International Journal of Soft Computing 11 (7): 465-472, 2016
ISSN: 1816-9503
© Medwell Journals, 2016

A Modifiable 2-Qubit Quantum Block Encryption Algorithm

[1]Alharith A. Abdullah, [2]Rifaat Z. Khalaf and [3]Mustafa Riza
[1]College of Information Technology, University of Babylon, Babil, Iraq
[2]College of Science, University of Diyala, Diyala, Iraq
[3]Department of Physics, Eastern Mediterranean University, North Cyprus,
via Mersin 10 Gazimagusa, Turkey

Abstract: In this study, a modifiable 2-qubit quantum block encryption algorithm employing the idea of superdense coding will be proposed. One of the most fascinating properties of this algorithm is that after a step of analysis we can decide when to change the operations of the algorithm whenever it is statistically necessary. The underlying operations in this algorithm are unitary operators which can be represented using rotation matrices. The parameters for the combination of the rotation matrices can be generated using a quantum random number generator and transmitted safely taking advantage of the BB84 protocol, to generate the needed unitary operators for decryption. The message, being transmitted over an insecure channel, will be encrypted using the modifiable 2-qubit block encryption algorithm developed in this study. The keys are created using a quantum random number generator are also transmitted securely applying the BB84 algorithm. The security analysis and an example illustrating how the algorithm works rounds off this study. An overview of the complete process from the generation of the algorithm to the decryption of the message is illustrated explicitly.

Key words: Quantum cryptography, quantum computation, quantum encryption algorithm, unitary operator, decryption

INTRODUCTION

Advances in quantum computation are always considered as threats to classical encryption systems. The most comprehensive summary in the field of quantum computation was given by Nielsen and Chuang (2010). Let us consider the first block encryption algorithms. These algorithms are very easy to implement but depend significantly on the key length to ensure an appropriate level of security. Obviously, the length of the key is important to make a brute force attack very difficult (Schneier, 2007) However, of course, longer keys also increase 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 a superposition of the computational basis vectors, we get:

$$|S\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1}$$

where, $\alpha, \beta \in C$ and $|\alpha|^2+|\beta|^2 = 1$. If we look at this infinite set, we can easily see that every point on this circle is an accumulation point. If, in an open interval around the point x of a set, there are infinitely many points, we call this an accumulation point. Whereas the set of integers has no accumulation point. So evidently one qubit is sufficient to store a key that is combinatorial inaccessible. The only restriction in this case is that every transmission channel has a certain amount of noise. Therefore, the noise level and the associated error correction are the only limiting characteristics for the key and its transmission. If we neglect this, one qubit is sufficient to prevent any combinatorial motivated brute force attack, as the number of possible keys is infinite, because of every point in the set is an accumulation point. The mathematical theory is telling us that the key space is infinite but the according to Bekenstein, there is an upper bound to the information in the universe contradicting the mathematical claim. So, despitethe mathematical reasons, we can say that the quantum key space is considerably large but not infinite which is also inline with the limitation caused by the noise. From the birth of the idea quantum computation, it was clear that the nature of quantum measurement plays an important role in the secure transmission of information. So, it is obvious that one of the first significant contributions to quantum computation would be a way to prevent eavesdropping. The BB84 protocol proposed by Bennett and Weisner (1992) allows secure quantum key distribution over an insecure channel. There are many aspects of quantum computation related to security. Another aspect was illuminated by Shor (1994) by his ground breaking works on polynomial time algorithms for prime number factorization. These works show how vulnerable classical public key encryption

Corresponding Author: Alharith A. Abdullah, College of Information Technology, University of Babylon, Babil, Iraq

