THE THREE STATES FUNCTIONS : THEORETICAL FOUNDATIONS AND ESTIMATED COMPLEXITY

Abderrahim Sabour[1], Ahmed Asimi[2] and Aboubakr Lbekkouri[1]

[1] Department of Mathematics and Computer Science Faculty of Sciences
University Mohammed V, Rabat, B.P 14106
elbekkouri@iihem.ac.ma
sabour.abderrahim@gmail.com
[2] Department of Mathematics and Computer Science Faculty of Sciences
University Ibn Zohr, Agadir, B.P 8106
asimiahmed@yahoo.fr

Abstract. The functions and classes of three states functions are fully used by the algorithm R.A NMJ to such a point that the theoretical analysis of the latter is connected to the one of the functions and the classes of functions. An analysis stands out to justify the tests carried out on the algorithm R.A NMJ

Keywords: evolutionist algorithms, three states functions, algorithm R.A NMJ, multidimensional scaling.

I- Introduction

The algorithm R.A NMJ [6,7,8,9,10] is a regenerator of cryptographically reliable binary sequences, that exploits the complexity of evolutionist algorithms [2] and simulates a dynamic and dissipative system with compensation created from a keyword of an arbitrary size. Though it is deterministic, the system raises extremely complex behaviors [1,5] that look disorganized. These practical results imposed a theoretical study of the different functions of the system. Well founded on the observer notion that arises in the form of a class of three states a , b and l , this class is used during process I, to create Data blocks of the individuals from the initial population starting from a keyword. Thus these three states functions were adjusted in order to define new mating functions and allow the evolution of the individuals while doubling the size of their Data block during process II.; It also intervenes twice during process III : The first time during the mating function II, and permits the regeneration of Data blocks of N bits starting from two blocks of N bits. And in the second time during the contribution function, function to which every individual will contribute to the binary sequence which will be done by XOR'ing the plaintext or cipher text. The importance of functions and classes of three states functions for the study of the vulnerability of the algorithm R.A NMJ has set a theoretical study of these functions. The definition of a metric on the set of three states functions has permitted the computation of a distance matrix associated to every class of functions. Matrices whose analysis (MDS) will permit to make an estimation on a collective complexity of its classes. The multidimensional scaling (MDS) [3, 4, 11] is an analysis method of proximity matrix (similarity or dissimilarity) established on a set of elements. The objective of MDS is to model the proximities between individuals in order to present them as faithfully as possible in a space of a weak dimension.

II- Notations and Definitions

We denote by:

|n: m|: the set of integers between n and m, with $n < m$.

(E): The cardinal of a set E.

$\langle .,. \rangle$: The inner product defined in $\mathbf{R}^d$.

$M_m(\mathbf{R})$: The set of square matrices of order m .

$\mathbb{F}$: The set of functions defined in $\mathbb{N}$, periodical of period T with two states $(\mathbb{F}_2)$ or three states $(\mathbb{F}_3)$.

$\wedge$: The logic operator « and ».

$|X|$: The sum of the absolute values of the entries of X .

The three states functions play an important role in this approach since they allow us to represent the notion of observer.

Definition 1 : For each two states or three states function F we assign a unique sequence f defined by : f=F(0)F(1)F(2)F(3)F(4)… F(n)…. And if there exists an integer k such that f=F(0)F(1)F(2)F(3)F(4)…F(k) F(0)F(1)F(2)F(3)F(4)…F(k)…, we say that F is periodic with period F(0)F(1)F(2)F(3)F(4)…F(k), called primitive signal of f, that we denote $Sp(\mathrm{F})$, therefore for every integer $n \in \mathbf{N}$ F(n)=F(n mod $Sp(\mathrm{F})$). And if f is a finite sequence, we extend it to a unique infinite periodic sequence whose size of its primitive signal is a divisor of that of f. We call a regenerator signal of F, that we denote S_R (F), every concatenation of its primitive signal.

Remark: The existence of a bijection between the set of two or three states periodic functions and the set of the associated primitive signals simplifies the study of these functions, which is reduced to the study of the characteristics of its associated primitive signals.

Definition 2: Let Γ_2 (Γ_3) be the set of two states functions 0 and 1(respectively. three states, a , b and l) whose associated sequences are periodic.

The study of the three states functions a , b and l will be done via the associated sequences.

