Research Journal of Applied Sciences 11 (10): 953-958, 2016
ISSN: 1815-932X

A New Quantum Block Encryption Algorithm Based on Quantum Key Generation

Alharith A. Abdullah, Ahmed M. Al-Salih and Ali K. Bermani
University of Babylon, College of Information Technology, Hillah, Iraq

Abstract: In this study a new quantum encryption algorithm based on quantum key generation will be proposed. The whole process including the Quantum Key generation, Quantum Padding bit generation and the Quantum Block encryption algorithm are based on the idea of quantum half adder with introduced bit-swapping in the encryption process, the transmission of the necessary information and the decryption that will be illustrated. The mechanism of the algorithm is explained with the aid of an example. Finally a short security analysis will be given to show the difference between it's the classical counterpart.

Key words: Quantum cryptography, quantum computation, quantum random number generator, quantum encryption algorithm and quantum half-adder

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 (2002). Considering the first block encryption algorithms, it is clear that these algorithms are generally very easy to implement and depend on long keys to ensure an appropriate level of security. Obviously, the length of the key is important in order to make a brute force attack significantly difficult. Therefore, reviewing the basics of a brute force or extensive search attack firstly is critical. The difficulties of this attack method are based on the combinatorics. We can easily calculate that the numbers of possible keys of a key with a key length of n-bits is 2". Therefore, if the intend is to test all possible keys to decrypt a ciphertext encrypted using a block cipher, the complexity for this attack is obviously 2", i.e., exponential. Furthermore the longer the key is, the lower is the probability to find the key. If we take a key of 128 bits length is taken, the number of possible keys becomes $2^{128} \approx 10^{38}$. Assuming that testing one key takes 1ns, it will take 10^{29} years on a single processor machine. If it is assumed that there are currently 10^{20} processors available on the world and if it is possible to use them all it still would take 10^{9} years using all available processors in the world.

So, obviously the key length significantly determines the success of the brute force attack probability (Schneier, 2007). However it also increases 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, the result would be:

$$|A\rangle = \alpha|0\rangle + \beta|1\rangle \quad (1)$$

where, $\alpha, \beta \in C$ and $|\alpha|^2 + |\beta|^2$. If this infinite set is examined it is possible to acknowledge 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 infinitely many points which is not the case in the case of integer numbers. Evidently one qubit is sufficient to store a key that is combinatorially inaccessible. The only restriction in this case is that every transmission channel has certain noise and depending on that noise 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, because every point in the set is an accumulation point. The mathematical theory is telling us that the key space is infinite but according to Bekenstein (1981) there is an upper bound to the information in the universe, contradicting with the mathematical claim that the quantum key space is infinite. Despite the mathematical reasons, it is fair to state that the quantum key space is considerably large but not infinite. From the birth of the idea quantum computation, it was clear that the nature of quantum measurement would play an important role in the secure transmission of information. Therefore, it is self-evident that one of the first significant contributions to quantum computation

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

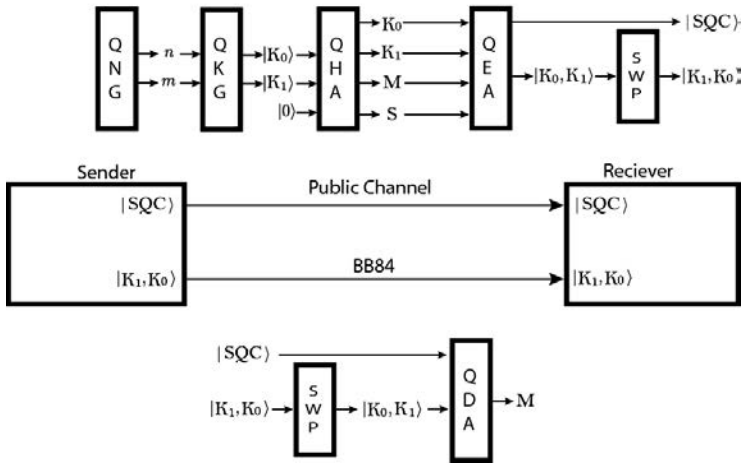

Fig. 1: Encryption, Transmission and Decryption Process. QNG: Quantum Random Number Generator, QKG:Quantum Key Generator, QHA: Quantum Half Adder, QEA: Quantum Encryption Algorithm, QDA: Quantum Decryption Algorithm, SWP: Swap gate