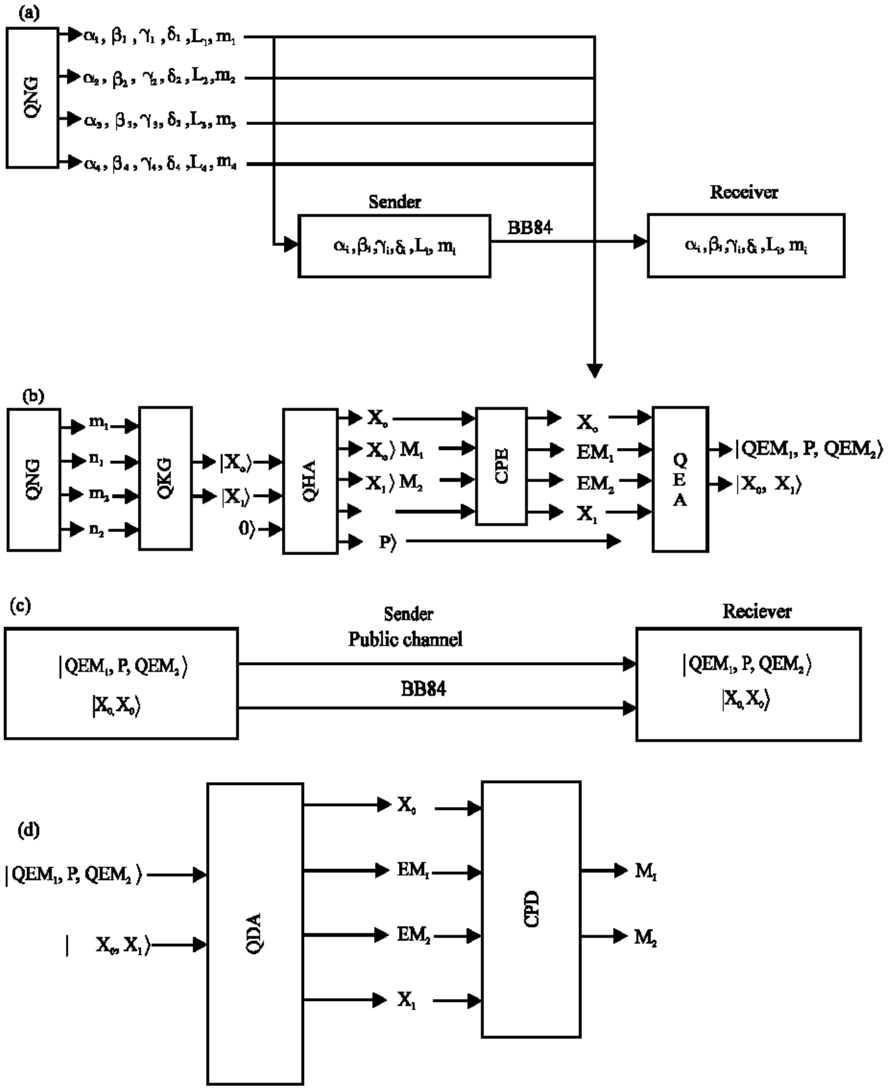

Fig. 1: Encryption,transmission and decryption process. QNG: Quantum Random Number Generator, QKG: Quantum Key Generator, QHA: Quantum Half Adder, CPE: Classical Pre-Encryption, QEA: Quantum Encryption Algorithm, QDA: Quantum Decryption Algorithm, CPD: Classical Pre-Decryption: a) Generation and distribution of the algorithm; b) Encryption process; c) Transmission of the cipher text keys; d) Decryption process

algorithms become if the prime number factorization can be accomplished in polynomial time. We would like to refer to the quantum encryption algorithm proposed in 206 by Zhou where a classical plaintext message is encrypted using a quantum computational algorithm employing six quantum keys divided into four groups. The output is a quantum ciphertext composed of three qubits. So in this algorithm a classical bit is encrypted three quits. Moreover, we would like to refer to the algorithms. All of them in common can apply under certain circumstances self-inverse unitary operations to a message to encrypt a message. Other encryption algorithms like Leung are relying on entanglement where the entangled key is sent over an insecure quantum channel. A generalisation of is given by Boykin and Vwani Roychowdhury. Furthermore, in a classical binary bit is encrypted using keys in a non-orthogonal quantum state which was extended by Zhou to a new quantum encryption algorithm. Horcas *et al.* (2007) proposed standard one-time pad encryption algorithm for classical messages without a pre-shared or stored key (Fig. 1). Cao and Liu refined this algorithm to a probabilistic algorithm. Khalaf and Abdullah (2014) proposed a novel quantum encryption algorithm that can be used to encrypt classical messages based on quantum shift register. Recently, Zhou present a new quantum image encryption algorithm based on generalized Arnold transform and double random-phase encoding and this is open new filed to developed the quantum encryption algorithm. All the ideas in Khalaf and Abdullah (2014) and Abdullah *et al.* (2015) discuss the quantum block encryption algorithm with hybrid keys and we are using same concept but with a novel scheme. In this study, we present the complete encryption process as depicted in Fig. 1.

