Chaos Crypto-Système basé sur l'Attracteur de Hénon-Lozi

A. ALI-PACHA[1], N. HADJ-SAID[1], A. M'HAMED[2], A. BELGHORAF[1]

[1]Université des Sciences et de la Technologie d'Oran USTO BP 1505 El M'Naouer Oran 31036 ALGERIE
Phone / Fax : 213 / 041- 46 26 85

[2] Institut National des Télécommunications, Evry France
E.Mail : alipacha@yahoo.com

Résume:

La cryptologie, véritable science régissant le codage de l'information, a connu une réelle explosion avec le développement des systèmes informatiques, passant d'une ère artisanale et confidentielle à des systèmes de très hautes technologies nécessitant une importante puissance de calcul. Elle a connu un plus large essor encore avec l'arrivée des systèmes de communications modernes (Internet, etc...) où il y a une nécessité absolue de protéger les données échangées des individus.

Depuis quelques années, les chercheurs s'intéressent à la possibilité d'utiliser des signaux chaotiques dans les systèmes de transmission de données, en particulier pour transmettre des quantités importantes d'informations sécurisées. L'intérêt d'utiliser des signaux chaotiques réside dans deux propriétés du chaos :
Un signal chaotique est un signal à large spectre et permet donc de transmettre des signaux très variés, d'autre part, un signal chaotique est obtenu à partir d'un système déterministe, il est donc possible de le reconstituer en se plaçant dans les mêmes conditions que celles qui ont contribué à le créer et, ainsi, de récupérer l'information de départ.
Dans cette communication on essaye de mettre certains concepts de la théorie du chaos à la disposition du chiffrement continue en particulier l'attracteur de **Hénon-Lozi**, des données (textes et images fixes) seront cryptées pour valider le chiffrement.

Mots Clés: Cryptographies; Chiffrement Continue, Chaos; attracteur, Générateur, Hénon Lozi

1. Introduction

Assurer un échange d'informations rapide, fiable et authentique, tel fut parmi les préoccupations majeures de l'humanité depuis bien plusieurs dizaines, voire même des centaines d'années. Cet aspect devient de plus en plus accentuer avec l'apparition du réseau.
L'échange quasi instantané de milliers d'octets pouvant contenir différents types d'informations, parfois cruciales, rend la protection de la communication et de l'échange d'informations d'une importance capitale.
La confidentialité du message, son intégrité et son authenticité, constitue généralement les caractéristiques fondamentales d'une communication sûre. La technique de cryptage ou de chiffrement, constitue l'un des outils les plus performants permettant d'assurer la quasi-totalité des services de sécurité.

La cryptologie est à la fois une science, un art et un champ d'innovation et de recherche. Deux alternatives ont alors été développées durant les dernières années : la cryptographie quantique et la cryptographie chaotique.

La première résout de manière radicale le problème de la confidentialité puisque par principe, elle offre une clé incassable (lié au principe d'incertitude d'Heisenberg), mais son débit est très limité (de l'ordre de quelques dizaines de kbits/s) et son coût de mise en œuvre reste très élevé.

La cryptographie par chaos, quant à elle, a déjà donné la preuve de sa faisabilité et de sa puissance de chiffrage (supérieur à 1 Gbits/s). Le chiffrement d'un message par le chaos s'effectue donc en superposant à l'information initiale un signal chaotique. On envoie par la suite le message noyé dans le chaos à un récepteur qui lui connaît les caractéristiques du générateur de chaos. Il ne reste alors plus au destinataire qu'à soustraire le chaos de son message pour retrouver l'information, autrement dit son principe de fonctionnement est le même que celui du chiffrement continue (stream cipher).

2. Théorie du Chaos

Il n'est pas rare d'entendre quelqu'un qualifier une situation de chaotique. Cette qualification porte par nature l'idée que cette situation relève du désordre ou de la plus grande confusion. Les phénomènes dans lesquels on ne pouvait déceler à priori aucune logique ont progressivement été regroupés sous le terme de "chaos" [5, 6, 7].