would present a way to prevent eavesdropping. The BB84 protocol proposed by Bennett (1984) allows secure quantum key distribution over an insecure channel. There are many aspects of quantum computation that are related to security. Shor (1994a, b, 1997) illuminated one aspect throughout his ground breaking works on polynomial time algorithms for prime number factorisation. This research shows 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 super dense coding. As Run and Hua (2005), Zhou *et al.* (2007), Cao and Liu (2010) they referred, have in common to apply under certain circumstances self-inverse unitary operations of a message to encrypt that message. Other encryption algorithms like are relying on entanglement, where the entangled key is sent over an insecure quantum channel. A generalisation of Leung is given by Boykin and Roychowdhury (2003). Furthermore, Cao and Liu (2010) encrypted a classical binary bit using keys in a non-orthogonal quantum state which was extended by Run and Hua (2005) to a new quantum encryption algorithm (Zhou *et al.* (2007). Proposed standard one time pad encryption algorithm for classical messages without a pre-shared or stored key (Shor, 1994). Refined this algorithm to a probabilistic algorithm. Proposed a novel quantum encryption algorithm that can be used to encrypt classical messages based on quantum shift register. Discuss the quantum block encryption algorithm with hybrid keys.

In this study we present the whole encryption process as depicted in Fig. 1.

MATERIALS AND METHODS

Quantum Key Generator (QKG): For the quantum key generation it is possible to think of many physical processes that actually underlies the Quantum Random Number Generation. However as the main focus will on the encryption algorithm, it is important to mention only a simple method for the generation of a quantum key as superposition state in the computational basis. In the following, the Quantum Random Number Generators (QRNG) will be used, currently available as input to the key generator. Therefore a very short overview of the QRNG will be given and how these quantum random numbers can be used for the generation of a Quantum Key.

Quantum Random Number Generator (QRNG): The probabilistic nature of quantum processes obviously make quantum processes a strong candidate for quantum number generation. For a long period, one of the best random number generators is based on radioactive decay. Of course the arrival of photons in a photo detector, statistical white noise and other processes are also used for random number generation. The most frequently used ones with non-measurable correlation are based on a quantum process.

There are numerous articles on quantum random number generation or processes that can be utilized to create QRNG's. We would like to cite some of the

publications of this still hot topic (Liang and Zeng, 2014; Boixo *et al*., 2014; Abellan *et al*., 2014; Weihs *et al*., 1998; Jennewein *et al*., 2000; Stefanov *et al*., 2000; Stipcevic and Rogina, 2000; Katsoprinakis *et al*., 2008; Wahl *et al*., 2011; Ma *et al*., 2013). Also there are also registered patents for QNRG available as (Murali *et al*., 2002).

Quantum Key Generator Algorithm (QKGA): Using a quantum random generator for integer numbers as discussed in the previous section, we will generate two integer random numbers n and m for each quantum key K_0 and K^1. Where K_0 and K^1 are quantum keys in the form:

$$\left|K_j\right\rangle = \alpha_j|0\rangle + \beta_j|1\rangle \quad (2)$$

With $j \in \{0, 1\}$, as our main focus is not on the quantum key generation but on the block encryption the study will propose to possible quantum key generation algorithms based on two integer random numbers n and m from a QRNG. For each one pair of random numbers n_j and m_j was needed to be generated. Therefore 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 as following to:

$$\alpha_j = \frac{e^{im_j/n_j}}{\sqrt{2}}, \beta_j = \frac{e^{in_j/m_j}}{\sqrt{2}} \quad (3)$$

