1st.International Conference of Information Technology to enhance E-learning and other Application,
(IT-ELA 2020), Baghdad College of Economic Sciences University, Baghdad, Iraq

Security of Enhancement of Adder in Stream Cipher System

Israa M.Hayder
Dept. of Computer Systems Techniques,
Qurna Technique Institute, STU,
Basrah, Iraq.
israa.mh@stu.edu.iq

Hussain A. Younis
College of Education for Women,
School of Computer Sciences, Universiti Sains Malaysia,
11800 USM, Penang, Malaysia
hussain.younis@uobasrah.edu.iq

Issa Ahmed Abed
Engineering Technical College, Southern Technical University, Basrah, Iraq
issaahmedabed@stu.edu.iq

Hameed A.K. Younis
College of Computer Science and Information Technology,
University of Basrah,
Basrah, Iraq.
hameedyounis882@gmail.com

***Abstract*—The strength of the encryption system depends on the power of the key generator that produces a pseudorandom stream. The generator generates a pseudorandom sequence so passes several tests. The non-linear flow coding system that relies on the Adder function has several unwanted vulnerabilities. It leads to failure to face randomness tests and relative success in the correlation attack. In this paper, the Adder function was developed by adding a third offset register to improve its ability to bypass randomness tests. In addition to increasing the non-linear complexity of the generated chain, it is resistant to breaking the code using a link attack. Many sequences were applied to the improved Adder system, and good results were obtained.**

Keywords*— *Adder generator, Correlation attack, Non-linear-feedback shift registers, Stream cipher.

I. Introduction

Stream cipher cryptosystems are one of the most important modern encryption systems that use a secret key in encryption and decryption [1]. These systems are the most common and used in the field of encryption today because of their important characteristics. It's including the failure to increase errors if they occur. Easy to use in practical applications, as well as fast implementation. The security of a streamlined encryption system depends on the algorithm used to generate a key sequence [2, 3]. Since there is a specific algorithm to generate a sequential key, this chain is cyclic, so it is semi-random and not completely random [4].

In previous work, A. K. Farhan [5] description a hybrid structure of encryption algorithm for stream cipher, this algorithm depends on specific elements for the selection of encryption process (logical operations (XOR, AND)) between the secret key and the plain text through encryption, decryption process. The specific intelligence elements choose from the key. N. Yerukala *et al.* [6] presents a new design of stream cipher for generating pseudorandom keystream with two LFSR's, one FCSR and a non-linear combiner function, which is a bit-oriented based on alternating step generator (ASGF). They design the FCSR controls two LFSR's. ASGF has two stages one is an initialization, and the other is keystream generation [17][18].

The work presented in this paper, the Adder function was developed by adding a third offset register to improve its ability to bypass randomness tests in addition to increasing the non-linear complexity of the generated chain. It is resistant breaking the code using a link attack. Many sequences were applied to the improved Adder system, and good results were obtained.

II. Stream cipher Systems with Security Degree

Until the degree of confidentiality of the cryptographic sy stem depending on the key sequence, certain attributes must characterize this sequence, which achieves a high degree of c onfidentiality[19]:

Such properties can be obtained on a random main-sequence [7]. But the key sequence generated in an excellent streamlined cryptographic system is almost random and not completely random because it is a periodic chain. So, the larger the length of the session, the better and preferably larger than the length of the message [8][15][16].

A. Randomness Tests

The random sequence has well-known *statistical attributes*, resulting in several randomization tests, through which we can test the sequential randomness of the key[9, 10]. There are many tests. To check the randomness of the binary chain, which is called *local randomness tests* (because it tests a single section (one cycle) of the binary chain. Initially, the success and failure rate of the tests should be determined. Therefore, statistical values were assigned to random strings with less than or equal to the value of the Chi-square, where the table value represents the (α%=5%) characteristic level of the distribution of the Chi-square. Randomness tests [11, 13].

B. Attack on Correlation

This approach is used to target non-linear coding schemes based on several linear displacement registers being non-linear uniform. It needs only knowledge of ciphertext without having to learn the corresponding text [13].

In 2012, The study showed a limitation of this type of system: a connection between the non-linear function inputs (linear displacement register outputs) and the generated key Z series. Based on this connection, it became possible to know some linear registers of displacement which are part of the network key called *a link attack*. Indicates a reduction in the number of attempts to find the system fragment when there is a link between the wall inputs and their outputs (i.e. the non-linear function) that is used to collect outputs [14].

