The Study of Sensitivity of R.A NMJ Algorithm

Abderrahim SABOUR

University Cadi Ayyad, Morocco

Summary
In this article, we will propose a study of the dynamis characteristics of the R.A NMJ algorithm which is a new regenerator of pseudo-random sequences. The objective is to put obviously the chaotic behavior of this regenerator through the calculation of the largest exhibitor of Lyapunov towards many disturbances. This process will allow us to explain the interest of this study on the vulnerability of our algorithm since the injection of a perturbation has the same effect as an error in estimation, where the interest of this study comes from.

Key words:
vulnerability of algorithm R.A NMJ, propagation of the estimation errors, Lyapunov exponent.

1. Introduction

The validation of a regenerator of binary sequences for cryptography use is done in two main parts. In the first part, we will analyse the statistical characteristics of the regenerated sequences. The success of these tests does not imply the surety of the generator, whereas their failure means that we should let down this regenerator. Only after the success of the first validation tests, we will move to the second validation test which depends both on the algorithm and on the mechanisms it uses. In other words each regenerator class has its own tests. Those tests are related to the called procedures in the regenerator class. The R.A NMJ algorithm is a regenerator of binary sequences that are cryptographically safe inspired from genetic algorithms and mainly based on functions and on three state functions. This regenerator associates to each password a population of initial individuals and after a maturation phase through nonlinear dissipative transformed with compensation. The system enters in an iterative process and at each iteration, each population individual will contribute in the binary sequence.
Our interest in the sensibility of disturbances is due to the fact that it can be seen as estimation errors of the cryptanalysis. In other words the system is determinist and we cannot speak about disturbances in the general sense of the term, but their usefulness consists in the analysis of the influence of estimation errors on the prediction of the subsequent states of the system. The study of the chaotic behaviour of a system begins with the analyse of its dynamic characteristics [6][1], whose most important are: its sensibility to initial conditions and to disturbances in the neighbourhood of the attractors. These two characteristics are qualified by determination of Lyapunov's exponents of the system which is not always possible, and is reduced to the determination of the Lyapunov's biggest exponent.

In this article we will study the dynamic of the R.A NMJ algorithm [10][14] : its sensibility to the initial conditions (sensibility to changes in the bits of a password) [14] and its sensibility towards disturbances (changes in the bits of Data block of an individual or changes in position of an individual towards the other population individuals) in the attractors neighbourhoods. This study is justified since the R.A NMJ algorithm simulates a dynamic system, dissipative under compensation, which uses the complexity of evolutionist algorithm, and utilize their suppleness and adapt them for the regeneration of binary sequences that are cryptographically safe. The definition of a distance of all the populations, based on data blocks of the individuals, allowed us to study of the influence of a disturbance on a given population in comparison with a reference population. This allows in one hand, the analysis of the nature of the convergence of the distance evolution in each iteration of the disturbed population in comparison with a reference population, and in the other hand the determination of the bigger Lyapunov exponent of the system.

2. Definitions

Definition 1
Let $a = a_0...a_{n-1}$ and $b = b_0...b_{n-1}$ two words formed by symbols *ai* et *bi* that are elements of a given set. The Hamming distance [3] is defined by:
$d_H(a,b) = \#\{\mathrm{i} \in \{0,...,\mathrm{n\text{-}1}\} / \mathrm{a_i} \neq b_i\}$

Definition 2. Let P1 and P2 be two populations of the same number of individuals N and of same size of the Data blocks. We define the distance between two populations P1 and P2 by :

$$dis(P_1,P_2) = \sum_{i=1}^{N} d_H(P_1\_Data(i), P_2\_Data(i))$$

With $P_j\_Data(i)$ the Data block of the individual *i* of the population P_j.

Definition 3 (see [2][7])

Manuscript received January 5, 2012
Manuscript revised January 20, 2012

Let X_0 and $X_1=X_0+\mu$ be two initial conditions for a system and $P_1(t)$ and $P_2(t)$ be two states of the system at the iteration t such that $P_1(0) = X_0$ and $P_2(0) = X_0+\mu$. If there exists a moment t_m, a real constant λ and a real constant a such that :

$$\forall t \in [0, t_m],\ dis(P_1(t), P_2(t)) \sim e^{\lambda t + a}$$

λ is called Lyapunov exponent.