Definition 3: *Let S and S' be two elements of Γ_2 (or), S and S' are equal and (we denote $S = S'$) if* $S(n) = S'(n)$ $\forall n \in \mathbb{N}$.

Theorem 1: *Let S and S' be two elements of Γ_2 (or Γ_3), $S = S'$ if and only if $Sp(S) = Sp(S')$.*

Definition 4: We define a subset Ω of Γ_3 by: G is an element of Ω if and only if $Sp(G) = a\ldots ab\ldots bl\ldots lb\ldots b$.

If we denote by :

X : the frequency of a in $Sp(G)$

Y : the frequency of b between a and b in $Sp(G)$.

Z : the frequency of l in $Sp(G)$.

T : the frequency of b in $Sp(G)$ following l

Then G will be denoted $G = [X, Y, Z, T]$.

The advantage of the set Ω is due to its structure which permits to authenticate its elements via the values of X, W, Y, Z and T.

Definition 5 : A matrix $M = (d_{ij}) \in M_m(\mathbf{R})$ is called a distance matrix if it satisfies the following

1) It is symmetric (i.e. $d_{ij} = d_{ji}$ for all i and j).
2) $d_{ii} = 0$ for all i
3) $d_{ij} \geq 0$ for all $i \neq j$.

Moreover it is Euclidean if there exists a configuration of points in a Euclidean space such that the distances between points are given by the matrix M, i.e. there exists an integer d and points $x_1, \ldots, x_m \in \mathbb{R}^d$ such that $d_{ij}^2 = \langle x_i - x_j, x_i - x_j \rangle = (x_i - x_j)^T (x_i - x_j)$ for all $i, j \in \{1, \ldots, m\}$.

Proposition 1: The function $w : \mathbb{F} \times \mathbb{F} \to \mathbf{R}$ defined by:

$\forall S, S' \in \mathbb{F}$ $w(S, S') = \#\{i \in \{0, \ldots, T-1\} / S(i) \neq S'(i)\}$, is a distance on $\mathbb{F}$.

Proof:

It is clear that for all elements S, S' of $\mathbb{F}$ we have: $w(S, S') \geq 0$ and $w(S, S') = w(S', S)$, $w(S, S') = 0 \Leftrightarrow S(n) = S'(n)$ $\forall n \in \{0, \ldots, T-1\}$. But it is known that $S(n) = S(n \bmod T)$ and $S'(n) = S'(n \bmod T)$ for all integers n. We deduce that $S(n) = S'(n)$ $\forall n \in N$, thus $S = S'$.

Let S , S' , S'' be three elements of $\mathbb{F}$. We consider the following sets:

$K = \{i \in \{0, \ldots, T-1\} / S(i) \neq S'(i)\}$

$H = \{i \in \{0, \ldots, T-1\} / S(i) \neq S''(i)\}$

$G = \{i \in \{0, \ldots, T-1\} / S'(i) \neq S''(i)\}$

Let's show that $K \subset H \cup G$ Let $i \in K$ then $S(i) \neq S'(i)$,

If $i \notin H \cup G$ then $i \notin H$ and $i \notin G$, thus $S(i) = S''(i)$ and $S'(i) = S''(i)$, therefore $S(i) = S'(i)$ which contradicts $S(i) \neq S'(i)$. We deduce that:
$\forall i \in K, i \in H \cup G$, which shows that $K \subset H \cup G$.
But K, H and G are three finite sets, thus $|K| \leq |H \cup G| \leq |H| + |G|$, therefore
$w(S, S') \leq w(S, S'') + w(S'', S')$, for all periodic functions S , S' and S'', of period T.

Proposition 2: The function $w: \mathbb{F} \times \mathbb{F} \to \mathbb{R}$ defined by
$D(S_1, S_2) = \dfrac{w(S_1, S_2)}{T}$, is a distance on $\mathbb{F}$ that we call normalized distance on $\mathbb{F}$.

Proof
From proposition 1 we get

1. $D(S, S') \geq 0$ and $D(S, S') = 0$ iff $S = S'$.
2. $w(S, S') \leq w(S, S'') + w(S'', S')$, for all S, S' and S'' of $\mathbb{F}$, thus $\dfrac{w(S, S')}{T} \leq \dfrac{w(S, S'')}{T} + \dfrac{w(S'', S')}{T}$,

   therefore $D(S, S') \leq D(S, S'') + D(S'', S')$.

