangle$	$\alpha\vert+-+\rangle-\beta\vert--+\rangle$
$\alpha\vert0+-\rangle-\beta\vert1+-\rangle$	$\alpha\vert0+-\rangle-\beta\vert1+-\rangle$	$\alpha\vert++-\rangle-\beta\vert-+-\rangle$
$\alpha\vert0--\rangle-\beta\vert1--\rangle$	$\alpha\vert0--\rangle-\beta\vert1--\rangle$	$\alpha\vert+--\rangle-\beta\vert---\rangle$

$i\alpha\|1++\rangle - i\beta\|0++\rangle$	$i\alpha\|1++\rangle - i\beta\|0++\rangle$	$i\alpha\|-++\rangle - i\beta\|+++\rangle$
$i\alpha\|1-+\rangle - i\beta\|0-+\rangle$	$i\alpha\|1-+\rangle - i\beta\|0-+\rangle$	$i\alpha\|--+\rangle - i\beta\|+-+\rangle$
$i\alpha\|1+-\rangle - i\beta\|0+-\rangle$	$i\alpha\|1+-\rangle - i\beta\|0+-\rangle$	$i\alpha\|-+-\rangle - i\beta\|++-\rangle$
$i\alpha\|1--\rangle - i\beta\|0--\rangle$	$i\alpha\|1--\rangle - i\beta\|0--\rangle$	$i\alpha\|---\rangle - i\beta\|+--\rangle$

As it was mentioned before, the possible states in group four are non-orthogonal, which makes the states undistinguishable for the opponent and this represents the aim in this proposed algorithm.

3 TRANSMISSION

The sender and receiver share four keys K1, K2, K3 and K4 by secure quantum channel and best way of sharing the keys is BB84 protocol which is the first quantum cryptography protocol based on the quantum property. It is explained as a method of securely communicating a private key from one party to another [4]. As for the quantum ciphertext $|\emptyset_{C}\rangle$ will send it over an insecure channel.

4 QUANTUM DECRYPTION ALGORITHM

All operations are carried out by the sender in the encryption are reversed in the decryption. This is because all of the operations in the encryption are unitary. Therefore all steps of decryption process are inverse of the steps of encryption process and can be performed easily as follows:

Firstly, Bob decrypts the state $|\emptyset_{C4}\rangle$ by using the key K4. If K4 is equal to $|-\rangle$, Bob applies H gate to $|\emptyset_{C4}\rangle$, or else receiver keeps it by itself. Consequently receiver obtains the state $|\emptyset_{C3}\rangle$. Following this, the receiver decrypt the state $|\emptyset_{C3}\rangle$ by using the key K3. If K3 is $|++\rangle$, receiver lets $|\emptyset_{C3}\rangle$ alone, or if K3 is $|+-\rangle$, receiver applies X gate to $|\emptyset_{C3}\rangle$. Alternatively if K3 is $|-+\rangle$, the receiver applies Z gate to $|\emptyset_{C3}\rangle$, or else if K3 is $|--\rangle$, the receiver applies Y gate to $|\emptyset_{C3}\rangle$. After this process, the receiver obtains the state $|\emptyset_{C2}\rangle$. Upon having $|\emptyset_{C2}\rangle$ the receiver continues to swap the qubits in $|\emptyset_{C2}\rangle$.When the key element K2 is equal to $|-\rangle$, the receiver swaps the qubits in $|\emptyset_{C2}\rangle$, otherwise, the receiver does not proceed to swap. After the above operations, the receiver obtains the state $|\emptyset_{C1}\rangle$. Finally, receiver separates the state $|\emptyset_{C1}\rangle$ and then obtains the anticipated qubits.

5 QUANTUM CIRCUIT IMPLEMENTATION

A quantum encryption algorithm based on bit-wise quantum computation was proposed.The quantum circuit implementation of the proposed algorithm is shown in figure 1, it was noticed that the figure shows that the inputs states are $\in \{0,1\}$ and each input state enter to H gate to get state $|+\rangle$ and $|-\rangle$. This represents the keys that were used in the circuit.SF carries out a quantum switch function using K2. When the K2 is $|+\rangle$, SF switches on to 1,alternatively SF switches on to 2. The encryption procedure runs from the left to right, while the decryption procedure runs from the right to the left and applies the gates X,Z,Y and H to the quantum state if their respective quantum control quantum bits are $|+-\rangle$, $|-+\rangle$, $|--\rangle$ and $|-\rangle$.