We understand that Lyapunov exponent characterises the chaotic quality of a system because it accounts for the sensitivity under initial conditions.

Definition 4

A chaotic system is a system whose Lyapunov exponent [1] is strictly positive.

Definition 5

Let M_1 and M_2 be key words of same size T in bytes, the standarized distance ε between M_1 and M_2 is defined by:

$$\varepsilon = \varepsilon(M_1, M_2) = \frac{d_H(M_1, M_2)}{8T}$$

3. Sensitivity under initial conditions

The sensibility to initial conditions [1] constitutes absolutely the main characteristic of chaotic systems. Whatever is the nearness of two initial states, the outcome trajectories of these two states diverges rapidly the one from the other. However, they remain linked to the same attractor thus confined in a delimited space. This has as consequences:

- The most insignificant noise corrupts absolutely the knowledge of the future states of the system. In fact, the divergence of trajectories in a delimited space means that they are rapidly uncorrelated. As a result, although the system is determinist, no long-term prediction is possible.
- If the system is a loop-system, the noise of measure can therefore corrupt profoundly the dynamics of whole system. Its behaviour is then changed in a radical way without proportion with the precision of measures.
- The slightest disturbance of the system can eventually drive to extremely different states. An insignificant event therefore does not have insignificant consequences always. This characteristic was noticed for the first time by E. Lorenz [5] on his meteorological model, it is known under the popular name of butterfly effect.

Remark

One of the challenges that the R.A NMJ algorithm should win is the creation of the initial population associated to an arbitrary password (process I). The use of transforms based on three states functions allows the resolution of this problem. The contribution of bits of a password to this population depends on the parameters of the class of three states, on the width (in bits) of a password and on the length of the Data blocks of the individuals.

3.1 Justification of the choice of characteristics of the three states class

Before starting the study of the chaotic behavior of R.A NMJ, we justify in the first part the choice of the platform which is made at the time of the creation of the initial population. The observer permits the transition of the key word to the Data blocks of the initial population. The general form is G =[X,Y,Z,T] and the associated values of DX, DY, DZ et DT authenticates the set of observers involved.

The original version of R.A NMJ, uses a class of three states functions defined by:

$\mathbf{D_X}$= |2 :7|, $\mathbf{D_Y}$=|1 :6|, $\mathbf{D_Z}$=|2 :7|, $\mathbf{D_T}$= |1 :5|

With 16 characters as Data block size of each individual and, in this case, regenerates a population of 2160 individuals since the values of DX, DY, DZ and DT determine the number of individuals of the population which is worth: 1080=(7-2+1).(6-1+1).6.5, and this version runs at each state the key word in both directions, this implies doubling the size of the population, which will give 2160 individuals.

Remarks

- The choice of a small population with individuals with small data blocks is done to simulate extreme conditions
- The objective is the study of the capacity of the system in amplifying the differences between very correlated passwords. Where from we are interested to the first 100 iteration of the process III.
- The process II was ignored to allow a treatment with a reduce size of data.
- The class of used functions is defined by the sets $\mathbf{D_X}$, $\mathbf{D_Y}$, $\mathbf{D_Z}$ and $\mathbf{D_T}$ allow the determination of the number of individuals of the population, which is equal to 162 individuals.

3.2 Contribution of password bits

This part has as aim the study of the contribution of password bits in the regeneration of data blocks of individuals of the initial population. The fact of using transforms based on three states functions α, β and λ, in which β corresponds to a systematic ignorance of a bits number, what justifies this study. We remark that only the length of the password and the parameters of the class of function have influence on this distribution. The diagrams **U1**, **U2**, **U3**, **U4** and **U5** of the following figure

represents the contribution of bits associated respectively to passwords of 64, 128, 256, 512 et 1024 bits. The x-axis represents the bits of the password, the y-axis corresponds to the number of contributions of the bits in the data blocks.

