Taylor & Francis
Taylor & Francis Group

Journal of Discrete Mathematical Sciences and Cryptography

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/tdmc20

Design and implementation of a system that preserves the confidentiality of stream cipher in non-linear flow coding

Hussain A. Younis, Israa M. Hayder, Israa Shakir Seger & Hameed Abdul-Kareem Younis

To cite this article: Hussain A. Younis, Israa M. Hayder, Israa Shakir Seger & Hameed Abdul-Kareem Younis (2020) Design and implementation of a system that preserves the confidentiality of stream cipher in non-linear flow coding, Journal of Discrete Mathematical Sciences and Cryptography, 23:7, 1409-1419, DOI: 10.1080/09720529.2020.1714890

To link to this article: https://doi.org/10.1080/09720529.2020.1714890

Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 23 (2020), No. 7, pp. 1409–1419
DOI : 10.1080/09720529.2020.1714890

Taylor & Francis
Taylor & Francis Group

Design and implementation of a system that preserves the confidentiality of stream cipher in non-linear flow coding

Hussain A. Younis *
College of Education for Women
University of Basrah
Basrah
Iraq

Israa M. Hayder
Department of Computer Systems Techniques
Technical Institute/ Qurna
Southern Technical University
Basrah
Iraq

Israa Shakir Seger
Central Library
Al-Muthanna University
Samawah
Al Muthanna
Iraq

Hameed Abdul-Kareem Younis
Department of Computer Science
College of Computer Science & Information Technology
University of Basrah
Basrah
Iraq

Abstract

In this paper, implementation of stream cipher algorithm based on nonlinear combination generator for any given sequences is introduced. The main contribution of this

*E-mail: hussain.younis@uobasrah.edu.iq

work is to enhance the security of this generator and level of complexity is added using logic functions. The proposed scheme was measured through a series of randomness tests.

Subject Classification: *20N05, 20N15, 94A60*

Keywords: *Nonlinear feedback, Shift register, Stream cipher, Measure of randomness.*

1. Introduction

Significant constituent in Streamlined encryption systems are a type of modern cryptographic systems that uses a secret key to decrypt and decrypt . Did not you discover anything about it? That the cryptographic system security algorithm relies on the algorithm to be specific to generate follow-up.

1.1 *A Stream Cipher*

A stream cipher is a method of encrypting text [11](to deliver figure content) in which a cryptographic key and calculation are connected to every paired digit in an information stream, one piece at any given moment. This strategy isn't tremendously utilized in present day cryptography. The principle elective strategy is the square figure wherein a key and calculation are connected to squares of information as opposed to singular bits in a stream. Thus, stream figure is one that encodes a computerized information stream one piece or one byte at any given moment. A square figure is one in which a square of plaintext is treated in general and used to deliver a figure content square of equivalent length [16].

Grouping of figures cryptosystems can either be mystery key and symmetric (AES, DES, RC4), or open key and deviated (ElGamal, McEliece, RSA). In a symmetric framework the sender and recipient have concurred on a mystery key, that is utilized for both encryption and decryption[3]. In a hilter kilter cryptosystem, the sender utilizes the beneficiary's openly accessible open key to scramble, and the collector would then be able to decode with his private key. The possibility of open key cryptography was proposed as of late as 1977 by Diffie and Hellman[20].The first open key cryptosystem was RSA, which was proposed in 1977 by Rivest, Shamir and Adleman [20].The letters RSA are the initials of their surnames. Government Communications Headquarters (GCHQ), a piece of the British insight, later uncovered that a portion of its specialists found open key cryptography earlier[8]. They have likewise discharged beforehand mystery papers to give proof to their cases. However, the credit for the

revelation must stay with the specialists who originally distributed their work in the open logical writing. In mystery key cryptography an open key cryptosystem is regularly used to convey the mystery key [4]. Symmetric cryptosystems is typically separated into square figures and stream figures Rueppel. portrays the distinction as: Block figures work with a fixed change on enormous square of plaintext information; stream figures work with a period differing change on individual plain-content digits[13,1].

A part called a keystream generator creates a grouping of bits, generally known as a keystream [12,19]. In the least difficult type of stream figure, a modulo-2 snake (selective or XOR door) consolidates each piece in the plaintext with each piece in the keystream to create the ciphertext [14]. At the less than desirable end, another modulo-2 viper joins the ciphertext with the keystream to recoup the plaintext.

1.2 *Stream Cipher Properties*

some plan contemplations are: significant lot without any redundancies, measurably irregular, relies upon huge enough key, huge direct multifaceted nature, relationship insusceptibility disarray, dispersion, and utilization of exceptionally non-straight Boolean capacities [2].