In this section, we denote by P a finite set of periodic two or three states functions not necessarily of the same period and k the least common multiple of their period

Proposition 3: The function: $D': P \times P \to \mathbf{R}$ defined by $D'(S, S') = \dfrac{\#\{\mathrm{i} \in \{0,...,\mathrm{k}-1\}, S(i) = S'(i)\}}{k}$ for all S and S' in P is a metric on P.
The proof is similar as of proposition 2.

Corollary 1 : Let S and S' be two elements of P of period T and T'
$$D'(S, S') = \frac{\#\{\mathrm{i} \in \{0,..., \; ppmc\,(T, T') - 1\}, S(i) \neq S'(i)\}}{ppmc\,(T, T')}$$

Proof:
It suffices to see that:
$$\#\{\mathrm{i} \in \{0,..., \; k - 1\}, S(i) \neq S'(i)\} = \frac{\#\{\mathrm{i} \in \{0,..., \; ppmc\,(T, T') - 1\}, S(i) \neq S'(i)\}}{ppmc\,(T, T')} \times k$$
And from proposition 3 we deduce that:
$$D'(S, S') = \frac{\#\{\mathrm{i} \in \{0,..., \; ppmc\,(T, T') - 1\}, S(i) \neq S'(i)\}}{ppmc\,(T, T')}$$
This relation is more general since it defines the distance between two periodic functions of an arbitrary period, independently from the other functions of the class.

III- Study of the inner characteristics of the classes of three states functions
R.A NMJ calls on two classes of three states functions, One of them (CI) during the creation of the initial population, and the other (CII) during the contribution of the individuals. The study of the characteristics of the classes of three states functions faces a big problem related to the interpretation of the states that are displayed during the superposition of two sequences associated to three states functions that are : (a, a), (b, b), (l, l), (a, b) or (b, a), (a, l) or (l, a), (b, l) or (l, b), and (x, y) corresponding to $((S_i(n) = x) \wedge (S_j(n) = y))$ or $((S_i(n) = y) \wedge (S_j(n) = x))$.
Let $G = [X, Y, Z, T]$ be the observer, the range of values denoted D_i, X, Y, Z, and T are variables and it is up to the designers to choose the adequate values. The original version of R.A NMJ uses two classes of three states functions defined by:
C I **:** $\mathbf{D_X}$= |2 :7|, $\mathbf{D_Y}$=|1 :6|, $\mathbf{D_Z}$=|2 :7|, $\mathbf{D_T}$= |1 :5| and *C II* **:** $\mathbf{D_X}$= |5 :8|, $\mathbf{D_Y}$=|1 :4|, $\mathbf{D_Z}$=|5 :8|, $\mathbf{D_T}$= |1 :4|.
The values of $\mathbf{D_X}$, $\mathbf{D_Y}$, $\mathbf{D_Z}$ and $\mathbf{D_T}$ determine the number of functions of classes CI an CII

$C\ I$: 1080 = (7-2+1)*(6-1+1)*6*5 et $C\ II$: 256 = (8-5+1)*(4-1+1)*4*4.

III-1 Distribution of distances of three states functions of the two classes

In this section we will focus on the distribution of distances of the observers $G_1,\ldots,G_m$ with regard to each other for the two classes of functions *C I* and *C II*, and this will be done via the analysis of distance matrices.
The analysis of distance matrices (Definition 5), associated to every class will allow, to give an estimation of the collective complexity of the elements of the class. The two following figures represent the histograms of distance matrices of classes I and II.