Resulting in:

$$\left|K_j\right\rangle = \frac{e^{im_j/n_j}}{\sqrt{2}}|0\rangle + \frac{e^{in_j/m_j}}{\sqrt{2}}|1\rangle \quad (4)$$

Alternatively we can also use:

$$\left|K_j\right\rangle = \frac{1}{\sqrt{2}}R_{n_j} \bmod 3(m_j)|0\rangle + \frac{1}{\sqrt{2}}R_{n_j} \bmod 3(m_j)|1\rangle \quad (5)$$

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

RESULTS AND DISCUSSION

The Quantum Half-Adder (QHA): The quantum half adder circuit for 2 qubits, depicted in the Fig. 2, will be used to generate the padding qubit which will be part of the ciphertext.

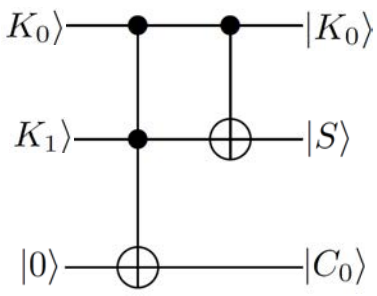

Fig. 2: Quantum half adder

The quantum half-adder circuit consists of quantum control control not gate (CCNOT-gate) (toffoli-gate) and quantum control not gate (CNOT-gate). The first circuit for the quantum half adder represents three inputs K_0, K_1 and $|0\rangle$ and three outputs $|K_0\rangle$, $|S\rangle$ and $|C_0\rangle$ as depicted in Fig. 2.

The physical implementation of the quantum half adder based on NMR was presented by Murali *et al*. (2002) whereas the optical version of the Quantum Half Adder can be referred to Barbosa (2006). Application of the quantum half adder gives us the output. If $|K_0\rangle$ and K_1 are the basis states, then the output of the Quantum Half adder is:

$$\begin{aligned} \left|S\right\rangle &= \left|K_0 \oplus K_1\right\rangle \\ \left|C_0\right\rangle &= \left|K_0 \cdot K_1 \oplus 0\right\rangle \end{aligned} \quad (6)$$

We take the output of $|S\rangle$; this state will be used as the padding qubits.

Quantum encryption Algorithm (QEA): The idea of the quantum encryption algorithm (QEA) is very straightforward. Based on the combination of the two measured key bits K_0 and K_1operation on $|M\rangle$ will be selected. As two bits are taken into account, four different combinations of these two bits can be obtained. So for each of the combination there must be a unique unitary operation assigned, as presented in the Table 1. Where the definition of the above unitary operation are:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Now, let $K_0 = 0$, $K_1 = 1$, $S = 1$, $M = 1$, then compare the pair $(K_0, K_1) = (0,1)$ with the bit pairs in the Table 1, to assign the unitary operation U01 and it represents H unitary gate for the encoding of M. Finally, apply the following operation on $|SM\rangle$ to get the quantum ciphertext with the padding bit $|SQC\rangle$ as depicted in Fig. 3:

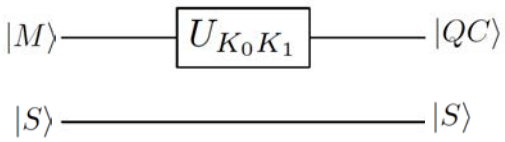

Fig. 3: Quantum Block of Encryption Algorithm

Table 1: Correspondence table for encryption

K_0, K_1	$U_{K0,K1}$
(0,0)	$U_{00} = I$
(0,1)	$U_{01} = H$
(1,0)	$U_{10} = ZH$
(1,1)	$U_{11} = X$

$$|SM\rangle \rightarrow (U_{01})|SM\rangle = |SQC\rangle \quad (7)$$

Transmission: Befor we transmit the two measurement keys $|K_0\rangle$ and $|K_1\rangle$ over a quantum secure channel (protocol BB84). The function of the bit-swapping circuit which is written as shown below is applied:

$$(|K_0\rangle|K_1\rangle \rightarrow |K_1\rangle|K_0\rangle) \quad (8)$$

And the definition of the SWAP function representation as:

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

The circuit for the SWAP gate consists of three CNOT gates as showed in Fig. 4.