Il n'existe pas de définition rigoureuse du chaos mais par chaos, il faut admettre la notion de "**phénomène imprévisible et erratique**". Cependant, depuis une vingtaine d'années, on attribue le terme chaos à des "comportements erratiques qui sont liés à des systèmes simples pouvant être régis par un petit nombre de variables entre lesquelles les relations décrivant leur évolution peuvent être écrites. Ces systèmes sont donc déterministes bien qu'imprévisibles.

La théorie du chaos, déjà entrevue par Jacques Hadamard et Henri Poincaré au début du XX^{e} siècle, a

été définie à partir des années 1960 par de nombreux scientifiques.

On appelle chaotiques des phénomènes complexes, dépendant de plusieurs paramètres et caractérisés par une extrême sensibilité aux conditions initiales : par exemple, les volutes décrites par la fumée d'une cigarette, ou la trajectoire d'un ballon qui se dégonfle. Ces courbes ne sont pas déterminées, modélisées par des systèmes d'équations linéaires ni par les lois de la mécanique classique; pourtant, elles ne sont pas nécessairement aléatoires, relevant du seul calcul des probabilités : elles sont liées au chaos dit déterministe. L'imprédictibilité est présente dans de tels systèmes, qui n'en sont pas moins munis d'un ordre sous-jacent. Les signaux chaotiques peuvent être obtenus à partir de circuits non linéaires où interviennent des paramètres.

Géométriquement, ces phénomènes dynamiques sont représentés dans un espace dont la dimension, qui peut être supérieure à celle de l'espace à trois dimensions, dépend du nombre de paramètres choisis pour les décrire. À chaque instant, l'état du phénomène est représenté par un point dans cet espace appelé espace des phases. L'évolution du système est décrite par la trajectoire de ce point. Pour les phénomènes les plus simples, ce point est attiré vers un point d'équilibre ou une courbe limite, près desquels il repasse périodiquement. Les mathématiciens appellent ces courbes limites des attracteurs étranges.

2.1 Système Dynamique Non Linéaire

Un système dynamique consiste en un espace de phase abstrait ou un espace d'état dont les coordonnées décrivent l'état dynamique du système à n'importe quel moment et dont une règle dynamique spécifie la tendance future immédiate de toutes les variables d'état composant le système, donnée par la valeur présente de ces mêmes variables d'état.

Mathématiquement, un système dynamique est décrit par un problème où seules sont données les valeurs de départ des variables d'état. Il peut avoir une composante de temps "**discrète**" ou "**continue**".

Une classe importante de phénomènes naturels peut être décrite par un ensemble de *p* équations différentielles ordinaires du premier ordre du type:

$$\frac{d}{dt} X_i(t) = F_i(X_j(t), \Lambda) \text{ Avec}$$

$$X \in IR^p, p \geq 1 \text{ et } i, j = 1, .., p.$$

p représente la dimension du système. La fonction F dépend des variables du système et du vecteur de paramètres Λ qui conditionne le comportement du système. Si F ne dépend pas explicitement du temps, mais seulement de X, le système est dit **autonome**.
Mais on peut également rendre compte de l'évolution d'un système dynamique au moyen d'une application à temps discret :

$$X_{n+1} = T(Xn, \Lambda) \text{ où}$$

$X_n \in IR^p$ ($p > 1$), *n* est un entier naturel,

X_0 est la condition initiale et Λ le vecteur de paramètres de la récurrence. Le débat entre modèle discret et modèle continu n'est pas aussi anodin qu'on pourrait le croire. Dans le cas continu (équations différentielles), il faut un minimum de 3 équations autonomes pour faire apparaître un comportement chaotique. Par contre, un modèle discret peut générer du chaos à partir d'une seule équation. Dans la suite de cette communication nous ne considérerons **que les systèmes à temps discrets :** attracteur de **Hénon-Lozi**.