2. Security Degree of Stream Cipher Systems

Since the degree of confidentiality of the cryptographic systems depends on the sequence of the key, so this sequence must be characterized by some qualities that achieve a high degree of confidentiality, which are:

- Have good properties, so as to eliminate the linguistic properties of the explicit text which can be useful when breaking the code, so that these properties are not reflected on the encoded text, and if there is repetition in the explicit text will disappear in the encrypted text because it will encode differently Using different parts of the sequential key. For this reason, it is preferable to use streamlined encryption in areas where data is frequently repeated, such as voice communications[5].
- Has a great linear complexity, and this leads to the knowledge that part of the sequence of the key does not benefit the attacker to know the rest, when the attacker knows the explicit text corresponding to a certain amount of text encoded.

- The greater the linear complexity, the greater the degree of confidentiality. The linear complexity of a series is defined as a shorter recorded linear displacement with a linear feedback function that generates the string.
- These properties are obtained when the key sequence is random. However, the key sequence generated in the good flow coding system is semi-random and not entirely arbitrary because it is a periodic series, so the longer the length of the cycle, the better, preferably the length of the message.

2.1 *Correlation Attack*

This method is used to attack nonlinear cryptographic systems based on the nonlinear unification of a number of linear offset registers, which requires knowledge of encrypted text only without having to know the corresponding text [7].

In 1985, research showed a weakness in this type of system, namely, the correlation between a part of the input of the nonlinear function (linear offset output outputs) and the sequence of the key generated by Z [15]. Based on this correlation, it became possible to know some of the linear displacement recorders of the system key which is called a link attack. This means reducing the number of attempts to find the system key when there is a correlation between the input and output of the nonlinear function used in the output of linear offset recorders, where each linear recorder can be independently identified from the rest of the recorders [17].

2.2 *Random Tests*

The random chain has known statistical characteristics, which led to the emergence of several tests to examine the randomness through which we can test the extent of arbitrary sequential key [6].

There are several tests to examine the extent of the randomized random series called local random tests because they test one section (one cycle) of the binary series. In the beginning, the degree of success and failure of the tests should be determined [3]. Therefore, statistical values were used for random sequences. The success rate was considered to be 95%, which is equal to (100-5)% = (1-α)% where α is called the characteristic level of the test [10]. The test is successful when its value is less than or equal to the value of the Chi-square where the grandparent value is at the α-distinct level of the Chi-square distribution. Random tests are [9]:

Table 1
Truth Table of the Hopper (J-K)

Y_2	Y2	Q_n
0	0	Q_{n-1}
0	1	0
1	0	1
1	1	Q_{n-1}

- Frequency test.
- Serial test.
- Poker Test.
- Self Correlation Test.

3. J-K Generator System

This system consists of :

1. k1 and GCD (k1, k2) = 1. Each of them has a linear feedback function that gives the greatest cycle and lengths of k1 and k2.

   whereas:

   k1 = Length (LFSR1) and k1 = Length (LFSR2)

2. The function of the correlation used between the outputs of the displacement recorders is the J-K function as in Figure (1). Table (1) shows the truth table for this function.

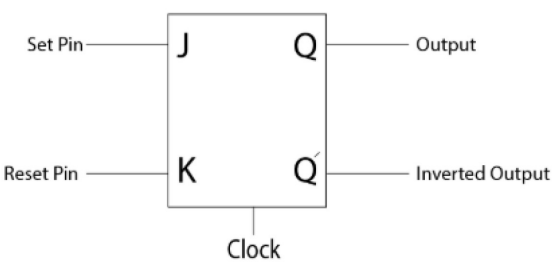

Figure 1
JK Flip-Flop

3.1 *Generator Action Strategy of J-K*

The JK's strategy is to generate the sequence of the key (semi-random series), which is $(2^{k1} - 1)$ $(2^{k2} - 1)$, which is the result of the introduction of the value of the primary registrars and their feedback. After many operations, Scraping and Combining with Standard 2 (Xor).

The mathematical equation used in the Z-series, which is Qn of the J-K function, is:

$$Q_n = (a_n \oplus b_n \oplus 1)Q_{n-1} \oplus a_n \tag{1}$$

Where an, bn are two sequences n in the series y1 and y2 in succession, and the combination function means 2 (XOR).

$$Q_0 = a_0 \tag{2}$$

$$Q_1 = (a_1 \oplus b_1 \oplus 1)a_0 \oplus a_1 \tag{3}$$

$$Q_2 = (a_2 \oplus b_2 \oplus 1)[(a_1 \oplus b_1 \oplus 1)a_0 \oplus a_1] \oplus a_2 \tag{4}$$

which are obviously not linear equations.

4. Developed J-K Generator System

This system consists of:

1. Registers offset each of them with a degree of linear feedback gives the greatest role and lengths K1
2. , K2, 1 = GCD (K1, K2)
3. Since k1 = length (LFSR1) and k1 = length (LFSR2) .
4. The function of the first connection (F): It is a function of hopper J-K as described previously in the form (1) .

a function of urine intention consists of:

- Linking (AND)
- Completely denied (NOT) .
- Combining function with the standard of XOR (2) .

