International Journal of Computer Networks and Communications Security

VOL. 3, NO. 6, JUNE 2015, 248–252
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

Generate Quantum Key by Using Quantum Shift Register

RIFAAT Z. KHALAF[1] and ALHARITH A. ABDULLAH[2]

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

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

E-mail: [1]rifat_driaa@yahoo.com, [2]alharith.khafaji@yahoo.com

ABSTRACT

In this paper we introduce a new fashion of quantum LFSR-based stream cipher. The basic component of LFSR based stream cipher is the LFSR (linear feedback shift register), so we describe how to build a quantum LFSR using the basic quantum gates. We have shown in our paper that this linear complexity ,period and statistical properties are identical with the classic case .We suggest a quantum stream cipher algorithm which can be built and worked in the quantum environment.

Keywords: *Quantum Computation, Quantum Cryptography, Quantum Shift Register, Linear Feedback Shift Register, Stream Cipher.*

1 INTRODUCTION

The world has witnessed in recent major development in the information and communication technology, Computer science has entered in all areas of life, including the sending and receiving information and protects an increasingly important tremendously, Information sent and addressed to me, and this requires careful secret storage of the data to be sent. For the appearance of quantum computing and quantum communication, it becomes increasingly important to develop methods for protecting quantum information versus the opponent effects of noise [1][2][3]. Researchers have developed in the field of quantum information many techniques to protect the quantum information [4][5][6]. Stream cipher systems that are used a secret key in the process of encryption and decryption, the stream cipher systems are one of the types of modern stream cipher systems and very important [7]. Advantages of these systems it is the most common and widely used in the field of encryption at the present time, because it has significant advantages including does not increase the errors in case they occur and ease of use in practical applications, in addition to the speed of execution. The algorithm are used to generate the key sequence are determined The security of stream cipher [8]. In the Y-00 protocol was to provide an accurate interpretation of the origin of the Security Y-00. Despite the fact that Y-00 protocol depends classical random and uncertainty. The Y-00 protocol was able to achieve a secure symmetric key at high speed (Gbps) and for long distance (1000Km). Although some researchers say that in Y-00 protocol is identical to the classical cryptography. In fact, he has no traditional analogue; gives also generalize even in the classical cryptography [9, 10].

2 SHIFT REGISTER WITH FEEDBACK

Each shift register consists of flip-flops. Flip-flop is a binary memory elements each of them is called a stage. A number of these stages is determined by the length and the degree of shift register complexity and can involve most of these stages by function called feedback function [11]. In each pulse shifts contents of any stage to the stage that preceded. Final stage shows where the output of the feedback function. The resulting sequence of shift register output is the content of the first stage.

3 LINEAR FEEDBACK SHIFT REGISTER BASED STREAM CIPHER

A convenient way to achieve long pseudo random sequence used by the majority but not all stream cipher process is used. Represents generators sequential to maximum length are used as part of the generators key stream in the stream cipher, due to their good statistical and large periods and less expensive implementation. A set of stream cipher are used (LFSR-based stream cipher), we mention the most common cases like SNOW, SOSEMAUNK, A5 became necessary for the cryptosystem designer to take into consideration the appropriate standards for generator key stream used in cipher. Some of these standards are: linear complexity, period and statistical test of a key stream [12].

4 QUANTUM SHIFT REGISTER

The main component of quantum shift register (QSR) is swap gates. The quantum shift register is a quantum circuit has the potential shift every data qubit to the nearest deciding a specific direction. Search more details in applications to arithmetic calculation and bitwise operations on two qubits. As is well known, the swap gate consists of three C-NOT gates [13]. A quantum circuit which can execute shift left on n-qubit data. There are many applications of a quantum shift register. The shift registers are mainly used in coding theory, especially in quantum error correction and quantum convolution code [14][15][16][17].

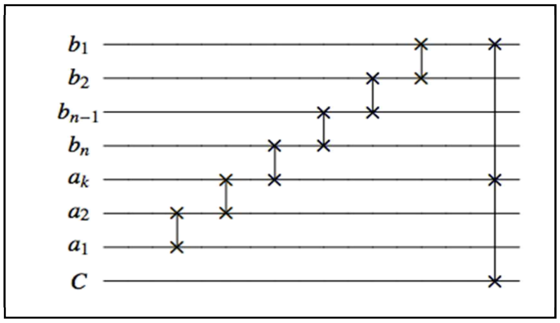

Fig. 1. The Quantum Left- Shift Register Which is Composed of The SWAP Gates on n-qubit

5 QUANTUM LINEAR FEEDBACK SHIFT REGISTER

The quantum linear feedback shift register (QLFSR) is essential in building quantum stream cipher algorithm. The length of quantum shift register is determined by the number of qubits (states), the contents of each qubit are shift to the next qubit in each pulse, the outputs of final qubit shows a quantum feedback function, the resulting sequence from the quantum shift register is the content of the first qubit.