After that, the keys are sent by the protocol BB84, for the quantum ciphertext $|QC\rangle$ which is concatenated with $|S\rangle$ send it over an insecure channel.

Quantum Decryption Algorithm (QDA): The idea for the Quantum Decryption Algorithm (QDA) is that the same quantum encryption algorithm is presented but with opposite direction. Based on the combination of the two measured key bits K_0 and K_1 that were received by secure channel the SWAP gate was introduced to get the right permutation and then selected the operation on $|S\rangle$.

As the two bits are taken into consideration, four different combinations of these two bits can be obtained. So for each of the combination there must be a unique unitary operation assigned and because the quantum gate that is used in the encryption is unitary, it was used in the decryption as well. In the end, the quantum ciphertext is applied to the unitary to get the message M as shown below in Fig. 5.

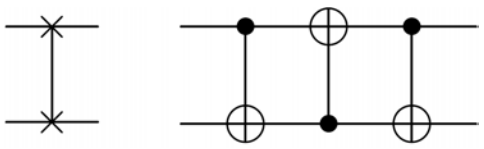

Fig. 4: Circuit of SWAP gate for two qubits

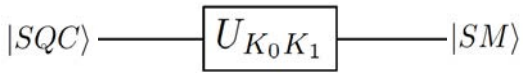

Fig. 5: Quantum Block of Decryption Algorithm

Security analysis: Summary for the security of proposal is given in this study, where the security of proposal is based on BB84 protocol. The opponent cannot drive the message M knowing the K_0 K_1 from a given quantum ciphertext $|QC\rangle$ because the quantum ciphertext is specific to the two pairs of conjugate states $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$. In addition if the sender and receiver come to an agreement to change the unitary operation periodically the opponent cannot find which operator of the possible operators I, H, ZH and X quantum gates is used in encryption algorithm, therefore this increases the security depending on the change. So the probability of each bit is bounded by 1/4. If the length of encrypted message block is n, then the probability become $1/4^n$ and it is concluded that the proposed algorithm is probabilistic. If the opponent can get the multiple duplications of the second qubit and measure them, he also cannot find the bit message M because the four states are uniformly distributed in the second position. For instance, if the opponent gets $|0 +\rangle$ and knows each qubit, he still cannot manage to find the message M because there are two preimages, $|01\rangle$ and $|10\rangle$ as shown in Table 2. Furthermore, the opponent cannot drive the message M from the qubit since the padding bit S has no relation with M. This comes from the fact that all quantum operators are executed on the second qubit.

Example: If the output of the first quantum random number generator is $|K_0\rangle = |1001\rangle$. And the output of the second quantum random number generator is $|K_1\rangle = |0011\rangle$. And if the classical message is M = 1100, then first of all the output of the quantum half adder S is computed. Hence, $|S\rangle = |1010\rangle$ now, we compute the quantum ciphertext where $|QC\rangle$ and in the Table 3 it shown that all cases of the quantum ciphertext depend on the key values of K_0 and K_1.

Table 2: All cases of the quantum encryption

SM	$K_0 K_1 = 00$	$K_0 K_1 = 01$	$K_0 K_1 = 10$	$K_0 K_1 = 11$
$\|00\rangle$	$\|00\rangle$	$\|0+\rangle$	$\|0-\rangle$	$\|01\rangle$
$\|10\rangle$	$\|10\rangle$	$\|0-\rangle$	$\|1+\rangle$	$\|11\rangle$
$\|01\rangle$	$\|01\rangle$	$\|0-\rangle$	$\|0+\rangle$	$\|00\rangle$
$\|11\rangle$	$\|11\rangle$	$\|1+\rangle$	$\|1+\rangle$	$\|10\rangle$