First we have to generate the angles and parameters for the generation of the unitary operators as in Eq. 2. Then using the quantum random number generator a pair of quantum keys are generated. The ciphertext to be transmitted is composed of the quantum padding bit and the quantum encrypted message. This message can be transmitted via an insecure quantum channel. In every instance, the measured keys or the algorithms that need to be changed, two messages have to be sent over a quantum secure channel. The first one is a two-qubit message for the measured values of the key using the BB84 algorithm; the second is a message incorporating the parameters of each operator for the encryption. So with these parameter changes we can also transmit the change of the encryption algorithm and it means that we use an unlimited number of operators in the algorithm, a new and unique feature which is different from others algorithms that were submitted previously. Thus, after receiving three messages from the sender, two messages over a secure channel, i.e. the key pair and the parameter list and one over an insecure quantum channel, we will discuss the decryption in study V.3 as an inverse operation of the encryption. Finally, we close the study with a security analysis and the conclusions.

Quantum Key Generator (QKG): For the quantum key generation, we could think of many physical processes that underly the quantum random number generation. However, as our main focus will on the encryption algorithm, we want to mention just a simple method for the generation of a quantum key as superposition state in the computational basis. The Quantum Random Number Generators (QRNG) currently available are used as input to our key generator. So a short overview of the QRNG is given in the following section and showing how this QRNG can be used for the generation of a quantum key.

Quantum Random Number Generator (QRNG): The probabilistic nature of quantum processes obviously makes quantum processes a strong candidate for quantum number generation. For a long period, one of the best random number generators was based on radioactive decay. Furthermore, the arrival of photons in a photodetector, statistical white noise and other processes were also used for random number generation. All these methods were based on quantum processes have a non-measurable correlation. There are numerous articles on quantum random number generation or processes that can be utilized to create QRNGs. We would like to refer some of the publications of this still hot topic (Boixo *et al.*, 2014; Abellan *et al.*, 2014; Jennewein *et al.*, 2000; Stefanov *et al.*, 2000; Katsoprinakis *et al.*, 2008). There are also registered patents for QNRG available as:

Unitary operators: Unitary operators form the foundation of the encryption algorithm being presented in this study. Unitary operators can be written in the form:

$$U = e^{i\alpha}R_1(\beta)R_m(\gamma)R_1(\delta) \tag{2}$$

Where:

$R_\lambda(\xi)=e^{i\alpha\lambda\xi}$ and $\boldsymbol{\sigma}_\lambda$ = Being the Pauli matrices and
α, β, γ = Or alternatively we can write every unitary operatoras

$$U = e^{i\alpha}A \times B \times C \text{ with } ABC = I \tag{3}$$

We start with the transmission the parameters for all unitary operators over a secure channel. For long cypher texts it is appropriate to change the parameters of the unitary gates and therefore the encryption algorithm, in order to facilitate greater security.

Quantum key generator algorithm: Using a quantum random generator for integer numbers as discussed in the previous section, we generate two integer random numbers n and m for each quantum key X_0 and $X_1 \times X_0$ and X_1 are quantum keys in the form

$$|X_j\rangle = \alpha_j|0\rangle + \beta_j|1\rangle \text{ with } j \in \{0,1\}$$

As the primary focus is on the block encryption algorithm and not on the quantum key generation, we just propose two trivial quantum key generation algorithms based on two integer random numbers n and m from a QRNG. For each key, we need to generate one pair of random numbers n_j and m_j. So the question is the following; how can we convert n_j and m_j into α_j and β_j? Assuming that $|0\rangle$ and $|1\rangle$ are equally likely, we can convert the random numbers n and m:

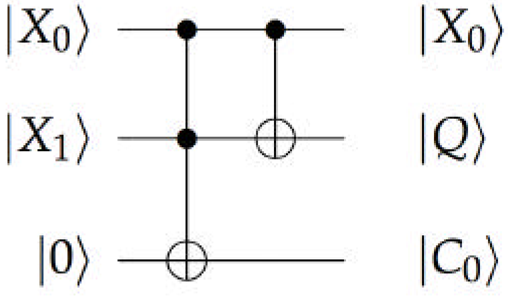

Fig. 2: First quantum Half Adder for two quantum bits

$$\alpha_j = \frac{e^{{im_j}/{n_j}}}{\sqrt{2}} \text{ and } \beta_j = \frac{e^{{in_j}/{m_j}}}{\sqrt{2}}$$

Resulting in:

$$\text{con}\,|\text{-}X_j\rangle = \frac{e^{{im_j}/{n_j}}}{\sqrt{2}}|\text{-}0\rangle + \frac{e^{{in_j}/{m_j}}}{\sqrt{2}}|\text{-}1\rangle\,\text{tent...} \quad (4)$$

Alternatively, we can also use:

$$|\text{-}X_j\rangle = \frac{1}{\sqrt{2}}R_{n_j}\,\text{mod}3(m_j)|\text{-}0\rangle + \frac{1}{\sqrt{2}}R_{m_j}\,\text{mod}3(n_j)|\text{-}1\rangle \quad (5)$$

where, $R_l(\alpha)$ denotes the Rotation operator with respect to the axis l. Of course, one can think of many more processes to generate quantum keys.

The Quantum Half-Adder (QHA): In classical computation, the half adder circuit randomises pseudo-random numbers but here the quantum half adder is used to generate padding bits. The quantum half adder circuit for two qubits, depicted in the figure below, is used for the generation of the padding qubit which is part of the ciphertext (Fig. 2).

The quantum half-adder circuit consists of quantum Control-Control-Not Gate (CCNOT-Gate or Toffoli-Gate) and quantum Control-Not Gate (CNOT-gate). This circuit takes three input qubits $|X_0\rangle$, $|X_1\rangle$ and $|0\rangle$ and returns three output qubits $|X_0\rangle$, $|Q\rangle$ and $|C_0\rangle$. The qubits $|Q, C_0\rangle$ form the two-bit quantum padding state $|P\rangle$.

In the literature, one can find various physical implementations of the quantum half-adder. Exemplarily, we would like to refer to Murali *et al*. (2002) for the NMR-based implementation and to (Barbosa, 2006) for the optical implementation.

Let us determine the output qubits $|\text{-}Q\rangle$ and $|\text{-}C_0\rangle$ of the quantum half-adder circuit in the case that the input states $|\text{-}X_0\rangle$ and $|\text{-}X_1\rangle$ are either just the basis states {$\text{-}|0\rangle$, $\text{-}|1\rangle$ or superposition states of the basis states. If $|X_0\rangle$ and $|X_1\rangle$ are either $|0\rangle$ or $|1\rangle$, then we get for the output qubits:

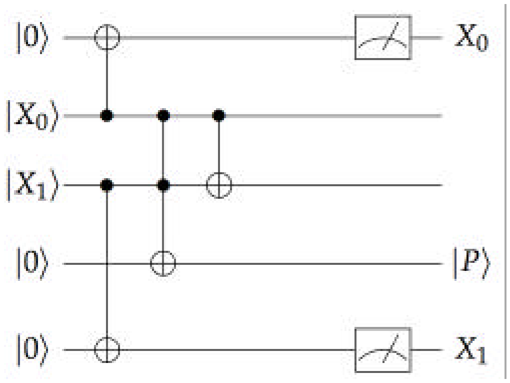

Fig. 3: Quantum half-Adder for two quantum bits and measurement for $|X_0\rangle$ and $|X_1\rangle$

$$|Q\rangle = |X_0 \oplus X_1\rangle$$

$$|C_0\rangle = |X_0 \times X_1 \oplus 0\rangle$$

If $|X_0\rangle$ and $|X_1\rangle$ are both superposition states, i.e., $|X_0\rangle = \alpha|0\rangle+\beta|1\rangle$ and $|X_1\rangle = \gamma|0\rangle+\delta\,|1\rangle$ then the output is a three qubit entangled state:

$$|P\rangle = |X_0, Q, C_0 = \alpha\gamma|000\rangle + \alpha\delta|010\rangle + \beta\gamma|110\rangle + \beta\delta|101\rangle$$

This state will be used as the padding qubits.