2.2 Attracteur

Si l'on observe l'ensemble des différents états successifs de l'espace d'état, on peut observer l'émergence d'une **trajectoire** dans cet espace. Cette trajectoire est également appelée **orbite** du système. Il est à noter que si les variables d'état prennent des valeurs réelles, l'orbite d'un système dynamique à temps continu sera une courbe alors que l'orbite d'un système dynamique discret sera représentée par une série de points.

L'attracteur est une limite vers laquelle semblent convergé les orbites du système. On peut définir un attracteur comme un ensemble compact de l'espace d'état vers lequel toutes les trajectoires environnantes convergent c'est à dire que l'attracteur décrit en fait une situation de régime telle qu'elle peut apparaître après disparition des **phénomènes transitoires**. Le bassin d'attraction est alors l'ensemble des points initiaux dont les trajectoires convergent vers l'attracteur : **attracteur étrange**.

Une des découvertes les plus spectaculaires des dernières années a été celle des attracteurs étranges, ces objets géométriques issus de l'évolution de systèmes chaotiques. Dans le plan, ils sont formés d'une suite infinie de points :

$$x_0, x_1, x_2, x_3 \ldots, x_n, \ldots$$

Qui dépendent de x_o la valeur initiale. Au fur et à mesure que le nombre de points augmente, une image se forme dans le plan et devient de plus en plus nette (figure 3). Cette image n'est pas une courbe ni une surface, c'est en fait un objet intermédiaire constitué de points avec entre eux des espaces inoccupés. L'objet est qualifié d'étrange en raison de sa structure pointilliste et de sa nature fractale. Une valeur différente de x_o conduit à une toute autre suite qui après une courte phase, dessine la même image.

- D'où qu'on parte, on se retrouve toujours sur l'attracteur, c'est le côté prévisible de l'évolution.

- Où se retrouve-t-on exactement sur l'attracteur? Il est impossible de répondre à la question, c'est le côté imprévisible de l'évolution.

On appelle attracteur cette forme (figure 3) qui apparaît de façon répétitive, indépendamment des conditions initiales ou des trajectoires. Les attracteurs étranges constituent ce que l'on appelle le chaos. Les trajectoires dans l'attracteur étranges ne doivent pas se couper. Cette propriété est très intéressante et sera exploitée dans le cadre de la cryptographie. Il est à noter qu'un attracteur chaotique n'occupe pas forcément un volume fini de l'espace d'état.

2.3 Sensibilité aux Conditions initiales

La sensibilité aux conditions initiales **(S.C.I)** est une caractéristique fondamentale des systèmes dynamiques. Il faut entendre ici qu'un système réagira de façon totalement différente selon la condition initiale. Ceci a notamment comme conséquence le fait qu'un système chaotique, même si toutes ses
imprévisible car sensible à d'infimes perturbations initiales.
Attracteurs étranges et chaos ont permis de mieux comprendre des phénomènes comme l'apparition de la turbulence en hydrodynamique, les perturbations orbitales dans le système solaire, et la météorologie, qui permet de bien illustrer la dépendance sensitive des conditions initiales, comme l'a fait Edward Lorenz dans sa célèbre remarque que «le battement des ailes d'un papillon aura pour effet après quelque temps de changer complètement l'état de l'atmosphère terrestre».

3. L'Attracteur de Hénon Lozi

L'attracteur est défini par le système d'équations suivant, ou **a** et **b** sont des constantes :

$$\begin{cases} X(n+1) = 1 + Y(n) - a * |X(n)| \\ Y(n+1) = b * X(n) \end{cases}$$

Si on programme ces formules avec Matlab on aura le graphe de la figure 3 avec 50.000 points avec les valeurs suivantes a = 1.7; b = 0.5 on aura ce graphe :

N	X (n)	Y (n)	N	X (n)	Y (n)
0	0	0	**8**	-0,198	0,2719
1	1	0	**9**	0,936	-0,099
2	-0,7	0,5	**10**	-0,689	0,468
3	0,31	-0,35	**11**	0,297	-0,345
4	0,123	0,155	**12**	0,153	0,148
5	0,946	0,062	**13**	0,888	0,076
6	-0,546	0,473	**14**	-0,434	0,444
7	0,544	-0,273	**15**	0,706	-0,217