Remarks

- The total amount of the Data Block (the Data Block size multiplied by the number of individuals of the population) of all the individuals is equal , in this case, to 3888 bits, an equiprobable distribution on the bits of the 5 tested passwords with length : 64, 128, 256, 512 and 1024 bits will give us respectively 3888/64=60.75, 3888/128=30,375, 3888/256=15,1875, 3888/512=7,59375 and 3888/1024=3,796875.
- The presented symmetry in this distribution is owed to the parsing, during the creation of the initial population, of the password in the both directions for each given observer.
- The diagrams **U1**, **U2**, **U3**, **U4** and **U5**, associated respectively to the password with length 64, 128, 256, 512 and 1024 bits, presents a contribution, almost equiprobable, of the different bits of the passwords.

In what follows, we will study the sensibility of the R.A NMJ algorithm towards initial conditions.

Remarks

- A good valuation of the total stability of a dynamic system begins with the valuation of the Lyapunov exponent witch gives us the average dilatation of each axis of a hyper- sphere defined by the phases space [4].
- The measure of the biggest Lyapunov exponent needs to iterate the dynamic of the model for two very close initial conditions, and to measure at the end of finite time the distance between two diagrams. To validate this counting, it is needed of course that these two initial conditions be located close to the attractor.

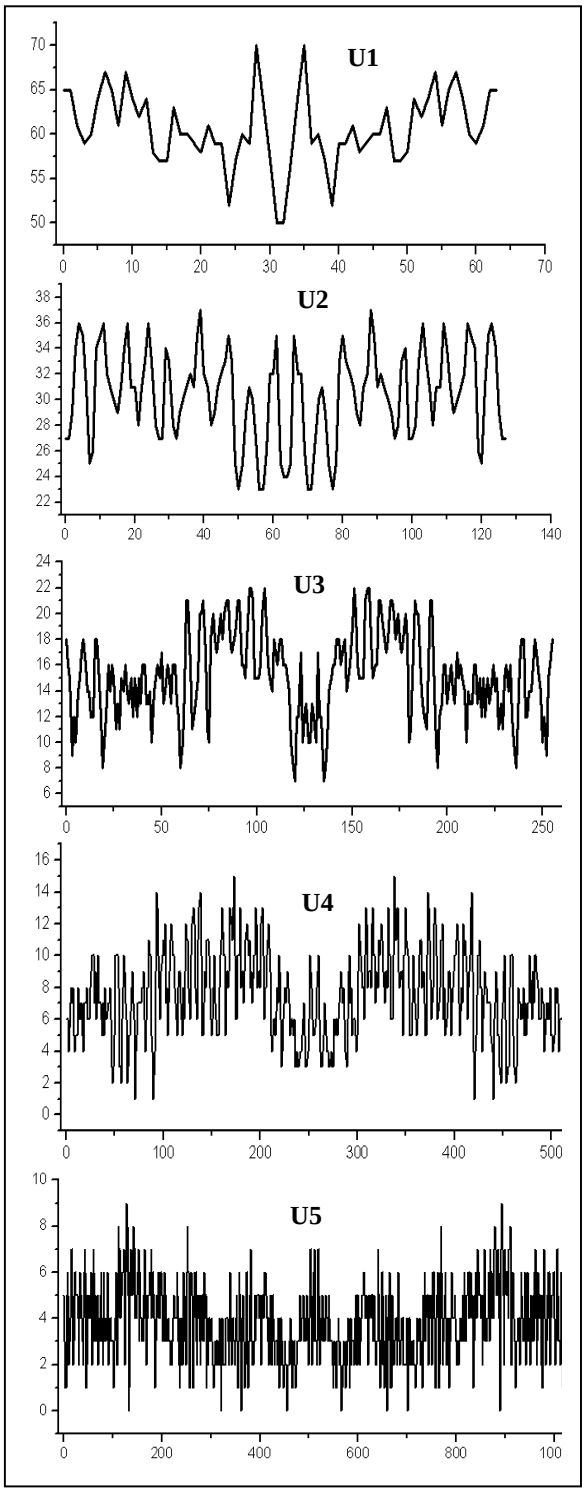

Fig. 1 Contribution of the password bits in the data block of the individuals.