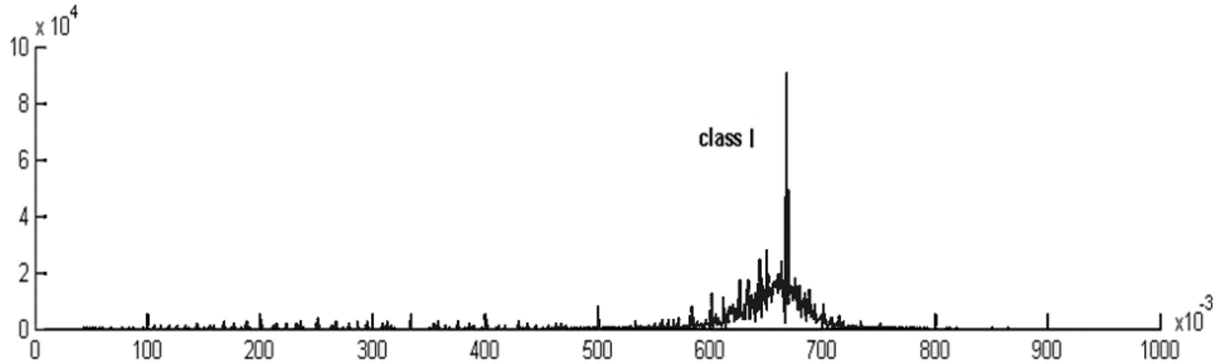

Figure 1: Histogram of the matrix $\left(d_{ij}\right)$ associated to class C I

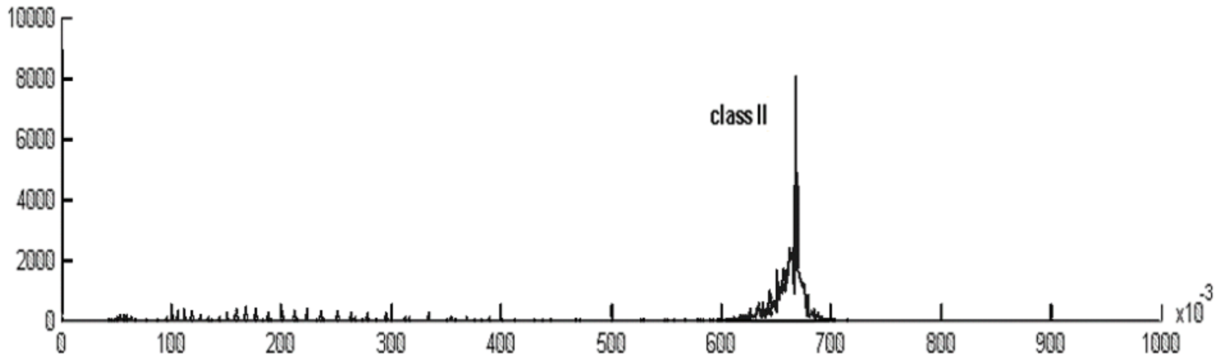

Figure2: Histogram of the matrix $\left(d_{ij}\right)$ associated to class C II

The x- axis represents the distances between the observers. The y- axis represents the frequency of the same coefficients of the matrix $\left(d_{ij}\right)$ of the class in question.

We notice that each histogram represents a pick at the value 0.66. This pick represents a kind of an attractor since we have a high density in the neighborhood at this point.

III-2. The classic algorithm MDS

The goal of the study of the characteristics of the three states functions is to estimate the complexity and theoretical bases of R.A NMJ, via more concise theory that might explain it globally or partially. The study of the characteristics of the three states functions used during the different steps of the algorithm R.A NMJ will give a theoretic view on this latter. It matters to study the complexity of the structure defined by the set of elements of the class but not of each element. The estimation of this collective complexity is essential to justify the use of the classes. Estimation that becomes possible via the analysis of the characteristics of distance matrices between pairwise elements of the class. The technique that will be used to exploit these matrices is the classic algorithm MDS [3, 4, 11] 'Multidimensional Scaling Techniques', technique that will allow the estimation of the coordinates of each element of the set of the Euclidean space. The use of the word 'estimation' is due to the fact that MDS tends to reduce the dimension of the Euclidean space while minimizing a "Stress function ".
The observable data that characterize a given process are in several cases of high dimensions, consequently hard to interpret and this is why the techniques of the analysis of data were created; their goal is to find the data structure in the intrinsic subspace of the observations. The projection algorithms of data (data projection algorithms) are used to represent in a two or three dimension spaces data having a very high dimension number. They not only permit to help understand the data but also to provide means to visualize them intuitively.