Figure (2) shows the link function of the J-K generator properties

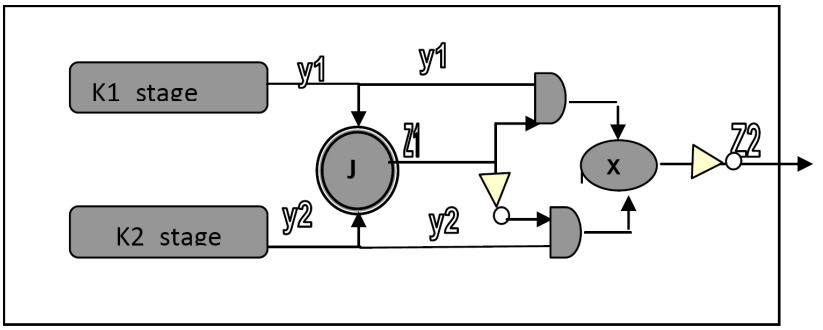

Figure 2

Key generator J-K developer

5. Experiments and Results

Randomized statistical tests were performed on many key values (primary values of resisters and feedback functions) on both generators and in the J-K generator the following results were obtained: (Table 2) shows the results. The tests examined were: Frequency test, Serial test, Poker Test, and Auto Correlation Test.

Experiment (1)

Table

(2) Random statistical tests of fractional series of J-K

No	Keyes		J-K Function			
	Primary Value	Feed Function	Texts of Frequency			
			Frequency test	Serial test	Poker Test	Correlation Test
1	0101	011	1424.	4.087	325	9
	111	110	√	√	X	X
2	110	110	4.087	4.087	30	3
	10	11	X	√	√	√

Table 3

Statistical tests of random string generated by J-K developer

No	Keyes		J-K Function			
	Primary Value	Feed Function	Texts of Frequency			
			Frequency test	Serial test	Poker Test	Correlation Test
1	0101	011	1422.	4.087	283	2
	111	110	√	√	√	√
2	110	110	1.609	.0055	109	2
	10	11	√	√	√	√

The results are shown in Table (3).

Experiment (2)

The development mechanism of the J-K generator has been based on increasing confidentiality by increasing the degree of immunity to the J-K generator chain. The series resulting from the effect of any of the generators using the nonlinear displacement offset technique has a weak correlation or reliability between the generated Z series and some linear offset record outputs.

In this example, we will explain a series of the generator and recognize part of it. We are trying to identify some of the outputs of the displacement registers (LFSR1, LFSR2). It is clear that if the outputs of the resistors are identified, the length and value of the resistors can be known, and thus we have broken the system and attacked it.

In the next experiment we will show an example of the series generated by the J-K generator and the series generated by the J-K generator.

Both series have the same values as resistors and linear feedback functions, and we will demonstrate the strength of the generated J-K generator series compared with the J-K generator series.

Suppose that the initial value of the displacement registers is respectively (111.11).

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

After the implementation of the two generators to produce chains, the following shows:

In the J-K generator series are generated

$$Z = 011001011000101011011$$

And a length of 21

After application

$$\begin{aligned} Q_r &= 0, Q_{r+1} = 0 \longrightarrow a_{r+1} = 0 \\ Q_r &= 0, Q_{r+1} = 1 \longrightarrow a_{r+1} = 1 \\ Q_r &= 0, Q_{r+1} = 0 \longrightarrow b_{r+1} = 0 \\ Q_r &= 0, Q_{r+1} = 1 \longrightarrow b_{r+1} = 0 \end{aligned}$$

We can know some of the outputs of shift register. Attacking it is possible, breaking the system and breaking the code.

the generator J-K developer

The chain was generated

$$Z = 001011001011011001001$$

And application

$$\begin{aligned} Q_r &= 0, Q_{r+1} = 0 \longrightarrow a_{r+1} = 0 \\ Q_r &= 0, Q_{r+1} = 1 \longrightarrow a_{r+1} = 1 \\ Q_r &= 0, Q_{r+1} = 0 \longrightarrow b_{r+1} = 0 \\ Q_r &= 0, Q_{r+1} = 1 \longrightarrow b_{r+1} = 0 \end{aligned}$$

We cannot simply detect the output of the displacement resistors or even some of them because of the linear complexity we have generated on the generator (J-K). Which further complicated the chain (this means a change in the behavior of the J-K generator) as we explained earlier.

From this experience, the link attack failed to obtain the key sequence and break the code in the J-K system compared to the previous J-K system.