Tableau 1 : valeurs X,Y,

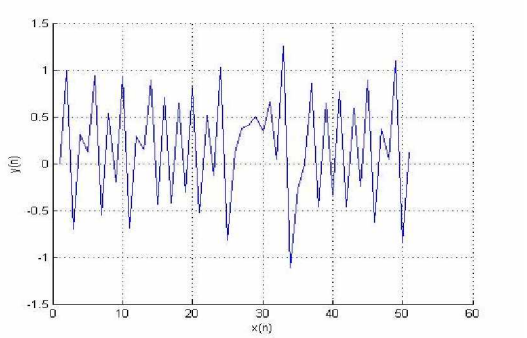


Figure 1: $x_{n+1} = x(n+1) = 1+y(n) - a * |(x(n))|$

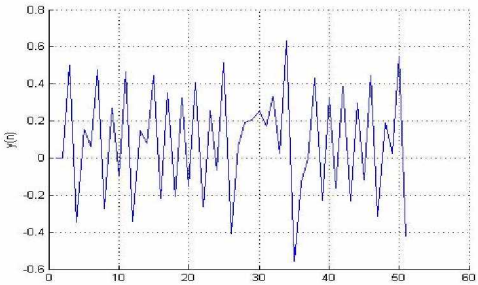


Figure 2:: $y_{n+1} = y(n+1) = b * x(n)$

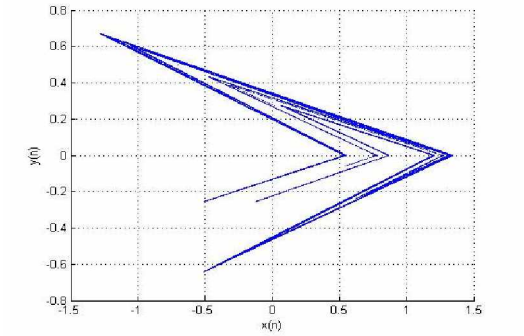


Figure 3. : L'attracteur de Hénon Lozi

4. Chiffrement continue

Le système de chiffrement continue consiste à produire [10] une suite chiffrante qui est le résultat de l'addition bit à bit du texte clair à la suite pseudo aléatoire (appelé codon). L'un des exemples les plus connus de chiffrement à flot est le système A5 utilisé par GSM, l'algorithme est utilisé pour chiffrer la communication entre le mobile et la borne reliée au réseau. C'est un système relativement simple pour protéger raisonnablement la communication sur le trajet aérien.
Les algorithmes de chiffrement en continu convertissent la donnée à chiffré 1 bit à la fois. La réalisation la plus simple d'un algorithme de chiffrement en continu est illustrée par la figure 4.

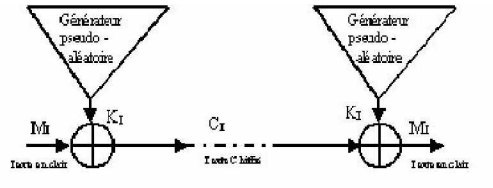


Figure 4 Chiffrement continu

Ce type de générateur engendre un flux de bits (appelons les codons) K_1, K_2, K_3, …, K_i. Ce flux est combiné par ou exclusif avec le flux de bits du texte en clair m_1, m_2, m_3, …, m_i pour produire le flux de bits de donnée chiffré.

$$c_i = m_i \oplus k_i \qquad (1)$$

Du coté du déchiffrement, les bits de donnée chiffré sont combiné par ou exclusif avec un flux identique de codons pour retrouver les bits du texte en clair :

$$m_i = c_i \oplus k_i = (m_i \oplus k_i) \oplus k_i = m_i \qquad (2)$$

4.1 Générateur Pseudo aléatoire : RDRL

Le chiffrement à flot [3, 9] qui existe actuellement est généré par un générateur pseudo-aléatoire RDRL (Registre à Décalage à Rétroaction Linéaire) qui produit une suite de longueur connue, de zéros et de uns logiques. Il est dit aléatoire car cette suite est arbitraire. Cependant, lorsque la suite arrive à son terme, le générateur ne s'arrête pas de fonctionner. La séquence déjà transmise est à nouveau reproduite (générateur **périodique**). D'où le qualificatif de pseudo-aléatoire. Le principal intérêt de l'étude des **G**énérateurs **P**seudo-**A**léatoires de **S**uites **C**rypto-graphiquement **S**urs **GPASCS** est qu'ils sont parfaits pour le chiffrement en continu. Leur construction se fait en tenant compte de:

1. Longue période,
2. Pas de répétitions,
3. Complexité linéaire locale
4. Critères de non linéarité pour des fonctions booléennes.

La clé de chiffrement est la même que celle du déchiffrement (chiffrement symétrique).l'état t initial du registre est la clé de chiffrement. Dans certain cas, la cryptanalyse peut se baser sur la répétitivité du signal transmis car les algorithmes de cryptage sont des suites de nombres pseudo aléatoires. Il est alors possible de reconstruire la clé à partir du signal crypté. Pour éviter ce type de faille, il faut donc que la clé ait une dimension suffisamment complexe pour que même à long terme, on ne puisse pas remonter au code. Le principe serait alors de se servir d'un bruit aléatoire évoluant dans le temps dont on connaît les caractéristiques en guise de clé.

4.2 Champs formant la clé de chiffrement

Dans ce qui suit on remplace le générateur RDRL par l'attracteur chaotique. Le choix de la clé de chiffrement, dans ce cas par exemple, doit être suivant :

1. le choix d'attracteur,
2. le travail suivant l'axes X/Y/Z ,
3. le pas d'échantillonnage, et
4. l'état initiale X_0 , Y_0 et Z_0 .

Nous avons crypté et décrypté nos données [7], avec la clé de chiffrement par défaut suivant :

- Attracteur : **Hénon Lozi**
- Pas : 1
- Axe : **X**
- On fait varier les valeurs initiales X_0 et Y_0.

5. Résultats et Interprétation :

Nous allons utiliser l'attracteur de Hénon Lozi pour crypter nos données. Le principe du chiffrement continu sera utilisé, les valeurs de X (tableau 2) seront converti en binaires pour être combiné avec les n-bits de données a crypté (figure 5).