6 QUANTUM LINEAR FEEDBACK SHIFT REGISTER BASED STREAM CIPHER

In Fig.2 the quantum linear feedback shift register based stream cipher (QLFSR-based stream cipher) which includes the following steps:

- Quantum shift register.
- Quantum XOR gate.
- Quantum feedback shift register.

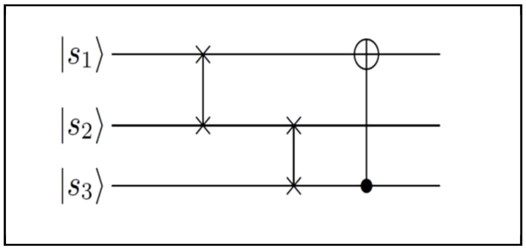

Fig. 2. Quantum linear feedback shift register consists of SWAP and C-NOT gate on 3-qubit.

$|S_1S_2S_3\rangle$ If we have a quantum register with length $|S_1S_2S_3\rangle$ represent a data input, then applied the algorithm of Quantum linear feedback shift register as follows: The quantum shift register has a number of positions. Each of these positions contains one qubit. Quantum register in which all qubits can be shifted one or more positions to the left or to the right. Then the shift operation be as follows depending on the swap gate. We do the shift between data becomes S2 replace the S1, S3 replace the S1 and S1 replace the S3. The quantum XOR function acts on the connection states in quantum register, Choose connect state that achieve the maximum period. For instance, if the number of connection states in the quantum register is two (like the connection between S1 and S2 in Fig. 2), the quantum XOR gate action is as follows: the second bit is the result of an XOR operation between the first and second bite, while the first bit is conserved. If we have the combination $|10\rangle$, this means, after transformation (quantum XOR): 1 for the first bit (conserved bit) and $1 \oplus 0 = 1$ for the second bit, so the quantum XOR of $|10\rangle$ became $|11\rangle$. After shifting work we apply a quantum XOR function of connection states. The quantum feedback function is representing the outputs of quantum XOR function is positioned in the final state (qubit) of quantum register. After know the states of the existing connect between the states, for instance, state of connectivity S1; S2 (give the maximum period). The output of a quantum XOR function placed in S3. In general, let the input quantum register as $|S_1S_2\cdots S_{n-1}S_n\rangle$. We apply the SWAP gate between n states as follows: SWAP1,2 we get $|S_2S_1\cdots S_{n-1}S_n\rangle$, SWAP2,3 we get, SWAP3,4 we get $|S_2S_3S_4S_1 \cdots S_{n-1}S_n\rangle$, in general SWAPn-1,n we get $|S_2S_3 \cdots S_nS_1\rangle$. After that we apply C-NOT gate. Fig.3 shows in one shift we need (n-1) SWAP and one C-NOT.

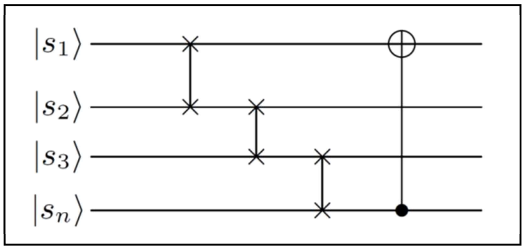

Fig. 3. Quantum linear feedback shift register consists of SWAP and C-NOT gate on n-qubit.

7 QUANTUM LINEAR FEEDBACK SHIFT REGISTER BASED ON STREAM CIPHER OUTPUTS

Taking any possible state of any quantum register in order to be as output, but we prefer to take the output of the first state (qubit) in order to ensure that the output is not linked to the initial value of the quantum register. For instance, if we have a quantum register with data input , then applied the algorithm of Quantum linear feedback shift register to compute the output keys as follows: quantum register with length 2-qubit $|S_1S_2\rangle$, the output key are S1; S1+ S2; S3. Quantum register with length 3-qubit $|S_1S_2S_3\rangle$, the output key are S1; S1+S2; S1+S2+S3; S2+S3; S1+S3; S2; S3. Quantum register with length n-qubit $|S_1S_2S_3 \cdots S_{n-1}S_n\rangle$, the output key are S1; S1+S2; S1+S2+S3; S2+S3; S1+S3; S2; S3 ⋯ Sn-1; Sn. A cryptosystem designer it is necessary to take into consideration the appropriate standards for key stream used in the design of the system. Some of these design criteria are linear complexity, period and statistical test of a key stream.