III. Adder GENERATOR

The Adder generator system is one of the non-linear flow coding systems which generates a pseudorandom sequence based on the Adder. This system is created by:

1. The displacement registers of each of them have a linear feedback function giving the greatest cycle of lengths K1, K2 such that $K_1 <> K_2$ & GCD $(K_1, K_2) = 1$, where K_1 = Length (LFSR1) and K_2 = Length (LFSR2).
2. The correlation function used between the outputs of the displacement registers is the Adder function shown in Fig1.
3. The material cost of the generator is simple.

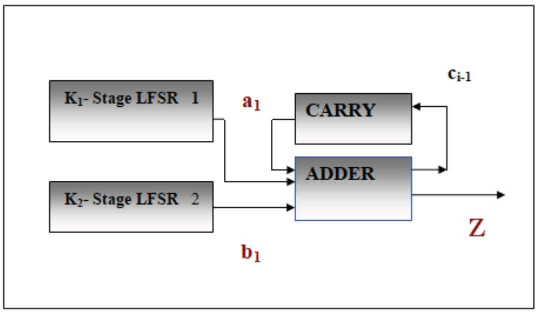

Fig. 1. Adder Algorithm.

It is clear and shown in the figure that the generator type collector (Adder) consists of two displacement registers and lengths K1, K2, respectively. It also had two feedback functions, and linking function (Adder), and carry and the result of all this is a pseudorandom sequence, which we mean sequential key (Z).

A. *Enhanced Adder System*

The strategy of the collector function is to generate a sequential key (pseudorandom sequence), which is a length $(2^{k_1}-1).(2^{k_2}-1)$ and is the result of entering the initial value of the registers LFSR1, LFSR2 and their counter-feedback

: The mathematical equation used to find the Zi sequence of the Adder function is

Zi = ai + bi + ci-1 (1)

ci = aibi + (ai + bi) ci-1 (2)

Since, bi, ai are sequential elements $1 < i < (2^{k_1}-1).(2^{k_2}-1)$ in sequence b1, a1 in turn, they are obviously nonlinear equations, where ai, bi , ci-1 are non-constant polynomials.

B. *The weakness of the Adder Generator*

Adder weakness can be summarized in two things:

1. The first is the complete lack of randomness, and this can be counted from the general weakness of the non-linear flow coding system.
2. The second is the possibility of attacking the system and breaking the code. By knowing part of the Z sequence from which you can learn some parts of the outputs of registers, including knowledge of offset registers. Hence, the idea of developing the Adder generator and reaching a new generator that may exceed this weakness, which is the developed Adder generator.

IV. Adder Generator Strategy

There is no significant difference in the components of the generator with three registers offset from the previous one only, but there are minor differences, including:

1. The developed Adder key generator consists of three offset registers.

   Since, K_3 = Length (LFSR3), K_2 = Length (LFSR2) and K_1 = Length (LFSR1)
2. It also consists of the Adder and Carries function as shown in Fig.2

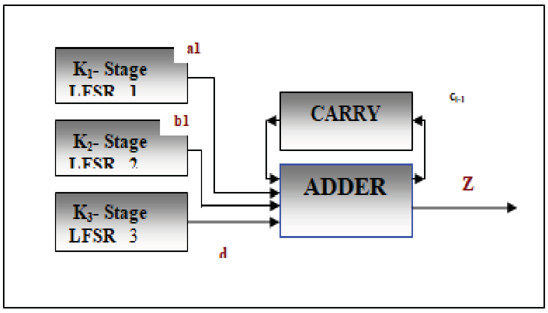

Fig. 2. Enhanced Adder Key Generator.

V. Experiments and Results

Several experiments were carried out on the sequential key sequences generated by the Adder generator and enhanced Adder generator system.

Experiment(1)

The randomness tests were carried out on several key values (initial values of the registers and feedback functions) on both generators. In the Adder, we obtained the following results: Table I shows in results.

TABLE I. RANDOMNESS TESTS FOR THE RESULTING SEQUENCE OF ADDER.