The classic algorithm MDS is a technique of data analysis that operates on distance matrices or similarity in order to make projections of the starting structure on a space, generally Euclidean, of n dimensions. We are interested by this technique because it gives the coordinates of its objects in a Euclidean space, which permits the estimation of each axis and thus gets an indication on the collective complexity on the set of objects. In other words, given a set of N objects in a space, for which the dimension is unknown to us , MDS permits to find, the minimal dimension of a Euclidean space ($\mathbb{R}^m$) in which N points configure, starting from the distances between N objects to which these points are associated; thus its coordinates in this Euclidean space ; while minimizing a ' Stress function', in our case , the equality of the sum of the squares of the differences of the distances with the sum of squares of differences of coordinates that we have at our disposal. In other words, MDS permits to assign coordinates to elements of the class, in a Euclidean space of minimal distance that will be used to evaluate the importance of each axis compared to the others.
We will give in the following an outline of this technique:
Let $D = (d_{ij})$ be the distances matrix of order n where d_{ij} is the distance between two observers Gi and Gj which follows from the metric (**Corollary 1**), the quadratic distances matrix $\Delta = (d_{ij}^2)$ and $B = \frac{1}{2}(I_n - \frac{1}{n}U_n)\Delta(I_n - \frac{1}{n}U_n)$ with I_n the unit matrix (identity) of order n and U_n a square matrix of order n whose coefficients are equal to 1. We compute the eigenvalues of the matrix B and the associated eigenvectors. Let then $(l_i)_{i=1}^d$ be the d positive eigenvalues of B such that $l_1 > ... > l_d$, and $(x_{(i)})_{i=1}^d$ the corresponding eigenvectors normalized by $x_{(i)}^T x_{(i)} = l_i$ where Y^T denotes the transpose of the vector Y . Further the coordinates of the points P_r in the Euclidean space $\mathbb{R}^d$, for $r \in \{1,...,n\}$ are given by $x_{(r)} = (x_{r1},...,x_{rd})$, which are the rows of the matrix $X = (x_{(1)},...,x_{(d)})$ of order $n \times d$.

Definition 5: Let S be the function defined from $\mathbf{R}^{n.d} \to \mathbf{R}$ by:
$S(x_{11},...x_{1d},...x_{n1},...x_{nd}) = \sum_{i=1}^{n}\sum_{j=i+1}^{n}\left| d_{ij} - \sqrt{\sum_{k=1}^{d}(x_{ik} - x_{jk})} \right|$, and the "Stress function" minimized by the algorithm MDS.

III-3 Results
The aim of this part is to present and interpret the results obtained during the algorithm MDS on distance matrices associated to two classes of three states functions used in the algorithm R.A NMJ.

III-3.1. Class CI used in R.A NMJ.

Class CI is defined by: $\mathbf{D_X}$= |2:7|, $\mathbf{D_Y}$=|1:6|, $\mathbf{D_Z}$=|2:7|, $\mathbf{D_T}$= |1:5| and is composed of 1080 functions. It plays a big role since it is the kernel of the function that regenerates the initial population associated to a given key word.
The distance matrix associated to class CI is of range 1057 and has 313 positive eigenvalues that will be taken into account.

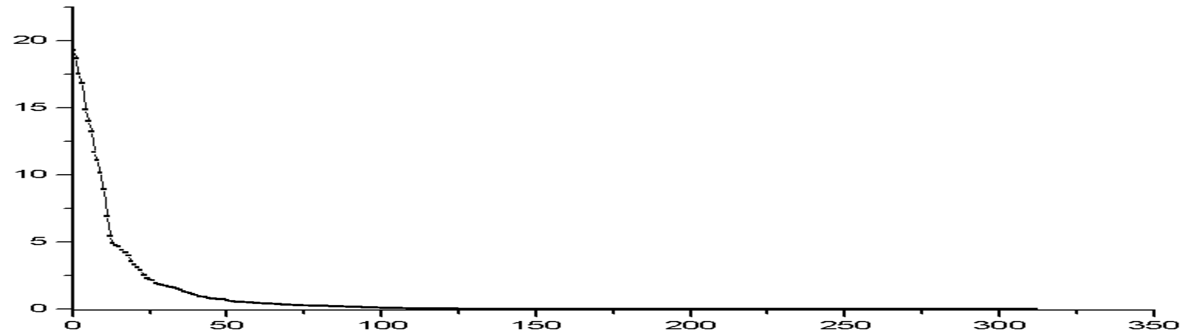

Figure 3 : This figure represents the 313 positive eigenvalues associated to class CI, picked in an increasing order.