Classical Pre-Encryption (CPE) and Classical Pre-Decryption (CPD) with measured Keys X_0 and X_1: For the classical pre-encryption, we first perform a measurement of the keys $|X_0\rangle$ and $|X_1\rangle$ in the computational basis at the end of the application of the QHA as shown in Fig. 3. Getting X_0 and $X_1 \epsilon \{o, 1\}$. Where:

$$X_0 = \begin{cases} 0 \text{ with probability} |\alpha_0|^2 \\ 1 \text{ with probability} |\beta_0|^2 \end{cases} \quad (6)$$

and:

$$X_1 = \begin{cases} 0 \text{ with probability} |\alpha_1|^2 \\ 1 \text{ with probability} |\beta_1|^2 \end{cases} \quad (7)$$

These values of X_0 and X_1 are used for the following classical pre-encryption as shown in Fig. 4. Let M_0M_1 be a 2-bit classical message. Then the classical message in quantum notation $|M_0M_1\rangle$ will be first encrypted according to the circuit depicted in Fig. 4.

For the decryption of the message $|EM_0, EM_1\rangle$, the keys X_0 and X_1 have to be transferred securely to the

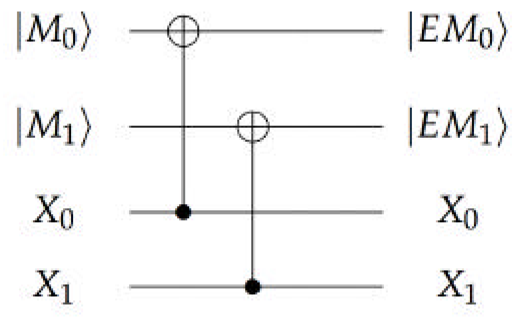

Fig. 4: First level encryption of the classical message

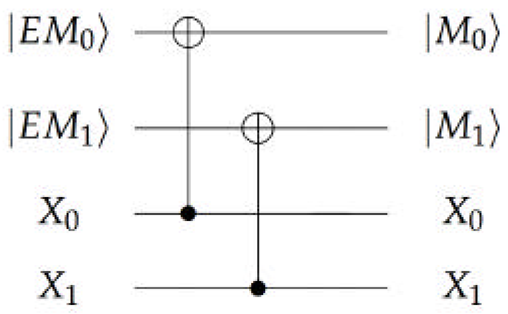

Fig. 5: First level decryption of the quantum encryption message

receiver. The pre-encrypted message and the transferred keys X_0 and X_1 serve as input for the classical decryption algorithm depicted in Fig. 5 which de facto is the classical pre-encryption algorithm depicted in Fig. 4 applied in reverse order.

Quantum Block Encryption Algorithm (QBEA) process and Quantum Block Decryption Algorithm (QBDA) Process: The idea of the algorithm is straightforward. For the encryption of each qubit we need one unitary operator; therefore, at least two distinct unitary operators become necessary for the encryption process. Following the idea of superdense coding, two out of four generated distinct unitary operators are selected according to the bit sequence of the measured quantum keys, as described below. Therefore, we first propose how the unitary operators are generated using a set of parameters being transmitted to the receiver using the BB84 algorithm. The generation of the operators allows us to send the parameters, responsible for the generation of the operators over a secure channel to change the algorithm, whenever it is necessary. The encryption algorithm is designed based on these operators. As we have generated two keys and we have a two bits message, we need to generate quantum ciphertext with three quantum bits.