4. Variation of the distance between the passwords

During the first test the value of ε was fixed at 0.016, in this part we will study the sensibility of the system towards lower values, chosen passwords, for a given ε :
They have the same length T.
Only the 8th bit is modified.
Password has more and more weak entropies.
for ε = 0,0052 : the used passwords have 24 characters:
M1= ‘bbbbbbbbbbbbbbbbbbbbbbbb’
M2= ‘cbbbbbbbbbbbbbbbbbbbbbbb’
for ε = 0,0026 : the used passwords have 48 characters:
M1= ‘bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb’
M2= ‘cbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb’
for ε = 0,0017 : the used passwords have 71 characters:
M1= ‘bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb’
M2= ‘cbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb’
for ε = 8.8028e-004 : the used passwords have 142 characters:
M1= ‘bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb’
M2= ‘cbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb’

The following table shows the results of the evolution of the distance between two populations associated to two passwords M1 et M2 with the same length T,
tableau suivant dresse les résultats de l’évolution de la distance entre deux populations associées aux deux mots de passe M1 et M2 de même taille T, according to the value of ε .
As we can figure out, we achieve a sensibility towards disturbances in the order of $1/\text{Ms0} = 1/276480 \approx 3*10^{-6}$ and this without any modification. Since each bit which arrives to bypass the process II will absolutely influence the evolution of the system.

	ε	
ITi	**V1**	**V3**
Mi	**V2**	**V4**

ETi: presents the iteration number i.
V1: presents the Hamming distance between two populations.
V2: the percent of the different bits between two populations V2=V1/Mi.
Msi: is the size of the Data block of the individuals of the population in the iteration number i.
V3: Lyapunov expoment for the individuals $V3 = Log\left(V1/\text{N}\right)$ in which N is the number of the individuals of the population.
V4 : Lyapunov exponent for the two populations $V4 = Log(V1)$.
Remarks

To interpret the value V2, we consider two random binary sequences S1 and S2, so the probability for one bit of S1 or S2 to be equal to 0 or 1 is 0.5. so the probability for bit number k of S1 to be equal to the bit number k of S2 is 0.5. which gives us 0.5 as optimal value for V2, we are close the that value already from the first iterations. This value is more significant then V3 and V4 since it does not depend on the individuals number and on the size of the data block, unlike V3 which depends on the size of individuals and V4 which depends on their number.
The following table presents the obtained results using the original version of the algorithm R.A NMJ which is characterized with the values: DX=|2 :7|, DY=|1 :6|, DZ=|2 :7| et DT= |1 :5| with 16 bytes as size of Data Block of the 2160 individuals, the size of this block is doubles three times the process II to obtain a population with individuals with Data blocks of 128 bytes.

Table 1: The evolution of the distance between populations

	$\varepsilon = 0{,}005$		$\varepsilon = 0.0026$		$\varepsilon = 0.0017$		$\varepsilon = 0.00088$	
Initial Ms0= 276480	1459	-0.39	666	-1.17	499	-1.46	247	-2.16
	0.52 %	7.28	0.24 %	6.05	0.18 %	6.21	0.089 %	5.5
IT1 Ms1= 552960	214782	4.59	208742	4.57	208446	4.56	187937	4.46
	38.84 %	12.27	37.74 %	12.24	37.69 %	12.24	33.98 %	12.14
IT2 Ms2= 1105920	550685	5.54	549936	5.53	551153	5.54	550519	5.54
	49.79 %	13.21	49.72 %	13.21	49.83 %	13.21	49.77%	13.21
IT3 Ms3= 2211840	1106136	2.47	1104510	6.23	1105961	6.23	1105876	6.23
	50.00 %	13.91	49.93 %	13.91	50.00 %	13.91	49.99 %	13.91
IT4 Ms4= 2211840	1105900	6.23	1104823	6.23	1106413	6.23	1104222	6.23
	49.99 %	13.91	49.95 %	13.91	50.02 %	13.91	49.92 %	13.91
IT5 Ms5= 2211840	1105213	6.23	1105017	6.23	1106747	6.23	1105601	6.23
	49.96 %	13.91	49.95 %	13.91	50.03 %	13.91	49.98 %	13.91

5. Sensibility towards disturbance in the neighborhood of an attractor

The first part of this article, devoted to the study of the chaotic behavior of the R.A NMJ algorithm, has as purpose the analysis of the sensibility towards initial conditions. The test results showed a big sensibility to the initial conditions. These results gave sense to the study of the chaotic characteristics of the R.A NMJ algorithm. In this paragraph, we will study the sensibility in the neighborhood of an attractor. This characteristic is very important due to the fact that the more the system is sensible toward disturbances in neighborhood of an attractor the more the prediction is difficult. In that case even a very weak estimation error, which can be considered as disturbance, can lead to totally different results and guaranteeing a strong undecidability for the system. In other words, an error in the estimation of one of the system parameters, even in the neighborhood of an

attractor, has a divergence between the real status and the estimates status of the system. The main problem is linked to the determination of the system attractors, thing that is indispensable to measure the sensibility towards disturbances on the systems in their neighborhood.