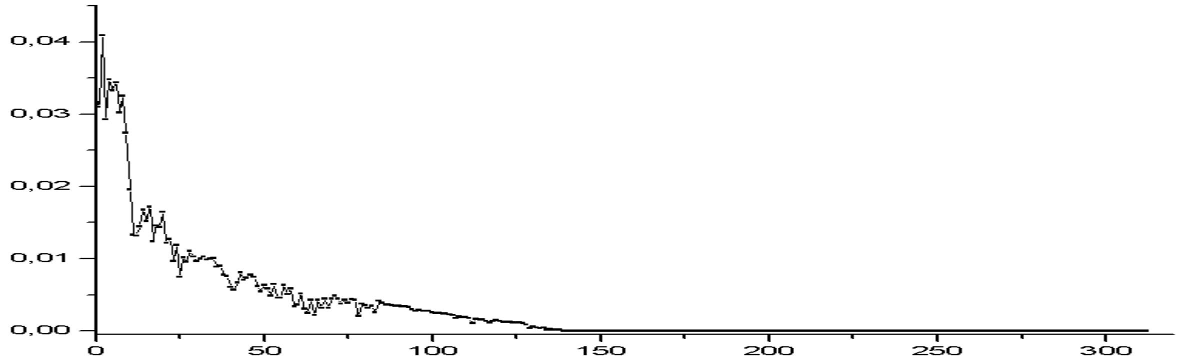

Figure 4 : The x-axis represents the indices of the axes associated to 313 positive eigenvalues, the y-axis represents the percentage $P\left(X_{(i)}\right)$ of the contribution of each axis compared to the other axes that constitute a Euclidean space.

This graph represents the importance of the axes associated to positive eigenvalue; an estimated value via the following relation: $P\left(X_{(i)}\right)=\frac{|X_{(i)}|}{|X|}$.

III-3.2 Class CII used in R.A NMJ

Class CII is defined by: $\mathbf{D_X}$= |5:8|, $\mathbf{D_Y}$=|1:4|, $\mathbf{D_Z}$=|5:8|, $\mathbf{D_T}$= |1:4|, it intervenes during the contribution function allowing to the individuals the contribution to binary sequences. Its matrix has a rank equal to 255 and has 83 positive eigenvalues.

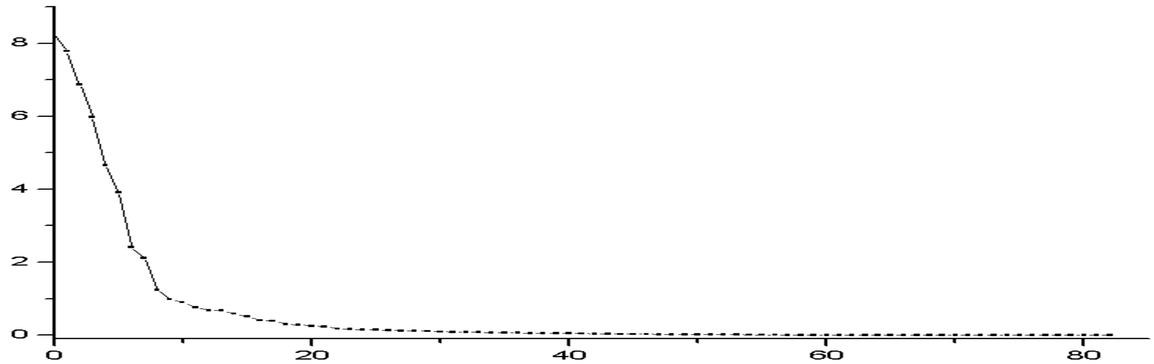

Figure 5: This figure represents the 83 positive eigenvalues associated to class CII, picked in an increasing order.