6 SECURITY ANALYSIS

No-cloning theorem is the basic idea proving a particular information is encoded and transmitted through non-orthogonal state and is secretary against opponent [16]. Under this theory, the different state of the quantum ciphertext cannot reach the excellence. In the proposed algorithms it is explained that the quantum ciphertext $|\emptyset_{C1}\rangle$ corresponds to 4 different states. The quantum ciphertext $|\emptyset_{C2}\rangle$ corresponds to 8 different states. The quantum ciphertext $|\emptyset_{C3}\rangle$ corresponds to 32 different states and the quantum ciphertext $|\emptyset_{C4}\rangle$ corresponds to 64 different states under different keys. For each bit, the probability is bounded by $\frac{1}{4^4}$. Supposing the length of the encrypted message block is n, the probability is bounded by $\frac{1}{4^{4n}}$, which is negligible. Since the information of quantum encryption algorithm encoded by non-orthogonal quantum state the opponent was able to obtain only the ciphertext, it can only complete one set of operations on each of the encrypted state just once. Because the opponent does not know the key, the results of measurement of the opponent are random. Through the foregoing, the ciphertext only attacks the impossible. Attack opponent is infeasible given he can find out the plaintext opponent or able to choose the plaintext of the attack. This is because the opponent could not be known by the ciphertext in contrast to the plaintext without knowing the key. The trojan horse attack is not only used commonly in classical encryption, but also common in the attack of a quantum encryption [17]. The aim of the trojan horse attack is to obtain the necessary information so that the attacker is able to break in the system, for example, trojan horse will send information feedback which is available in 0 and 1 when the similar case for ciphertext is in $|0\rangle$ and $|1\rangle$.Because of the different state of the ciphertext which is non-orthogonality, the trojan horse sending information feedback is not useful in breaking in the system, exemplified by the ciphertext in $|+\rangle$ and $|-\rangle$ where no specific information is sent as feedback. Security is the essence of non-orthogonal quantum ciphertext. In this article qubit was chosen as the key instead of the classic bits for the implementation of the algorithm. In order to reduce the problem of managing the key, re-repeating of the first three keys can be done. In addition to group of four of the key to be secretary, proposed algorithm kept realized through the analysis of algorithm security. Results showed that the receiver can be vague given that there is no opponent. Therefore, the existence of any attacker can be detected by sender and receiver. The shared key can be reused, if there is no opponent, on the other hand the proposed algorithm takes the form of blocking encryption.

7 CONCLUSION

The quantum technology is a new and improving technology, specifically in the field of quantum cryptography. Parallel to this statement, many in the computer advancement field would acknowledge that science and technology advances very rapidly which will result in production of quantum computers in the immediate future. This knowledge brings quite a problem which is treatment or transfer of the existing information. The information that is used today is in classical form and it is nearly impossible to convert it to quantum information using pre-shared classical keys, even if it is familiar with the personnel trying to implement quantum information, because of significant security problems. Therefore the improvement of quantum encryption algorithm that is proposed provides security in such instances. Interestingly, this proposal can be viewed as the generalization of BB84 protocol in the procedure of two users communicating with the help of a shared key. The security and the physical implementation of the proposed algorithm are analysed in detail and it is concluded that the improvement can prevent the quantum attack as well as the classical attack. Preventing two kinds of attack and protecting the information from new prying manner is the goal. Finally, it should be mentioned that improvements can be made to the algorithm by the users in order to make it more powerful and secure.

8 REFERENCES

[1] Nielsen MA, Chuang IL. Quantum computation and quantum information. Cambridge university press; 2010.

[2] Schneier B. Applied cryptography: protocols, algorithms, and source code in C. john wiley &amp; sons; 2007.

[3] Bekenstein JD. Universal upper bound on the entropy-to-energy ratio for bounded systems. Phys Rev D. 1981 Jan; 23:287-298.

[4] Bennett C. An update on quantum cryptography. ADV CRYPTOLOGY. 1984; p. 475-486.

[5] Shor PW. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM journal on computing. 1997; 26(5):1484-1509.

[6] Shor PW. Algorithms for quantum computation: discrete logarithms and factoring. In: Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on. IEEE; 1994. p. 124-134.

[7] Shor PW. Polynomial time algorithms for discrete logarithms and factoring on a quantum computer. In: Algorithmic Number Theory. Springer; 1994. p. 289-289.

[8] Zhou NR, H ZG. A realizable quantum encryption algorithm for qubits. Chinese Physics. 2005;14(11):2164.

[9] Zhou N R ZGHXJ Liu Y, C ZF. Novel qubit block encryption algorithm with hybrid keys. Physica A: Statistical Mechanics and its Applications. 2007;375(2):693-698.

[10] Zeng GH. Encrypting binary bits via quantum cryptography. Chinese Journal of Electronics. 2004;13(4):651-653.

[11] Cao Z, Liu L. Improvement of one quantum encryption scheme. In: Intelligent Computing and Intelligent Systems (ICIS), 2010 IEEE International Conference on. vol. 1. IEEE; 2012. p. 335-339.

[12] Zhou N, Zeng G, Nie Y, Xiong J, Zhu F. A novel quantum block encryption algorithm based on quantum computation. Physica A: Statistical Mechanics and its Applications. 2006; 362(2):305 – 313.

[13] Hua T, Chen J, Pei D, Zhang W, Zhou N. Quantum Image Encryption Algorithm Based on Image Correlation Decomposition. International Journal of Theoretical Physics. 2014;p.1-12. Available from: http://dx.doi.org/10.1007/s10773-014-2245-z.

[14] Leung DW. Quantum vernam cipher. Quantum Information and Computation. 2002;2(1):14-34. Cited By (since 1996)40.

[15] Boykin PO, Roychowdhury V. Optimal encryption of quantum bits. Physical review A. 2003;67(4):042317.

[16] Wootters WK, Zurek WH. A single quantum cannot be cloned. Nature. 1982;299:802-803.

[17] Peng J, He G, Xiong J, Zeng G. Trojan Horse Attack Strategy on Quantum Private Communication. In: Chen K, Deng R, Lai X, Zhou J, editors. Information Security Practice and Experience. vol. 3903 of Lecture Notes in Computer Science. Springer Berlin Heidelberg; 2006. p. 177-186.