The system attractors that the R.A NMJ algorithm simulates are difficult to determine because of the non-mastering of the functioning of the system. To bypass this constraint we adopt the following procedure:

1. We start from a population created from an arbitrary password.
2. We iterate the process III many times.
3. We apply a disturbance to the system.
4. We calculate the divergence between the disturbed system and non-disturbed one.

Remarks

The choice of the initial state (the password and the associated population) must have a minimal influence while studying the sensibility towards disturbances in neighbourhood of an attractor. The necessity of iterating the process III many times (10^6 iterations in our test), lets the functions of the system to allow the system to decrease the impact of the initial state, which leads to the appearance of the attractors.

The process II is ignored because this process doubles the size of the individuals at each iteration and this enlarges exponentially the existence space of the individuals

5.1 The characteristics of a population

In this part, we will study the evolution of a population having the following properties:

1) The password is "bbbbbbbb": the choice of the password is arbitrary since the fact of iterating 1000000 the process III will strongly decrease the dependency of the system to the initial conditions.

2) The used class for the creation of the initial population is defined by: DX= |2 :4|, DY=|4 :6|, DZ=|5 :6| et DT= |4 :5|.

3) The size of the Data bock of each individual is 2 characters (instead of 3 characters for the tests sensibility towards initial conditions).

4) We iterate one million times the process III of the R.A NMJ algorithm.

5) We inject a disturbance in the system and we calculate the divergence the disturbed population in comparison with a reference population.

6) We are interested on the divergence of the two populations in the 500 iteration after the injection of the disturbance.

5.2 The disturbances in the neighborhood of the attractors

In these tests, two types of disturbances are defined: The modification of the status of a set of bits of the Data blocks of individuals at a given moment. To allow a robust test, we fix the number of the bits to change to one bit. Changing one bit corresponds to a modification of 0.086 % of the Data block (this value depends on the number of individuals (Nb_ind) and on the size of the Data block (T_bd) : $(NB\_ind * T\_bd)^{-1} = (72 * 16)^{-1}$).

The second test is linked to the distribution of the individuals at a given time. This distribution will evolve with the help of the order function. Thus two kinds of disturbances are tested:

The modification of one bit in the Data block of a given individual: this test allows the study of the influence of the modification of Data block one bit and the study of the influence of this modification on the evolution of the system.

The modification of the position of a given individual: this test allows the study of the influence of the modification of position of one individual on the evolution of the system.

5.2.a Changing the bit

The mating functions I and II are the only ones able of changing the Data block of the individuals of given population. This test has as purpose the study of the influence of the modification of one bit on the evolution of the population. The choice of the bit to modify ($0 \rightarrow 1$) or ($1 \rightarrow 0$) is arbitrary, since it is enough to give the index of the individual and the index of the bit of the Data bock to modify. For example the two following figures presents respectively the results of the modification of the 5th bit of the Data Bloc of the individual 20.

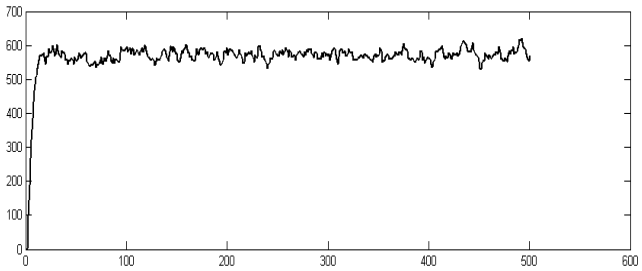

Figure 2: Evolution of the distance between two populations after changing one bit

The X-axis presents the iterations of the process III (500 iterations) after changing the bit 5 of the individual 20, the Y-axis presents the distance between the two populations (disturbed and reference population), it is stabilized and

converges towards the half of the sum of the length of the Data block of the individuals.
The following figure presents the evolution of the Lyapunov exponent after changing the bit of the Data block of an individual.