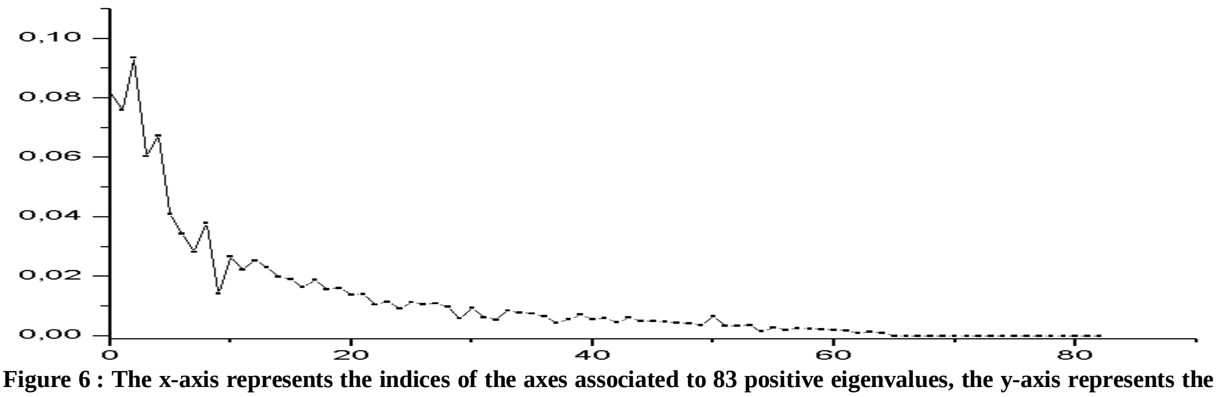

Figure 6 : The x-axis represents the indices of the axes associated to 83 positive eigenvalues, the y-axis represents the percentage $P\left(X_{(i)}\right)$ of the contribution of each axis compared to the other axes that constitute a Euclidean space.

Remark

Even though MDS gives only an approximated estimation (since MDS takes into account only the dominant aspects of the populating, the rare species are ignored, because they put difficulties in interpretation) of the dimension of a Euclidean space that would satisfy the distances between all pairwise elements of the set. The results found are 313 and 83 respectively for the first and second class, give an indication on the collective complexity of its classes. In the sequel we will focus on the transform W that describes the way in which the algorithm R.A NMJ calls for three states functions.

IV- Study of the characteristics of the transform W

In this part we will study the influence of the ignorance of the bits on the transition functions based on the three states functions via the study of their linearity while trying to find an algebraic structure that will explain their dissipative transforms.

Definition 6: Let v be the transform defined by $v:\{a,l\}\times\{0,1\}\rightarrow\{0,1\}$ such that $v(a,k)=k$ and $v(l,k)=\bar{k}$ with c $\bar{0}=1$ and t $\bar{1}=0$.

Definition 7: The transform defined by: $W:\Omega\times\Gamma_2\rightarrow\Gamma_2$ with $W(G,S)=S'$ permits the transition of a given observer G, from the binary sequence associated to S to the corresponding binary sequence associated to the function S'.

To determine the value of S', we construct two sequences $(t_i)_i$ and $(k_i)_i$ by:

$$t_0 = \inf\ \{n \in N\ /\ G(n) = b\}$$
$$k_0 = \inf\ \{n \in N\ /\ G(n) \neq b\}$$

We have two cases: $t_0 > k_0$ or $t_0 < k_0$ otherwise $G(0)=b$ or $G(0)\neq b$. And since $G\in\Omega$, then $G(0)=a$, therefore $t_0 > k_0$ and $k_0 = 0$.

And we define:

$$t_{i+1} = \inf\ \{n \in N\ /\ n > k_i; G(n) = b\}$$
$$k_{i+1} = \inf\ \{n \in N\ /\ n > t_i; G(n) \neq b\}$$

The function S' is defined by:

$$S'(n)=v(G(m),S(m))$$

with $m=k_r+d$, $n=d+\sum_{i=0}^{r}(t_i-k_i)$ and $0\le d\le t_{r+1}-k_{r+1}-1$.

IV-1 Characteristics of the transform W

Definition 8:

We define $B_3=\{a,b,l\}$ equipped with two binary operations $+,*$ such that:

$$a+a=a\ ;a+b=b+a=b\ ;a+l=l+a=l\ ;b+l=l+b=a$$
$$a*a=a*l=l*a=b*a=a*b=a$$
$$l*b=b*l=l\ ;\ l*l=b$$

Theorem 2:

(B_3, +,*) *is a commutative field.*

The study of the linearity poses a big problem since $\Omega\times\Gamma_2$ is not a vector space neither on $\{0,1\}$, nor on B_3. To encounter this problem we associate to each observer G a function $W_G:\Gamma_2\rightarrow\Gamma_2$ such that $W_G(S)=S'$. With these conditions we can study the linearity of W_G.

Proposition 4: W_G *is linear if and only if* $W_G(S_1+S_2)=W_G(S_1)+W_G(S_2)$ *for all elements* S_1 *and* S_2 *in* Γ_2.