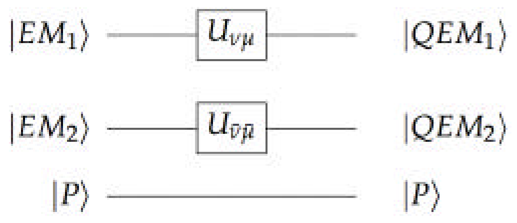

Fig. 6: Quantum block of encryption algorithm with $\bar{\mathrm{r}} = \neg\gamma, \bar{\mu} = \neg\mu$ and $\gamma, \mu \in \{0,1\}$

Table1: Correspondencetableforencryption

(X_0, X_1)	$U_{\gamma\mu}$
(0, 0)	U_{00}
(0, 1)	U_{01}
(1, 0)	U_{10}
(1, 1)	U_{11}

Quantum encryption: The idea for the Quantum Encryption Algorithm (QEA) is very straightforward. We will use the same principle as in the super dense coding presented by Bennett and Wiesner (1992). Based on the combination of the two measured key bits X_0 and X_1 we will select the operation on $|EM\rangle$. As we have two bitsof consideration, we can have four different combinations of these two bits. So for each of the combination there must be a unique unitary operation assigned, i.e., $U^{-1}_{\gamma\mu} \neq U_{ij} \text{ if } \gamma \neq i \text{ and } \mu \neq j$ resulting in the Table 1.

Let $X_0 = 0, X_1 = 1, P = 1, EM_1 = 1, EM_2 = 0$. Then, we compare the pair $(X_0, X_1) = (0, 1)$ with the bit pairs in the Table 1, to assign the unitary operation U_{01} for the encoding of EM_1 and U_{10} for the encoding of EM_2. So finally, we apply the following operation on $|EM_1\rangle|EM_2\rangle$ (Fig. 6):

$$|EM_1\rangle = (\mathbf{I} \otimes U_{01}) = U_{01}|EM_1\rangle = |QEM_1\rangle$$
$$|EM_2\rangle = (\mathbf{I} \otimes U_{10}) = U_{10}|EM_2 = |QEM_2\rangle$$

Resulting in the quantum cipher text $|QEM_1, QEM_2\rangle$ of the two bit message.

MATERIALS AND METHODS

Transmission: We transmit the parameters for the unitary Gates over a quantum secure channel and send the two keys X_0 and X_1 using a quantum channel by BB84. For the quantum ciphertext which is insert $|QEM_1\rangle$ and $|QEM_2\rangle$ between are send over an insecure channel.

Table 2: Correspondencetablefordecryption

(X_0, X_1)	$U_{\gamma\mu}^{-1}$
(0, 0)	U_{00}^{-1}
(0, 1)	U_{01}^{-1}
(1, 0)	U_{10}^{-1}
(1, 1)	U_{11}^{-1}

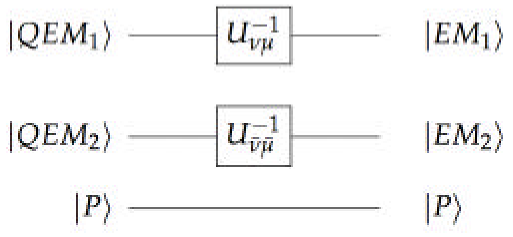

Fig. 7: Quantum block of decryption algorithm

Decryption: The idea for the Quantum Decryption Algorithm (QDA) is same quantum encryption algorithm but with opposite direction. Where based on the combination of the two measured key bits X_0 and X_1 that we received by secure channel we will select the operation on $|QEM_1\rangle$. As we have two bits of consideration, we can have four different combinations of these two bits. So, far each of the combination there must be a unique inverse unitary operation assigned, i.e., $U_{\gamma\mu}^{-1} \neq U_{ij}$ if $\gamma \neq i$ and $\mu \neq j$ resulting in the Table 2.

At the end we apply the quantum cipher text to the inverse of the unitary to get the decryption message Dm_i as shown in Fig. 7. And then we apply the inverse of the classical first level decryption to decrypt DM_i and get M_i.

RESULTS AND DISCUSSION

Example: In the following example we discuss how our algorithm work, where the sender send all the parameter to the receiver to set all the unitary operations before starting the encryption process and where we assume that the value of the unitary are:

$$U_{00} = Z, U_{01} = H, U_{10} = e^{i\alpha} R_1(\beta)$$
$$R_m(\gamma) R_1(\delta), U_{11} = I$$