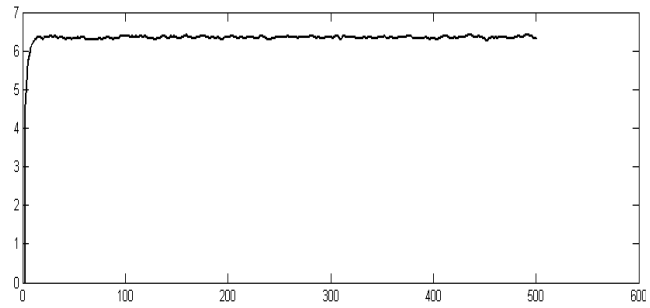

Figure 3: Evolution of the Lyapunov exponent after changing one bit

We determine a quick convergence of the diagram towards the value $\lambda = 6.3475$, which corresponds to the biggest Lyapunov exponent.

5.2.b Changing the position

The order function camouflages the distribution of the individuals at a given instant, by applying a sequence shift based on the Control Block of the individuals in conflict. We mention that the Control block of the shifted individuals does not change. This test will analyze the influence of the modification of an individual on the system.

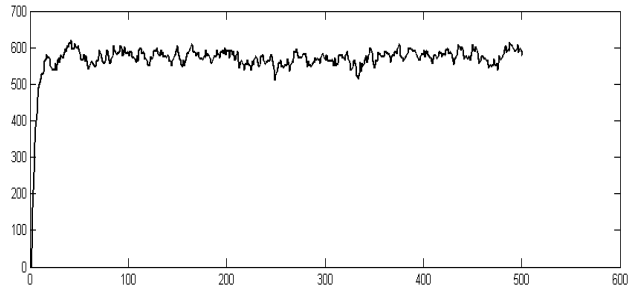

Figure 4 : Evolution of the distance between two populations after changing the position of a given individual

The X-axis presents the iterations of the process III (500 iterations), the Y-axis presents the distance between the two populations.
We notice that, the system is stabilized and converges towards the half of the sum of the length of the Data block of the individuals of one of the populations.
The following figure presents the evolution of the Lyapunov exponent after changing the position of a given individual

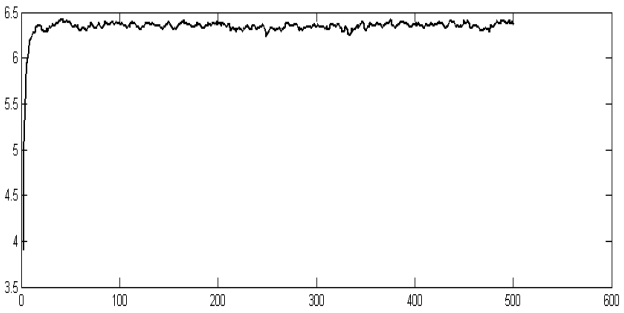

Figure 5: Evolution of the Lyapunov exponent after changing the position of a given individual

Remark
These two tests allow an explicit valuation of the vulnerability of this cryptosystem. But they are far from being uncorrelated due to the fact that the process III, which will be iterated, is a succession of calls of the order function and the mating function II. So a disturbance of the distribution of the individuals will lead, sooner or later(This depends on the number of individuals in mating at an iteration of the process III), to the mating of two individuals, a mating that is due to the spread of the initial disturbance.
For a trajectory to be chaotic or unstable, it is necessary that at least one of the Lyapunov's exponents must be positive. In fact in our case, it is enough to consider the biggest exponent to conclude on the stability of a diagram.

6. Conclusion

Understanding how the system amplifies these perturbations will impose to follow the evolution of the system across the miscellaneous process. The process I is only corresponding to a password a population of individuals. The process II and III spreads the disturbances in two different ways:
Low spread: We only double the size of the Data block of individuals at each iteration, in addition each affected individual will affect his mate during the mating, which is also going to affect others
High spread: as soon as one of its affected bits arrives to the control block of the individual, three cases are possible: When the sub-mating block is affected, this will modify the parameters of the mating function and this will give birth to disturbing individuals, and will lead to the deviation of both populations.
The priority sub-block will disturb the distribution of the population individuals. This modification of the position will impose, at the moment of the mating function, different couples which will lead to the deviation of both populations.
The contribution sub-block: (only process III) this disturbance will affect the choice of the three state

function that will be used for the contribution of the individual in the mask, without any disturbance of the system.