7.1 Linear complexity

Define linear Complexity is the shortest n length for quantum linear feedback shift register (QLFSR) which outputs are identical to the original output [18]. The linear complexity of the finite and infinite sequence as follows: L(s) = 0 if the sequence of S = 00 ⋯ 0, L(s) = if no QLFSR generates the sequence S, otherwise, the length of the shortest QLFSR that generates s is L(s) where t is the generated sequence and L is the linear complexity.

7.2 Period

Define the period for QLFSR, which consists of n-states that the length of the stream before it repeats itself, and the short period for QLFSR to encrypt different parts of the plain text with the same key stream, which causes a large breach. In practice, the stream period must be long enough, the plain text without repeating the key stream. As long as possible compatible with the large state space, this is produced by sequential maximum length. Greatest period to ensure a good statistic [19]. We define the associated matrix of a quantum sequence, and show how it relates to the least period length of the quantum sequence. A qth – quantum sequence $|\mathrm{xi}\rangle$ over Fq (the Galois Field of order q) has an associated $\mathrm{q} \times \mathrm{q}$ matrix (where q=2k). We generalize the SWAP matrix (GS) as follows.

$$= \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}$$

And generalize the C-NOT (GC) matrix as follows:

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

Let $\mathrm{A} = (\mathrm{G_S} \cdot \mathrm{G_C})_{\mathrm{q-1 \times q-1}}$, if one considers the ith state vector.

$$|\mathrm{x_i}\rangle = |\mathrm{x_i}, \mathrm{x_{i+1}}, \cdots \mathrm{x_{i+q1}}\rangle$$

Then

$$|\mathrm{x_i}\rangle\ \mathrm{A} = |\mathrm{x_i}, \mathrm{x_{i+1}}, \cdots \mathrm{x_{i+q-1}}\rangle$$
$$= |\mathrm{x_{i+1}}, \mathrm{x_{i+2}}, \cdots, \mathrm{x_{i+q-1}}, \mathrm{x_{i+q}}\rangle$$

$$= |\mathrm{x_{i+1}}\rangle$$

Hence,

$$|\mathrm{x_{i+1}}\rangle = |\mathrm{x_i}\rangle\ \mathrm{A}\ \text{For all } \mathrm{i} \geq 0 \qquad (1)$$

Lemma:

Suppose $|\mathrm{x_i}\rangle$ is a qth quantum sequence over Fq, with associated $\mathrm{q} \times \mathrm{q}$ matrix A. Then the state vectors $|\mathrm{x_i}\rangle$ are such that $|\mathrm{x_i}\rangle = \mathrm{AI}$. For all i = 0, 1, 2, ⋯.

Proof:

We proceed by induction on i. For i = 0, the result is trivially true. It has already been verified that $|\mathrm{x_{i+1}}\rangle = |\mathrm{x_i}\rangle\mathrm{A}$ for all $\mathrm{i} \geq 0$. Assume the result holds for the $(\mathrm{i}-1)_{\mathrm{st}}$ state vector $|\mathrm{x_{i-1}}\rangle$, so that $|\mathrm{x_{i-1}}\rangle = |\mathrm{x_0}\rangle$, and consider the ith state vector, $|\mathrm{x_i}\rangle$ by equation 1; $|\mathrm{x_{i-1}}\rangle = |\mathrm{x_i}\rangle\mathrm{A}$ for all $\mathrm{i} \geq 1$ and, using the inductive hypothesis, we have$|\mathrm{x_i}\rangle = |\mathrm{x_0}\rangle \mathrm{AI} - 1\mathrm{A} = |\mathrm{x_0}\rangle \mathrm{AI}$ for all $\mathrm{i} \geq 0$. Thus, by mathematical induction, the lemma is proved. So by lemma, $|\mathrm{x_{i+n}}\rangle = |\mathrm{x_0}\rangle \mathrm{A_{i+n}} = |\mathrm{x_0}\rangle \mathrm{A_i} = |\mathrm{x_i}\rangle$ for all $\mathrm{i} \geq 0$. Therefore, n is a period length of the purely periodic quantum sequence $|\mathrm{x_i}\rangle$. For instance, for tow state:

$$\mathrm{Shift} = [\mathrm{SWAP_{1,2}} \cdot \mathrm{CNOT_{1,2}}]$$

$$|\mathrm{Shift_1}\rangle = |0_1 0_2\rangle\langle 0_1 0_2| + |1_1 1_2\rangle\langle 0_1 1_2| + |0_1 1_2\rangle\langle 1_1 1_2| + |1_1 0_2\rangle\langle 1_1 0_2|$$

$$|\mathrm{Shift_2}\rangle = |0_1 0_2\rangle\langle 0_1 0_2| + |1_1 0_2\rangle\langle 1_1 1_2| + |1_1 1_2\rangle\langle 1_1 0_2| + |0_1 1_2\rangle\langle 0_1 1_2|$$

$$|\mathrm{Shift_3}\rangle = |0_1 0_2\rangle\langle 0_1 0_2| + |0_1 1_2\rangle\langle 1_1 0_2| + |1_1 0_2\rangle\langle 0_1 1_2| + |1_1 1_2\rangle\langle 1_1 1_2|$$

$$[\mathrm{SWAP_{1,2}} \cdot \mathrm{CNOT_{1,2}}] = |0_1 0_2\rangle\langle 0_1 0_2| + |0_1 1_2\rangle\langle 0_1 1_2| + |1_1 0_2\rangle\langle 1_1 0_2| + |1_1 1_2\rangle\langle 1_1 1_2|$$

For n state.

$$\mathrm{Shift} = [\mathrm{SWAP_{1,2}} \cdot \mathrm{SWAP_{2,3}} \cdots \mathrm{SWAP_{n-1,n}} \cdot \mathrm{CNOT_{1,2}}]$$

$$= |0_1 0_2 \cdots 0_{n-1} 0_n\rangle\langle 0_1 0_2 \cdots 0_{n-1} 0_n| + |1_1 0_2 \cdots 0_{n-1} 1_n\rangle\langle 0_1 0_2 \cdots 1_{n-1} 0_n| + |0_1 0_2 \cdots 1_{n-1} 0_n\rangle\langle 1_1 0_2 \cdots 0_{n-1} 1_n| + \cdots + |0_1 1_2 \cdots 1_{n-1} 1_n\rangle\langle 1_1 1_2 \cdots 1_{n-1} 0_n|$$

$$|0_1 0_2 \cdots 0_{n-1} 0_n\rangle\langle 0_1 0_2 \cdots 0_{n-1} 0_n| + |1_1 0_2 \cdots 0_{n-1} 1_n\rangle\langle 0_1 0_2 \cdots 1_{n-1} 0_n| + |0_1 0_2 \cdots 1_{n-1} 0_n\rangle\langle 1_1 0_2 \cdots 0_{n-1} 1_n| + \cdots + |0_1 1_2 \cdots 1_{n-1} 1_n\rangle\langle 1_1 1_2 \cdots 1_{n-1} 0_n|$$

$$|0_1 0_2 \cdots 0_{n-1} 0_n\rangle\langle 0_1 0_2 \cdots 0_{n-1} 0_n| + |0_1 0_2 \cdots 1_{n-1} 0_n\rangle\langle 1_1 0_2 \cdots 0_{n-1} 1_n| + |1_1 0_2 \cdots 0_{n-1} 1_n\rangle\langle 0_1 0_2 \cdots 1_{n-1} 0_n| + \cdots + |0_1 1_2 \cdots 1_{n-1} 1_n\rangle\langle 0_1 1_2 \cdots 0_{n-1} 1_n|$$

$$= [\mathrm{SWAP_{1,2}} \cdot \mathrm{SWAP_{2,3}} \cdots \mathrm{SWAP_{n-1,n}} \cdot \mathrm{CNOT_{1,n}}]$$

$$= |000 \cdots 00\rangle\langle 000 \cdots 00| + |000 \cdots 01\rangle\langle 000 \cdots 01| + \cdots |111 \cdots 10\rangle\langle 111 \cdots 10| + |111 \cdots 11\rangle\langle 111 \cdots 11|$$

After n step to reach the identity.