To show the nonlinearity of this transform, suffices to show that there exist two elements S_1 and S_2 of Γ_2 such that $W_G(S_1+S_2)\neq W_G(S_1)+W_G(S_2)$.

Let $G=[X,Y,Z,T]$ be the observer and let S_1 and S_2 be two functions such that $Sp(S_1)=1$ and $Sp(S_2)=0$. We have $S_1+S_2=S_1$.
To show that $W_G(S_1+S_2)\neq W_G(S_1)+W_G(S_2)$ we need to prove that there exists $m\in\mathbb{N}$ such that $W_G(S_1+S_2)(m)\neq(W_G(S_1)(m))\oplus(W_G(S_2)(m))$.
For $m=X+Y+1$ we have: $W_G(S_1)(m)=0, W_G(S_2)(m)=1$. And since $W_G(S_1+S_2)(m)=0$ and $(W_G(S_1)(m))\oplus(W_G(S_2)(m))=1$ then $W_G(S_1+S_2)\neq W_G(S_1)+W_G(S_2)$, therefore the transform W_G is nonlinear.

Lemma 1: The function W_G is non injective, for each observer G.

Proof: Let S_1 and S_2 be two elements of Γ_2 such that:
$S_R(S_1)=$"1100011001100011110101011011011101101111000011001100100001111",
$S_R(S_2)=$"110101101010011111110100001010110110110100011100110010101010"

And let G be an observer defined by: $G=[X_G,Y_G,Z_G,T_G]$ with $X_G=3, Y_G=2, Z_G=2$ and $T_G=3$. We check that $S_R(W_G(S_1))=S_R(W_G(S_2))=$ "110001000001010110100000100110".
This shows that the function W_G is non injective. And we verify that there exists at least $2^{E\left[\left(\frac{Y_G+T_G}{X_G+Y_G+Z_G+T_G}\right)*L(S_R(S_1))\right]}$ sequences S_i such that $W_G(S_1)=W_G(S_i)$, in this case this will give about 2^{30} functions S_i. Suppose now that S' is known and $G=[X_G,Y_G,Z_G,T_G]$ is the observer used during the transition, once we compute the number of possible cases N_S for S in term of the parameters of X_G,Y_G,Z_G,T_G and $L(S')$, we find that $N_S > 2^{E\left[\left(\frac{Y_G+T_G}{X_G+Z_G}\right)*L(S_R(S'))\right]}$.

V- Conclusion

The nonlinearity, the non injectivity of the functions W_G, in addition of the dissipation associated to the state b, dissipation that will be compensated by the function W_G itself, are piling up since R.A NMJ is a system that simulates the evolution of a population of individuals, which is heterogeneous dynamic with feedback. These characteristics justify that R.A NMJ is a chaotic system sensitive to the initial state and allow to generate an avalanche effect for very close states. This sensitivity will warranty the non-reducibility of the research space during an exhaustive attack through enumeration of key words.
Moving towards evolutionist algorithms to generate crytographically reliable sequences is a hard decision to take and justify because of the stakes of this discipline, only the stored complexity in these processes and the results found motive this study.
Actually, the complexity of biological systems go beyond the one of the physics phenomena , moreover its techniques offer simplicity either at the stage of elaboration or in the study of vulnerability. Also the evolutionist algorithms may be an alternative for the generation of cryptographically reliable binary sequences.

VI- References

[1] M. R. Garey, D. S. Johnson, Computers and Intractability: A guide to the theory of NP-completeness, W.H. Freeman & Company, 1979
[2] J. Horn, D.E. Goldberg, Genetic Algorithms difficulty and the modality of fitness landscapes. Foundations of Genetic Algorithms 3, Scan Francisco, Morgan Kaufmann, 243-269 (1995).
[3] J. B. Kruskal, M. Wish. Multidimensional Scaling. Sage Publications. Beverly Hills. CA (1977).
[4] K. V. Mardia , J. T. Kent, J. M. Bibby, Multivariate Analysis. Academic Press (1979).
[5] C. Papadimitriou, Computational Complexity, Addison-Wesley, 1993.
[6]. 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.
[7]. 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.

[8]. 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
[9]. 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
[10]. 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
[11].S. S. Schiffman, M. L. Reynolds, Young. F. W. (1981). Introduction to Multidimensional Scaling. Academic Press, New York