The obtained results showed that R.A NMJ is a chaotic system very sensitive to the initial state and generates enormous effect. This sensitivity does not allow the reduction of the research space at the time of an exhaustive attack via key words numbering. The study of the chaotic behavior of R.A NMJ is not finished, since it remains to determine the attractors of this latter and their characteristics in term of the number of the individuals, of the Data block size and the parameters of classes of three states functions used in the different steps.

References

[1] G.L. Baker, J.P. Gollub, Chaotic Dynamics, an Introduction, 2nd Edition (Cambridge Univ. Press,Cambridge, 1996).

[2] J.P. Eckmann, D. Ruelle, Ergodic theory of chaos and strange attractors, Reviews of Modern Physics, Vol.57, N°3, Part I, 1985, pp. 622,623.

[3] Richard Hamming error-detecting and error-correcting codes Bell System Technical Journal 29(2):147-160, 1950

[4] R.C. Hilborn, "Chaos ans Nonlinear Dynamics", 1994, Oxford University Press Acton, F.S., 1990, _Numerical methods that work, Corrected edition, Washington, Mathematical Association of America.

[5] E. LORENZ, Deterministic Nonperiodic Flow, J. Atmos. Sci. Vol.20 pp.130-141.

[6] C. MIRA, Cours de systèmes asservis non linéaires, Dunod, Paris, 1969, p.12.

[7] E. Ott, Chaos in Dynamical Systems (Cambridge Univ. Press, Cambridge, 1993).

[8] A. Sabour, A. Asimi and A. Lbekkouri, Etude théorique de l'observateur : Fonctions dissipatives du R.A NMJ, Les journées d'Optique et du traitement de l'information « OPTIQUE'06 », Rabat 2006.

[9] A. Sabour, A. Asimi and A. Lbekkouri, Genetic Regenerator of pseudo-random sequences R.A NMJ, International Symposium on AI 50 Years' Achievements, Future Directions and Social Impacts (ISAI'06), Aug. 1-3, 2006, Beijing, P.R.China.

[10] A. Sabour, A. Asimi and A. Lbekkouri, Etude du Comportement Chaotique du R.A NMJ via la Sensibilité aux conditions Initiales. 3rd International Symposium on Image/Video Communications over fixed and mobile networks, Tunisia 2006

[11] A. Sabour, A. Asimi and A. Lbekkouri, Régénérateur génétique des suites binaires cryptographiquement sûres R.A NMJ, Colloque International Sur l'Informatique et ses Applications IA'2006 Oujda, 31 Octobre, 1 et 2 Novembre 2006

[12] A. Sabour, A. Asimi , A. Lbekkouri and H. Bouyakhf, Etude de la Complexité des Classes de Fonctions à Trois Etats, The Maghrebian Conference on Sofware Engineering and Artificial Intelligence (MCSEAI'06), Agadir Morocco, December 07 to 09, 2006

[13] A. Sabour, A. Asimi and A. Lbekkouri, Genetic Regenerator of pseudo-random sequences R.A NMJ, IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.1, January 2007

[14] A. Sabour, A. Asimi and A. Lbekkouri, Study of the Chaotic Behaviour of R.A NMJ Via Sensitivity Under Initial Conditions, 3rd International Symposium on Computational Intelligence and Intelligent Informatics ISCIII2007 Agadir Morocco, March 28 to 30, 2007

[15] A. Sabour, A. Asimi and A. Lbekkouri, THE THREE STATES FUNCTIONS: THEORETICAL FOUNDATIONS AND ESTIMATED COMPLEXITY, The 3rd International Conference on Information Technology ICIT 2007, May 9-11, 2007 AL-Zaytoonah University, Amman, Jordan

Abderrahim SABOUR received his PhD degree in Computer Science from the University Mohammed V-Agdal in 2007. His research interest includes artificial intelligence and computer security. He is an assistant professor at the Cadi Ayyad University since 2009.