ISSN: 0067-2904

Using the Basic Efficiency Criteria to Estimate the Security of the New Digital Algebraic Generator System (NDAGS)

Mithaq Abdulkareem Abdulwahed*[1], Ayad G. Naser Al-Shammari[2]
[1]Department of Mathematics, College of Science, University of Baghdad, Baghdad, Iraq
[2]Directorate General for Vocational Education Ministry of Education, Baghdad, Iraq

Abstract

The Multiplicative Cyclic Group has been used to construct a New Digital Algebraic Generator System (NDAGS). This cryptosystem can be classified as a stream cipher cryptosystem. In this paper we will estimate the efficiency and security of the (NDAGS) by using the Basic Efficiency Criteria (BEC). A comparison has made between the some known generators and (NDAGS). The results of applying the BEC and the comparison results proof the high efficiency of the (NDAGS).

Keywords: Cryptography, Periodicity, Linear Complexity, Correlation Immunity, Randomness

استخدام مقاييس الكفاءة الاساسية لتخمين امنية منظومة المولد الجبري الرقمي الجديد(NDAGS)

ميثاق عبد الكريم عبد الواحد*[1]، اياد غازي ناصر الشمري[2]
[1]قسم الرياضيات، كلية العلوم، جامعة بغداد، بغداد،العراق
[2] وزارة التربية، المديرية العامة للتعليم المهني، بغداد، العراق

الخلاصة

تم استخدام الزمرة الضربية الدوارة (MCG) لبناء منظومة المولد الجبري الرقمي الجديد (NDAGS). هذه المنظومة يمكن ان تصنف على انها من نظم التشفير الانسيابي. في هذا البحث سوف يتم تخمين كفاءة وامنية لمنظومة (NDAGS) باستخدام مقاييس الكفاءة الاساسية (BEC). تم اجراء عملية مقارنة بين بعض المولدات المعروفة ومنظومة(NDAGS). ان نتائج تطبيق (BEC) ونتائج المقارنة اثبتت الكفاءة العالية لمنظومة (NDAGS) .

1. Introduction

Stream ciphers are an important class of encryption algorithms. They encrypt individual characters (usually binary digits) of a plaintext message one at a time, using an encryption transformation which varies with time. The main properties of stream ciphers separating them from block ciphers are that the encryption function works on individual symbols (letters) of the underlying alphabet and that the encryption function is time-varying [1].

Stream ciphers have extensive applications; many of them are in the area of wireless communication. As an example, they are part of the security framework in GSM networks, Bluetooth or WLANs [2].

*Email: methaq90alheety@gmail.com

2. Basics of New Digital Algebraic Generator [3]

The New Digital Algebraic Generator Unit (NDAGU)[4] considered a new basic unit can be acts as a digital key generator for stream cipher cryptosystems. Let S be the digital sequence generated from NDAGU s.t. S=NDAGU(q,α_1,α_2,k,m), where:

- q is prime number.
- α_1 and α_2 any two generators (primitive elements) of the group MCG to generate numbers of the group from 0 to q-1.
- k any starting point of elements $1\le k\le q-1$.
- m is the digit number of the sequence S, if $s_j \in S$, $0\le s_j<m$.

according to the steps:

Let $x=f(\alpha_1,k,q)$ and $y= f(\alpha_2,x,q)$, $1\le k,x\le q-1$, where $x=k^{\alpha 1} \pmod q$, $y= x^{\alpha 2} \pmod q$ and $s_i=y \text{ div } m$;

We can use NDAGU as a construction unit for NDAG cryptosystem (NDAGS) with Combining Function (CF). If S is the sequence which is generate from NDAGS has a F_n as a combining function with n_NDAGU's then:

$S=F_n(S_1,S_2,\ldots,S_n)$ s.t. $S_i=NDAGU_i(q_i,\alpha_{ti},\alpha_{ri},k_i,m)$, where $1\le i\le n$.

S_i represents the sequence i generate from the NDAGU i.

Its important to define the addition and multiplication operations s.t.:

$s_j = s_{ij} + s_{kj} \pmod m$ $\left.\begin{matrix}\\ \\ \end{matrix}\right\} \in S,\ j=1,2,\ldots$

$s_j = s_{ij} * s_{kj} \pmod m$ $\left.\begin{matrix}\\ \\ \end{matrix}\right\} \in S_i \text{ and } s_{kj}\in S_k,\ 1\le i,k\le n.$

3. Estimation of Basic Criteria for NDAGS Efficiency

In order to use NDAGU or NDAGS as a key generator in cryptography with trust, we must first estimate the theoretical efficiency criterion of them. If these criterions pass the logical calculations of the cryptanalyst, then we can judge that the proposed generator is efficient to be used in cryptography field. Now we are going to deal with these criterions in details.