6. Conclusion

The power of the streamlined coding system depends on the power of the key generator, which produces a semi-random series with random properties. In this research, the idea of the J-K generator was developed, the development of a generator developed beyond the weakness of the previous generator, a more secretive process and strong resistance to the attackers. This was done by introducing additional logic gates (AND, NOT, XOR) that exceeded the random tests of the J-K generator (frequency test, Serial test, poker test, Auto correlation test) and success. As the attacker, cannot apply the correlation attack on the Z-generated series

to determine the value of linear displacement registers that generated the Z series, which led to increase linear complexity of the Z series. This resulted in a change in J-K generator behavior and thus failure of the link attack to analyze the system and break the code. Several strings (initial record values and different feedback functions) have been applied to the developed J-K system and good results have been obtained.

References

[1] Alaa k., A New Random Keys Generator Depend on Multi Techniques ,*Eng. &Tech Journal*, pp. 427-434. (2015).

[2] Awad, W., mproving Information Security Practices through Computational Intelligence, IGI Global, USA . (2015).

[3] Andrea A. & Lionel B., A Hitchhiker's Guide to Statistical Tests for Assessing Randomized Algorithms in Software Engineering , Technical Report, Simula Research Laboratory, pp. 197-201. (2011).

[4] DHIREN R. P., Information Security : Theory and Practice , Asoke K.Hall of india ,New Delhi. (2008).

[5] Francesco P. & Ugo F. Providing true end-to-end Security in Converged Voice Over IP Infrastructures , Computers & Security, Science Direct, pp. 433–449. (2009).

[6] Gary W. O . A First Course in Design and Analysis of Experiments , (2010). http://creativecommons.org/licenses/by-nc-nd/3.0/.

[7] Hussain A. Y. , Issa A. A., Isra`a M. H. & Hameed A.Y., Adaptive Least-Significant-Bit Substitution Applied in Data Hiding Structure for RGB Image ,*Journal of Engineering and Applied Sciences* , pp. 3754-3760. ., (2019).

[8] Henk C., van T& Sushil Jajodia.2011. Encyclopedia of Cryptography and Security", Springer, USA.

[9] ILPO V., New Tests of Random Numbers For Simulations In Physical System, Thesis, Research Institute for Theoretical Physics University of Helsinki Helsinki, Finland. (1994).

[10] Janet F., Predictiong Negotiation Skills , *Journal of Business And Psychology*, Human Sciences Press pp. 137-165. (1993).

[11] John R.,Vacca H., Computer and Information Security Handbook , Elsevier, USA. pp. 34-36.(2012).

[12] Liang Liu & Jun Ye,Identity-based re-encryption scheme with lightweight re-encryption key generation, *Journal of Discrete Mathematical Sciences and Cryptography*, , (2018).

[13] Md T.U. H., Rajesh K. S., Stream Ciphers Encript Transformation ,International Journal on Computer Science and Engineering , pp. 2836-2837. (2010).

[14] Paris K., N., George P. & Athanassios N. S., FPGA-based Performance Analysis of Stream Ciphers ZUC, Snow3g, Grain V1,Mickey V2, Trivium and E0, Microprocessors and Microsystems journal, Elsevier , pp. 235-245. (2013).

[15] Ram Gopal Sharma, Priti Dimri & Hitendra Garg, Visual cryptographic techniques for secret image sharing: a review, *Information Security Journa*l: A Global Perspective, Volume 27, - Issue 5-6. (2019).

[16] Richard K., Richard E. K. & Neil S., Cryptology: Classical and Modern ,France. (2018).

[17] Staffelbach O.,. Correlation Attacks on Stream Cipher , GRETAG ,Switzerland. (1985)

[18] Suyel N. & Ganesh C. D. Advances of DNA Computing in Cryptography , *Taylor and Francis group*. (2019).

[19] Tim K. & Dave N, Data Network Engineering ,Kluwer Academic publishers, Norwell. USA. (1999).

[20] Whitfield D. & Martin E. H. New Directions in Cryptography, IEEE Transactions on Information Theory, pp. 644–654. (1977).

[21] Abderrahmane Nitaj & Emmanuel Fouotsa (2019) A new attack on RSA and Demytko's elliptic curve cryptosystem, *Journal of Discrete Mathematical Sciences and Cryptography*, 22:3, 391-409, DOI: 10.1080/09720529.2019.1587827

[22] Morteza Norouzi (2019) Normal subfuzzy (*m, n*)-hypermodules, *Journal of Discrete Mathematical Sciences and Cryptography*, 22:3, 433-451, DOI: 10.1080/09720529.2019.1614336

[23] Chung-Ho Chen (2019) Optimal manufacturing target setting by considering process adjustment cost and quality loss, *Journal of Information and Optimization Sciences*, 40:1, 23-27, DOI: 10.1080/02522667.2017.1411016

Received September, 2019