No	Keyes	Adder Function				
	Primary Value	Feed Function	Texts of Frequency			
			Frequency test ≤ 3.84	Serial test ≤ 5.99	Poker Test > 1.995	Run Test < 11.07
1	01	11	1.2	3	3.8	T0=24.2 T1=7.22
	101	11	√	√	√	x
2	10	10	1.4	2.93	3.9	T0=24.8 T1=7.63
	010	01	√	√	√	x
3	11	11	1.9	3.13	4.1	T0=25.2 T1=7.81
	110	10	√	√	√	x
4	101	110	2	1.83	5.93	T0=8.2 T1=24.2
	0011	11	√	√	√	x
5	111	101	2.9	2.3	6.14	T0=8.4 T1=24.6
	1001	101	√	√	√	x
6	011	011	3.4	2.6	6.32	T0=8.6 T1=24.9
	0101	101	√	√	√	x

In the developed Adder, we have obtained the following results: Table II shows in results.

TABLE II. TABLE II: RANDOMNESS TESTS OF THE CHAIN GENERATED BY THE DEVELOPED ADDER

No	Keyes	Adder Function				
	Primary Value	Feed Function	Texts of Frequency			
			Frequency test ≤ 3.84	Serial test ≤ 5.99	Poker Test > 1.995	Run Test < 11.07
1	01	11	0.359	1.756	15.68	T0=7.54 T1=4.28
	101	11				
	011	11	√	√	√	√
2	11	01	0.362	1.851	14.81	T0=7.66 T1=4.47
	011	01				
	101	01	√	√	√	√
3	10	10	0.397	1.872	14.47	T0=7.91 T1=4.28
	110	10				
	110	10	√	√	√	√
4	11111	110	0.071	0.054	10.6	T0=1.78 T1=1.04
	111	11				
	11	11	√	√	√	√
5	1001	101	0.082	0.057	9.8	T0=1.91 T1=1.14
	101	10				
	10	10	√	√	√	√
6	1101	111	0.042	0.061	9.1	T0=2.21 T1=2.39
	110	11				
	11	10	√	√	√	√

The tables show that passing tests in the enhanced Adder system is better than the previous Adder system. The first generator failed to pass the run test while the upgraded generator successfully passed the test.

Experiment(2)

The Adder generator's creation mechanism relied on increasing secrecy by boosting the linker's immunity provided by the Adder generator. A correlation or reliability between the Z-series and some linear displacement records outputs weaken the series resulting from the effect of any generator using non-linear displacement linear registers.

The example shows, we will show a stream generated by the generator and identify a part of it. We try to identify some of the outputs of the displacement registers (LFSR1, LFSR2).

If the outputs of the registers are recognized, the lengths and the value of the registers can be known, and we have broken the system and attacked it.

In the following experiment, we will illustrate an example of the sequence generated by the generator Adder and the chain generated by the developed generator Adder. Both sequences have the same register values and linear feedback functions. We will show the strength of the chain generated from the upgraded Adder as compared to the sequence generated from the Adder. Suppose that the initial value of the displacement registers is (111,11), respectively. The feeding functions for each register are:

$$F(S0,S1)=S0 \oplus S1 \text{ ،} F(S0,S1,S2)=S0 \oplus S1$$

Respectively

And that means $\oplus$ it is the XOR function.

After the implementation of both generators to produce chains shows the following:

In the Adder generator are:

Z= 011001011000101011011

with a length of $(2^2-1)(2^3-1) = 21$

And by applying

Qr=0, Qr+1 =0 ⟶ ar+1 =0

Qr=0, Qr+1 =1 ⟶ ar+1 =1

Qr=0, Qr+1 =0 ⟶ br+1 =0

Qr=0, Qr+1 =1 ⟶ br+1 =0

where Qr: previous state

We can find out some of the outputs of the offset registers. Attacking it is possible and breaks the system and breaks the code.

Add a third register (11111) with feedback function F(S0,S1,S2,S3,S4)=S0 $\oplus$ S1 $\oplus$ S3

The generated chain was

Z = 00101100101101100100l……

= 651

And by applying

Qr=0, Qr+1 =0 → ar+1 =0

Qr=0, Qr+1 =1 → ar+1 =1

Qr=0, Qr+1 =0 → br+1 =0

Qr=0, Qr+1 =1 → br+1 =0

We cannot simply detect the outputs of the displacement registers or some of them because of the linear complexity of the generator. This issue increased the complexity of the chain (this means a change in the behaviour of the Adder generator) explain past experiences. From this experience, the correlation attack failed to obtain the key sequence and break the code in the developed Adder system compared to the previous Adder.

VI.Conclusion

In this paper, the generator concept has been established, and the access to the new generator goes beyond the previous generator's vulnerability and makes the attackers more hidden and resistant. This enhancement was to bypass random generator tests, as well as to increase the immunity of correlation. Many sequences were applied to the improved Adder system, and good results were obtained.