3.1 Periodicity Criterion [3]

We show before that the Periodicity (P) of single NDAGU is q-1when using MCG $\langle G,*\rangle$ of order q-1.

$P(MCGU) = q-1$

but, $P(NDAGS)=l.c.m\ (q_1-1,q_2-1,\ldots,q_n-1)$

Where q_i is the prime number of NDAGU number i in the NDAGS, since all the numbers q_i-1 are even number then the gcd between $(q_i-1)>1$, so we try to choose q_i grantees that gcd between at most $(q_i-1)=2$.

3.2 Linear Complexity Criterion [5]

Another definition of Linear Complexity (LC) is the minimum number of known sequence digits to deduce the rest unknown digits of the sequence. This definition is developed by Massey in 1969 [6], when he found an algorithm called BerliCamp-Massey, which was first applied on the output of LFSR, so he defined the linear complexity to be "the length of the equivalent minimum LFSR can generate the given sequence". If the length of the result LFSR≥½L, where L is the length of the given sequence, then the sequence has high linear complexity. Table-1 shows P(S) and LC(S) of various NDAGU and NDAGS.

Table 1-P(S) and LC(S) of various NDAGU and NDAGS

n	*primes*	*P(S)*	*L*	*LC(S)*
1	509	508	508	**257**
2	101 997	24900	2000	**1091**
3	**199** **1103** **3607**	**65567878**	**8000**	**4898**

3.3 Correlation Immunity Criterion [7]

The Correlation Immunity (CI) criteria applied on NDAGS only, since we have to compare the sequence S_i which is generated from the NDAGU number i in the NDAGS, with final output sequence S (using m=2 only). Table-2 shows the correlation immunity of various NDAGS

Table 2-the correlation immunity of various NDAGS

N	Primes	L	Pr(x_i)	CI(S)
2	101 997	2000	49.5% 49.9%	2
3	199 1103 3607	5000	50.53% 51.02% 49.76%	3
5	**149** **509** **1051** **1301** **2003**	**8000**	**51.03%** **50.01%** **49.59%** **48.89%** **49.85%**	**5**

3.4 Randomness Criterion [3]

In this subsection we will estimate the Randomness (R) criteria for, binary sequence (m=2) only, generated from NDAG. We hope to discuss the estimation of this criterion for digital sequences (m≥2) generated from NDAG in section 5. In order to test the randomness of NDAGS sequences we plane to apply two kinds of randomness packages, these packages are described as follows:

1. We programmed the first package, using three main tests found by Golomb [8], these tests are Frequency, Run and Auto Correlation test with 10 shifts. These tests are applied on binary sequences only, in this subsection we will develop and generalize these tests to suitable of implementation on digital sequence. Table-3 shows the randomness results of NDAGU and NDAGS on binary sequences using XOR function as a CF.

Table 3-Randomness results of NDAGU and NDAGS on binary sequences.

n	Primes	L	Randomness (P=Pass,F=Fail) Frq Run AC
1	10771	5000	P P P F P P P P P P P P F
2	101 997	8000	P P P P P P F F P P P P F
3	199 1103 3607	10000	P P P P P P F P F P P P

2. The second package, is Crypt-X'98 package [9] which is designed by Information Security Research Centre at Queensland University of Technology to test the stream and block cipher. Applying this package can be considered as a supporting to our work in part (1) of this subsection. The tests of this package are: Periodicity, Linear Complicity, Frequency (F), Binary Derivative (BD), Change Point (CP), Subblock (SB), Run (R) and Sequence Complicity (SC) tests. Table -4 shows the randomness results of NDAGU and NDAGS on binary sequences using XOR function as a CF.

Table 4-Crypt-X'98 randomness results of FDAGU and FDAGS on binary sequences.

n	Primes	L	Crypt-X'98 randomness Tests					
			FT	BDT	CPT	SBT	RT	SCT
1	10771	5000	P	P	P	P	P	P
2	101 997	8000	P	P	P	P	P	P
3	199 1103 3607	10000	P	P	P	P	P	P

4. Theoretical Comparison between NDAGU and LFSR

First, we have to answer why we chose this comparison? As known before that, the LFSR is considered the basic unit of LFSR systems construction, because it has high periodicity and good

randomness. There are many known generators which depend basically on LFSR unit, like Geffe, Brüer, Stop-and-Go,…,etc [5]. The LFSR unit has three basic elements, these elements are: length, tap and initial values (key). The initial key values must be changed periodically (every message, every day, every week,…,etc), so its considered to be secret, but the length and the tap still fixed until the encryption algorithm changed, so they may be public. The NDAGU has the variables q , α_1 , α_2 , k and m which are the components of the initial key. We have to take this concept in consideration when we deal with the following differences:

1. For known algorithm, all the elements of every basic unit are known accept the initial key, so the length and tap of LFSR unit are public, but all the variables of the NDAGU still unknown.
2. The periodicity of the sequence generated from LFSR unit with length q (not necessary prime) is 2^q-1, but the period of the sequence generated from FDAGU is q-1 for each choice of two primitive elements, this period can be increased by
3. changing the choice every (q-1) length from the generated sequence, so the new period will be (q-1)*ϕ(q-1)*(ϕ(q-1)-1).
4. The common generated sequence from LFSR is binary, but in NDAGU, the sequence is digital ($1<m\leq(q-1)/2$).
5. The length, tap and initial values of LFSR unit can be detected from some available length of the generated sequence by using, for example Massey algorithm [6], but it is not easy to find the initial value of the NDAGU because of the high non-linearity of the function g.

5. Testing the DS Generated from NDAGS

In this section we will test the digital sequences generated by NDAGS by using the Digital Randomness Tests (DRT) introduced by [10].

Now we will test three different digital sequences for m=3, 5 and 7, with different length L=2000, 5000 and 8000 digits respectively. All these sequences are generated from different linear NDAGS's (CF is XOR function) have the initial keys described in Table-5.

Table 5-he Three NDAGS's initial key

NDAGS	N	q_i	α_{1i}	α_{2i}	k_i	m
1	2	101 997	2 7	8 855	1 1	3
2	3	199 1103 3607	3 5 5	44 125 3125	1 1 1	5
3	5	149 509 1051 1301 2003	2 2 7 2 5	8 8 567 8 125	1 1 1 1 1	7

The three following tables (Tables -6, 7, 8)) show the randomness test results of the three DS mentioned above by using DRT.

Table 6-DRT results of NDAGS output with L=2000 for m=3.

Test	T^* Value	υ	Pass Value T_0
Frequency	2.428	2	6.01
Run	6.971 7.229 6.63	6 6 5	12.31 12.31 10.97
Auto Correlation	No# of fail values $0.0\leq T_A(\tau)\leq 14.238$ 0.05% for 500 shift	1	3.81

Table 7-DRT results of NDAGS output with L=5000 for m=5.

Test	T^* Value	υ	Pass Value T_0
Frequency	2.294	4	9.52
Run	1.4	3	7.84
	3.49	4	9.52
	5.73	4	9.52
	6.62	3	7.84
	10.99	4	9.52
Auto Correlation	No# of fail value $0.0 \le T_A(\tau) \le 9.465$ 0.07% for 500 shift	1	3.81

Table 8-DRT results of NDAGS output with L=8000 for m=7.

Test	T^* Value	υ	Pass Value T_0
Frequency	6.992	6	12.309
Run	2.997	4	9.52
	3.458	3	7.84
	7.088	4	9.52
	5.982	3	7.84
	6.283	3	7.84
	1.823	3	7.84
	3.429	3	7.84
Auto Correlation	No# of fail values $0.0 \le T_A(\tau) \le 15.899$ 0.068% for 500 shift	1	3.81

Tables-(6, 7, 8) prove the randomness properties of the digital sequences generate from various NDAGS's with different m (m= 3, 5 and 7).

6. Practical Comparison between NDAGS and Other Generators

In this section, we try to make a comparison study between NDAGS and other generators, for digital sequences with L=5000 and m=10 for the compared generators. Of course, the first generator is the NDAGS number two which is mentioned in Table-9 of the previous section. The second is the binary LFSR and RNG.

6.1 Practical Comparison between NDAGS and LFSR

In this subsection we chose binary LFSR with length 31 and the 3rd stage tapping as a connection function, in order to get DS, we have to choose 4 bits from four different positions from the LFSR. The four bits transformed to hex (0..15) if we take mod 10, we get a DS with m=10. Table-9 shows the DRT results of DS generated from NDAGS and LFSR.

Table 9-practical comparison between NDAGS and LFSR results

Test	DPES			LFSR		
	T^*	υ	T_0	T^*	υ	T_0
Freq.	4.05	9	16.95	402.6	9	16.95
Run	1.30	2	6.01	39.28	2	6.01
	0.93	2	7.84	39.06	2	6.01
	1.88	3	7.84	27.22	4	9.52
	1.99	2	6.01	7.49	2	6.01
	2.86	2	6.01	29.42	3	7.84
	0.99	2	6.01	18.39	2	6.01
	0.42	2	6.01	51.60	2	6.01
	2.78	2	6.01	34.47	1	3.81
	1.04	3	7.84	48.51	2	6.01
	3.30	2	6.01	58.17	2	6.01
A.C.	No# of fail values 0.0≤T≤5.4 0.06% for 500 shift	1	3.81	No# of fail values 4.04≤T≤16.64 44.5% for 500 shift	1	3.81

From Table-9 we conclude that NDAGS randomness results are more better from randomness results of LFSR, but this not mean that the LFSR has no randomness properties.