And the parameters for the U_{10} are:

$$(\alpha = 90°, \beta = 74°, 1 = 1, \gamma = 0°, m = 2, \delta = 106°)$$

We apply the parameter to compute the U_{10}:

$$U_{10} = e^{i90°} \left[\begin{matrix} \left(\cos\frac{74°}{2} \times I - i \sin\frac{74°}{2} \times X \right) \\ \left(\cos 0° \times I - i \sin 0° \times Y \right) \\ \left(\cos\frac{106°}{2} \times I - i \sin\frac{106°}{2} \times X \right) \end{matrix} \right]$$

$$U_{10} = 0 + i\left[\left(\frac{4}{5} \times I - i\frac{3}{5} \times X \right)(1)\left(\frac{3}{5} \times I - i\frac{4}{5} \times X \right) \right]$$

$$U_{10} = i[(\frac{12}{25} \times I^2 - i\frac{16}{25} \times IX - i\frac{9}{25} \times IX - \frac{12}{25} \times X^2)(1)]$$
$$U_{10} = i[-iIX]$$

So the final result for the unitary of U_{10} is X. Now, if we have the output of the first quantum key generator is:

$$|X_0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

and the output of the second quantum key generator is:

$$|X_1\rangle = \frac{1}{\sqrt{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle$$

and if we have the classical message is:

$$M = |11\rangle$$

Before we make the classical pre-encryption we should take the measurement to the values of X_0 and X_1. Then we make the classical pre-encryption between the classical message and the output of the quantum key generator after the measurement for them.After that we compute the output of the quantum half-adder P and it is:

$$P = \frac{1}{\sqrt{6}}|0\rangle + \frac{1}{\sqrt{3}}|0\rangle + \frac{1}{\sqrt{3}}|1\rangle + \frac{1}{\sqrt{6}}|0\rangle$$

Now, we compute the quantum encryption message after the unitary transformation. The full encryption process is in Table 3. After the encryption process we transmit to the receiver the value of $|X_0, X_1\rangle$ over public channel and the value of ?over secure channel. The receiver will make the decryptionprocess where all the encryption process will invert to get the final the classical message $|M_1\rangle$.

Security analysis: The security of the scheme is directly based on BB84 protocol. In some sense, it is just the

Table 3: The results of encryption process in the above example

X_0	X_1	P	EM_1	U_{X_0,X_1}	QEM_1	EM_2	$U_{\bar{X}_0,\bar{X}_1}$	QEM_2	$\|QEM_1, P, QEM_2\rangle$
0	0	0	1	U_{00}	$-\|1\rangle$	1	U_{11}	$\|1\rangle$	$-\|101\rangle$
0	1	1	1	U_{01}	$\|-\rangle$	0	U_{10}	$\|1\rangle$	$\|-11\rangle$
1	0	1	0	U_{10}	$\|-\rangle$	1	U_{01}	$\|-\rangle$	$\|-1-\rangle$
1	1	0	0	U_{11}	$\|0\rangle$	0	U_{00}	$\|0\rangle$	$\|1000\rangle$

generalization of BB84 protocol in the scenario of two users communicating with the help of a shared key. We now give a brief argument for the security of the improved scheme. Given a ciphertext $|QEM_1, P, QEM_2\rangle$ an adversary cannot derive M_1M_2 without the information of (U_{00}, U_{01}, U_{10}, U_{11}) because the qubit $|EM_1\rangle|EM_2\rangle$, is constrained to the two pairs of conjugate state ($|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$) Because of the encryption transformation, the adversary cannot determinewhich operator of the possible operators $U_{00} = Z, U_{01} = H, U_{10} = e^{i\alpha}R_1(\beta)R_m(\gamma)R_1(\delta), U_{11} = I$ has been used. For each bit of M_1, the probability is bounded by 1/4. Suppose the length of the encrypted message block is n, the probability is bounded by $1/4^n$ which is negligible. Furthermore, if the adversary can obtain the multiple duplications of the first qubit and measure them, he cannot determine the bit M_1 because the four states are uniformly distributed in the first position. For example, if the adversary obtains |i and knows each qubit, he can still not determine M_1 because there are two preimages, (U_{01}, U_{10}). Finally, the adversary cannot derive $|M_1\rangle$ from the qubit $|P\rangle$ since the padding bit P has no relation to M_1. This comes from the fact that all quantum operators are performed on the first qubit. In the same way, we calculate M_2. For each bit of M_2, the probability is bounded by 1/4. Suppose the length of the encrypted message block is n, the probability is bounded by $1/4^n$ which is negligible. Furthermore, if the adversary can obtain the multiple duplications of the third qubit and measure them, he cannot determine the bit M_2 because the four states are uniformly distributed in the first position. For example, if the adversary obtains $|1\rangle$ and knows each qubit, he can still not determine M_2 because there are two preimages, (U_{00}, U_{01}). Finally, the adversary cannot derive $|M_2\rangle$ from the qubit $|P\rangle$, since the padding bit P has no relation to M_2.