7.3 Statistical Test

If we have a quantum sequence and required of us evaluate these statistically, there are many statistical tests to determine the behavior of a quantum sequence statistically. Include these tests (run test, poker test, frequency test, serial test, auto correlation test and linear complexity test) [20]. These tests are generally testing the random distribution, relying linearity between the substrings of fixed length, and distribution ones and zeroes in a quantum sequence. Is the level of compression which can be implemented on sequential test and if the quantum sequence complexity enough to be random.

8 CONCLUSION

The linear complexity for quantum linear feedback shift register (QLFSR) is identical to the linear complexity in the linear feedback shift register (LFSR) case. The maximum period for key stream in (QLFSR) are the same maximum period of key stream in (LFSR) case. The application of statistical properties of (QLFSR) on sequential give the same results of applying statistical properties in the (LFSR) case. It is known in quantum shift register that there are more than two connection state, in this case cannot be used a quantum XOR circuit but the circuit is used controlled swap (fredkin gate). For instance, If the number of connection states in the quantum register is 3 the quantum fredkin gate action as follows: if the first bit of Fredkin gate is 1, then swaps the last two bits. In general, an n-input Fredkin gate has n-2 control lines which pass through the gate do not change and two target lines on which the values are swapped if all the control lines have value 1.

9 REFERENCES

[1] H.C.BennettandG.Brassard,"Quantumcryptography:public key distribution and coin tossing," in Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, vol. 175, pp. 175-179., New York, NY, USA, (1984).

[2] 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).

[3] F. Gaitan, "Quantum Error Correction and Fault Tolerant Quantum Computing," (CRC Press, Inc., Boca Raton, FL, USA, 2007).

[4] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," Phys. Rev. A 52, R2493 (1995).

[5] R. Z. Khalaf and A.A. Abdullah, "Novel Quantum Encryption Algorithm Based on Multiqubit Quantum Shift Register and Hill Cipher". Advances in High Energy Physics, Article ID 104325,USA,(2014).

[6] 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).

[7] W. Stallings, "Cryptography and Network Security: Principles and Practice / Edition 5," 5th ed., Pearson Custom Computer Science Series (Prentice Hall, 2010) iSBN-13: 9780136097044.

[8] G. Carter, "Statistical Tests for Randomness," EISS,England, (1989).

[9] P.Tombesi and O.Hirota," Proc. QCMC'00 ," Plenum Press (2001).

[10] H. P. Yuen, quant-ph/0311061 (2003).

[11] R. A. Rueppel, "Analysis and Design of Stream Ciphers," SpringerBerlinHeidelberg,(1986).

[12] P. P. Deepthi, Deepa Sara John and P. S. Sathidevi, "Design and analysis of a highly secure stream cipher based on linear feedback shift register", Elsevier, computers and elecrtical engineering, pp 235-243. (2009).

[13] D. Coppersmith, "IBM Research Report," RC 19642 (1994).

[14] Mark M. Wilde, "Quantum-shift-register circuits". Phys. Rev. A, 79:062325, Jun 2009.

[15] JH Park, JH Kang, TB Jung, KR Jung, CH Kim, YH Kim, SS Choi, and TS Hahn, "Low error operation of a 4 stage single flux quantum shift register built with y-ba-cu-o bicrystal josephson junctions". Applied Superconductivity, IEEE Transactions on, 11(1):625–628, 2001.

[16] Jae-weon Lee, Eok Kyun Lee, Jaewan Kim, and Soonchil Lee. "Quantum shift register". arXiv preprint quant- ph/0112107, (2001).

[17] Markus Grassl and Thomas Beth. "Cyclic quantum error–correcting codes and quantum shift registers". Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences, 456(2003):2689–2706, (2000).

[18] A. Ahmad and A. Elabdallai, "An Efficient Method to Determine Linear Feedback Connections in Shift Registers That Generate Maximal Length Pseudo-Random Up And Down Binary Sequences." Computer Electronic Engineering 23, 33 (1997).

[19] D.-Y. W. Kencheng Zeng, Chung-Hung Yang and T. Rao, "Pseudorandom Bit Generators in Stream-Cipher." Cryptography: IEEE (1991).

[20] S. Cagigal, N.P; "Algorithmic Determination of linear feedback in a Shift Register for pseudo random binary sequence generation Bracho," Electronic Circuits and Systems, IEE Proceedings 133, 191 (1986).