A new design of stream cipher developed generator using FCSR is proposed, which is a software-oriented stream cipher to generate a pseudorandom sequence with 3LFSRs. Keystream of generator passes almost all NIST tests for randomness used tests. Throughput comparison of old Adder generator is presented. And brute force attack complexity of new generator is high. This complexity is very high when compared to popular ciphers. In developed generator, key size and combination of 3LFSRs and non-linear combiner functions play a major role in resistance to several attacks. It is secure enough against exhaustive search, algebraic and distinguishing attacks, for fixed extreme patterns of key and six inputs producing completely random output. The correlations between keystream and ciphertext have to be performed and exploit other attacks as future work.

References

[1] W. Stallings, "Cryptography and Network Security", Pearson Edition, Inc., USA, 2003.

[2] H. Malepati, "Digital Media Processing: DSP Algorithms Using C", Elsever, UK, 2010.

[3] B. White, A. Coulson, J. Doll, B. Habbershaw, Cecilia Carranza Lewis, Thomas Liu, Ryan McCarry, Eysha Shirrine Powers, Philippe Richard and Romoaldo Santos, IBM Redbooks," Getting Started with z/OS Data Set Encryption", 2018.

[4] D. A. Levin, and Y. Peres, "Markov Chains and Mixing Times", AMS., USA, 2017.

[5] A. K. Farhan, "Proposed Hybrid Approach of Stream Cipher Base on Selector of Encryption operation and Key Symmetric Translate", Eng. & Tech., Vol. 29, No. 11, 2011.

[6] N. Yerukala, V. Nalla, P. Guddeti, and V. Kamakshi Prasad, "Alternating Step Generator Using FCSR and LFSRs: A New Stream Cipher", International Journal of Intelligent Engineering and Systems, Vol. 12, No. 5, 2019.

[7] G. A. Marson, and B. Poettering, "Practical Secure Logging: Seekable Sequential Key Generators", ESORICS 2013.

[8] R. Ferdous, R. Lo Cigno, and A. Zorat, "Classification of SIP Messages by A Syntax Filter and SVMs", 5 - 38123 POVO, Trento - Italy, DISI - Via Sommarive, 2012.
http://disi.unitn.it.

[9] W. F. Rosenberger, and J. M. Lachin, "Randomization in Clinical Trials: Theory and Practice", Wiley, Canada, 2015.

[10] H. Demirhan, and N. Bitirim, "Statistical Testing of Cryptographic Randomness" Journal of Statisticians: Statistics and Actuarial Sciences, 2016
www.istatistikciler.org

[11] W. M. Fawaz, A. Rehim, I. Amr Ismail and E. Morsy, "Testing Randomness: Poker Test with Hands of Three Numbers", Journal of Computer Science 8 (8): 1353-1357, 2012.

[12] RL.Morin, "Monte Carlo Simulation in the Radiological Sciences", CRC Ervivals, 2019.

[13] I. M. Hayder, H. A. Younis, H. A. Younis, "Digital Image Enhancement Gray Scale Images In Frequency Domain", IOP Conf. Sequence: Journal of Physics: Conf. Sequence, 2019.

[14] R. A. Rueppel. "Analysis and Design of Stream Ciphers", Springer-verlay, berlin.Heidelberg, 2012.

[15] S. B. Sadkhan, N. A Abbas, "Privacy and Security of Wireless Communication Networks", Book- 2013 Mobile Networks and Cloud Computing Convergence for Progressive Services and Applications, IGI Global

[16] S. B. Sadkhan, Dh. Mohammad, "Hybrid Strategies for Choosing Suitable Cryptosystem Based on Game and Information Theories", 2019 International Engineering Conference (IEC), PP: 95-100

[17] S. B. Sadkhan, Dh. M. Reda, "A Proposed Security Evaluator for Cryptosystem based on Information Theory and Triangular Game", 2018 International Conference on Advanced Science and Engineering (ICOASE), PP: 306- 311.

[18] S. B. Sadkhan, S. F. Jawad, "Complexity Evaluation of Constructing Method for Saturated Best Resilient Functions in Stream Cipher Design", 2019 1st AL-Noor International Conference for Science and Technology (NICST), PP: 85-88

[19] S. B. Sadkhan, Z. Hamza, "Proposed Enhancement of A5/1 stream cipher", 2019 2nd International Conference on Engineering Technology and I ts Applications (IICETA), PP: 111-116