Table 3: The cases of the quantum ciphertext

SM	$K_0 K_1 = 00$	$K_0 K_1 = 01$	$K_0 K_1 = 10$	$K_0 K_1 = 11$
$\|11\rangle$	$\|11\rangle$	$\|1+\rangle$	$\|1-\rangle$	$\|10\rangle$
$\|01\rangle$	$\|01\rangle$	$\|0-\rangle$	$\|0+\rangle$	$\|00\rangle$
$\|10\rangle$	$\|10\rangle$	$\|1-\rangle$	$\|1+\rangle$	$\|11\rangle$
$\|00\rangle$	$\|00\rangle$	$\|0+\rangle$	$\|0+\rangle$	$\|01\rangle$

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 handle or transfer all of the existing information in the form of classical form which is familiar to the people in quantum information and pre-shared classical keys as long as the security cannot be guaranteed. Therefore a new quantum block encryption algorithm based on quantum half adder is proposed and shown that it possesses security. Stimulatingly, our study can be observed 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 analyzed in details and it is concluded that the new proposed algorithm can prevent the quantum attack as well as classical attack. Managing to prevent two kinds of attacks 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.

REFERENCES

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,

Bekenstein, J.D., 1981. Universal upper bound on the entropy-to-energy ratio for bounded systems. Phys. Rev. D., 23: 287-298.

Bennett, C.H. and G. Brassard, 1984. An Update on Quantum Cryptography. In: Workshop on the Theory and Application of Cryptographic Techniques, Robert, B.G. and C. David (Eds.). Springer, Berlin, Germany, ISBN:978-3-540-39568-3, pp: 475-480.

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.

Boykin, P.O. and V. Roychowdhury, 2003. Optimal encryption of quantum bits. Phys. Rev. A, Vol. 67,

Cao, Z. and L. Liu, 2010. Improvement of one quantum encryption scheme. Proceedings of the 2010 IEEE International Conference on Intelligent Computing and Intelligent Systems (ICIS), October 29-31, 2010, IEEE, New York, USA., ISBN:978-1-4244-6585-9, pp: 335-339.

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,

Liang, Y. and H. Zeng, 2014. Single-photon detection and its applications. Sci. China Phys. Mech. Astron., 57: 1218-1232.

Ma, X., F. Xu, H. Xu, X. Tan and B. Qi *et al*., 2013. Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction. Phys. Rev. A, Vol.87,

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, 2000. Quantum Computation and Quantum Information. Cambridge University Press, Cambridge.

Run, Z.N. and Z.G. Hua, 2005. A realizable quantum encryption algorithm for qubits. Chin. Phys., 14: 2164-2164.

Schneier, B., 2007. Applied Cryptography: Protocols, Algorithms and Source Code in C. 2nd Edn., John Wiley and Sons, New Delhi, India, ISBN-13: 9788126513680, Pages: 784.

Shor, P.W., 1994a. Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, November 20-22, 1994, Santa Fe, NM., pp: 124-134.

Shor, P.W., 1994b. 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.

Shor, P.W., 1997. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput., 26: 1484-1509.

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

Wahl, M., M. Leifgen, M. Berlin, T. Rohlicke and H.J. Rahn *et al*., 2011. An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements. Appl. Phys. Lett., Vol.98,

Weihs, G., T. Jennewein, C. Simon, H. Weinfurter and A. Zeilinger, 1998. Violation of bell's inequality under strict einstein locality conditions. Phys. Rev. Lett., 81: 5039-5043.

Zeng, G.H., 2004. Encrypting binary bits via quantum cryptography. Chin. J. Electron., 13: 651-653.

Zhou, N., Y. Liu, G. Zeng, J. Xiong and F. Zhu, 2007. Novel qubit block encryption algorithm with hybrid keys. Phys. A. Stat. Mech. Appl., 375: 693-698.