6.2 Practical Comparison between NDAGS and RNG

In the same comparison study, we can show that the Random Number Generator (RNG) which is found by Mitchell [11], it is a digital generator (m=10 only) with good random sequence, but it has low complexity, with period less or equal q-1 for some primes. We expect that the choices of the primes will drop to 35% in order to gain period equal q-1, while the choices of NDAGS still open to all primes. Table-10 shows the period of some primes for RNG system with frequencies of the sequence digits.

Table 10-periods of RNG primes and frequencies of sequences digits

Primes	***Period***	***Frequencies***									
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
991	495	55	54	59	45	45	52	52	39	46	48
997	166	29	14	18	15	11	11	14	18	13	23
1003	464	52	36	52	60	36	53	32	39	55	49
1013	253	26	29	29	22	20	26	29	26	25	31
1019	1018	103	102	102	102	102	102	101	101	102	101

Lets now take q=997 to generate 996-digits sequence (using α_1=7, α_2=885 and k=1) to compared with same q for RNG in Table-11 calculating the Standard Deviation (SD), of the frequency of sequence digits, from the average.

Table 11-SD deviation of the sequences digits from the average

Gen.	***Period (L)***	***Frequency***										***SD***
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	
NDAGS	996	99	100	100	100	99	100	99	100	100	100	0.52
RNG	166	29	14	18	15	11	11	14	18	13	23	5.68

We notice that the frequencies of digits of RNG have high deviation (SD=5.68) from the expected value (16.6), but the frequencies of digits of NDAGS have low (SD=0.52) from the expected value (99.6), so we conclude that the frequencies of digits of NDAGS are uniform distribution.

7. Conclusions

i. From the comparison between NDAGU and LFSR, the following differences are obtained:

ii. For unknown cryptosystem, consists of LFSR's, then the variables are the length, tap and initial values of each LFSR are unknown, but for NDAGS variables are α_{ti},α_{ri},q_i,k_i and m are all unknowns.

iii. For known algorithm, the initial values of each LFSR is unknown only, but in NDAGS, α_{ti}, α_{ri}, q_i, k_i are unknown which are can be considered as initial values.

iv. The local periodicity of the generated sequence of LFSR with length r is 2^r-1, but the period of the sequence generated from NDAGU is $P_2^{g(q)}$*(q-1), where $P_2^{g(q)}$ is the permutation of 2 from g(q).

v. The common generated sequence from LFSR is binary, but in MMCGU, the sequence is digital ($1<m\leq q-1$).

1. The NDAGU can be developed to increase its periodicity, complexity and randomness by using other non-used generators of G to generate new A(q).
2. We can construct an efficient stream cipher cryptosystem depends on combination of number of LFSR's and NDAGU's.

References

1. Ekdhal, P. **2003**. "On LFSR based Stream Ciphers Analysis and Design**"**, Ph.D. Thesis.

2. Rechberger, C. **2004**. "Side Channel Analysis of Stream Ciphers", Master's Thesis, Institute for Applied Information Processing and Communications (IAIK) Graz University of Technology, Graz, Austria.

3. Schneier B. **1995**. "*Applied Cryptography*", John Wiley & Sons.

4. Abdulwahed and Al-Shammari. **2018. "**Construct a New System as a Combining Function for the LFSR in the Stream Cipher Systems Using Multiplicative Cyclic Group**",** *Iraqi Journal of Science*, **59**(3B): 1490-1500

5. Rivest, R. L. **1997**. "*Hand Book of Applied Cryptography*", John Wiley & Sons.

6. Massey, J.L. **1969**. "Shift Register Synthesis and BCH Decoding", *IEEE Transaction on Information Theory*, **IT-15**(1).

7. Staffelbach, O. J. and Meier, W. **1988**. "*Fast Correlation Attack on Stream Cipher*", Springer-Verlag,

8. Golomb, S.W. **1982**. "*Shift Register Sequences*" San Francisco: Holden Day 1967,(Reprinted by Aegean Park Press in 1982).

9. Gustafson, H., Dawson, E. Nielsen, L. and Caelli, W. **1988**. "*A Computer Package for Measuring the Strength of Encryption Algorithm*", Information Security Research Centre at Queensland University of Technology.

10. Ali, F. H., Ahmed, S. M. and Shamran, M. U. **2009**. "Generalize the Randomness Tests to Test the Digital Sequences Produced from Digital Stream Cipher Systems", *Iraqi Journal for Science*, Baghdad University, College of Science.

11. Mitchell, D. W. **1993**. "*A Nonlinear Random Number Generator with Known, Long Cycle Length*", Dept. of Economics, West Virginia University, Morgantown WV 26506-602 USA.