CONCLUSION

The quantum technology is very important and being improved continuously, especially in the field of quantum cryptography. At the same time, the most of the world is challenging the fact that science and technology is in constant progress 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 classical form which is more conventional to the people in quantum and pre-shared classical technology since the security cannot be guaranteed. Therefore, we present a new quantum block encryption algorithm based on quantum half-adder, in this study we improved the quantum encryption algorithm, entailing two key bits to encrypt one message bit. The output of the algorithm is just composed of two qubits and one padding bit. The algorithm saves about half the cost without the loss of the security and the security is further improved through using the unitary operator without specifying the operator but only through the parameter that is used in the unitary where the sender and receiver generate the parameter for the generation of the unitary operators and there is agreement about these unitary operators before the encryption process begins. This makes the algorithm probabilistic rather than deterministic.

REFERENCES

Abdullah, A.A., R. Khalaf and M. Riza, 2015. A realizable quantum three-pass protocol authentication based on hill-cipher algorithm. Math. Prob. Eng., 2015: 1-6.

Abellan, C., W. Amaya, M. Jofre, M. Curty and A. Acin *et al*., 2014. Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode. Opt. Express, 22: 1645-1654.

Barbosa, G.A., 2006. Quantum half-adder. Phys. Rev. A, Vol. 73,

Bennett, C.H. and S.J. Weisner, 1992. Communication via one-particle and 2-particle operators on einstein-podolsky-rosen states. Phys. Rev. Lett., 69: 2881-2884.

Boixo, S., T.F. Ronnow, S.V. Isakov, Z. Wang and D. Wecker *et al*., 2014. Evidence for quantum annealing with more than one hundred qubits. Nat. Phys., 10: 218-224.

Horcas, I., R. Fernandez, G.J.M. Rodriguez, J. Colchero and G.J.W.S.X.M. Herrero *et al*., 2007. WSXM: A software for scanning probe microscopy and a tool for nanotechnology. Rev. Sci. Instrum., Vol. 78,

Jennewein, T., U. Achleitner, G. Weihs, H. Weinfurter and A. Zeilinger, 2000. A fast and compact quantum random number generator. Rev. Sci. Instrum., 71: 1675-1680.

Katsoprinakis, G.E., M. Polis, A. Tavernarakis, A.T. Dellis and I.K. Kominis, 2008. Quantum random number generator based on spin noise. Phys. Rev., Vol.77.

Khalaf, R.Z. and A.A. Abdullah, 2014. Novel quantum encryption algorithm based on multiqubit quantum shift register and hill cipher. Adv. High Energy Phys., Vol. 2014,

Murali, K.V.R.M., N. Sinha, T.S. Mahesh, M.H. Levitt and K.V. Ramanathan *et al*., 2002. Quantum-information processing by nuclear magnetic resonance: Experimental implementation of half-adder and subtractor operations using an oriented spin-7/2 system. Phys. Rev. A, Vol.66.

Nielsen, M.A. and I.L. Chuang, 2010. Quantum Computation and Quantum Information. Cambridge University Press, Cambridge, USA.

Schneier, B., 2007. Applied Cryptography: Protocols, Algorithms and Source Code in C. John Wiley and Sons, Hoboken, New Jersey, USA.

Shor, P.W., 1994. Polynomial Time Algorithms for Discrete Logarithms and Factoring on a Quantum Computer. In: International Algorithmic Number Theory Symposium, Adleman, L.M. and M.D. Huang (Eds.). Springer, Berlin, Germany, ISBN: 978-3-540-49044-9, pp: 289-289.

Stefanov, A., N. Gisin, O. Guinnard, L. Guinnard and H. Zbinden, 2000. Optical quantum random number generator. J. Mod. Opt., 47: 595-598.