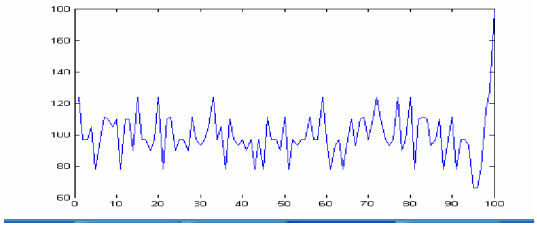


Figure 5a: Courbe de l'image en claire ⊕

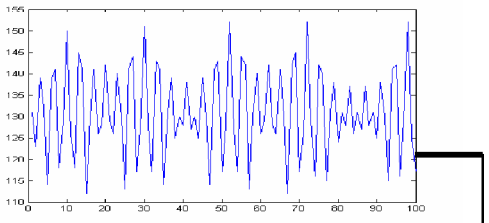


Figure 5b: Courbe de données

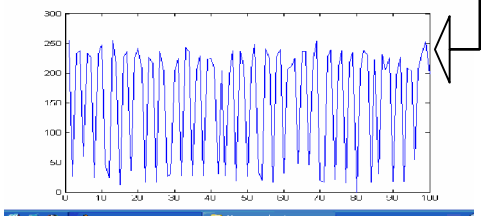


Figure 5c: Courbe de l'image cryptée

N°	x	X normaliser	X Décimal Arrondi
0	0	17,583	18
1	0	17,583	18
2	1	18,583	19
3	-6,4833	11,1	11
4	9,27	26,853	27
5	2,6958	20,279	20
6	-15,285	2,2974	2
7	9,3106	26,893	27
8	11,515	29,098	29
9	-12,044	5,5386	6
10	-0,11417	17,469	17
11	20,82	38,403	38
12	-3,7106	13,872	14
13	-11,168	6,4144	6
14	14,942	32,525	33
15	11,685	29,268	29
16	-17,583	0	0
17	0,73095	18,314	18
18	11,028	28,611	29
19	-3,7169	13,866	14
20	-1,3754	16,207	16
21	12,81	30,393	30
22	-0,58418	16,999	17
23	-3,9149	13,668	14
24	10,282	27,865	28
25	0,57087	18,154	18
26	-16,88	0,70333	1
27	11,722	29,304	29
28	14,258	31,841	32
29	-12,444	5,1389	5
30	-2,7808	14,802	15
31	21,877	39,46	39

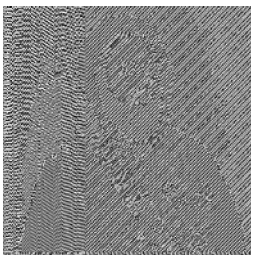
Tableau 2 : des Valeurs de X utilisé pour le cryptage

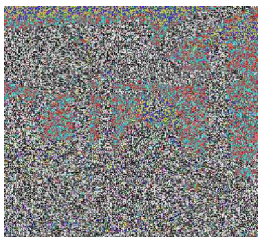
5.1 Image

Emir Abdelkader

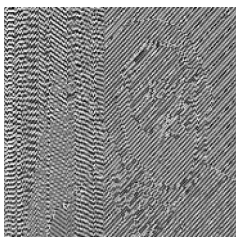
mosquée

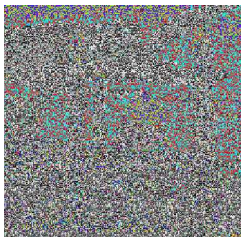
On voit que si on change les valeurs des conditions initiales le résultat est changé, il est clair que le choix des valeurs initiales sont importantes comme dans exemples, les images chiffrées ci-dessous sont brouillées.





(X_0= 2, Y_0= 2.5)





(X_0= 0.02, Y_0=0.02)

5.2 Texte

Le principe utilisé pour le cryptage d'image est utilisé dans le cryptage du texte, l'attracteur c'est l'attracteur de Hénon Lozi avec un pas de 0.005.

Chiffrement	Clé par défaut avec	
Texte en claire :	**X_0 = 1, Y_0 = 1**	**X_0 = 0.2, Y_0 = 2.5**
la cryptologie a connu une rapide évolution à notre époque surtout en ce qui concerne ces deux facteurs	• t>DSjaznj ~zuu2r?KO| |z s|x;cuasyw % / uibkivsp/ "ctyp`/÷lq lkk%pxh {|fj 20~u 2de.`fI |||s ~o~`!mua L{fk/|l`pkk om	~m4hcwfm`}e tgq(a!k{`z|!ufp - `jcepo1/9 dcx • dyv{. *|abjj 1àcadlu0ya• g dfy4)! qe2np(qt`4n|gr uk{k3jw|8rkgr 3jrifk`k|
Le besoin de communications sécurisées a donné naissance à une nouvelle science que nous appelons cryptologie..	Nd"bdsmio! fe!bnomtoh ccthn or"sëctsksè dr!cenolé!n `iqs`oae!?!t od"nnutem mgrchdlcd! ptd"nour!cp re mnls!bsyrtn mnfke/	Od"bgsnhl ee"cnlouohbct hno r!sëctshrègs!`! enlné!lahsraob g á!tod lotwdmm d!qcheobg ptd!omus `qremnor!aryq unnoghd.

On voit que si on change les valeurs des conditions initiales le résultat est changé.

6. Conclusion :

L'utilisation du chaos dans les télécommunications est étudiée depuis plusieurs années. Le chaos est obtenu à partir de systèmes non linéaires; il correspond à un comportement borné, de ces systèmes, ce qui le fait apparaître comme du bruit pseudo aléatoire. Il peut donc être utilisé pour masquer ou mélanger les informations dans une transmission sécurisée.

L'originalité de cette communication repose sur la prise en compte des propriétés de signaux chaotiques issue soit d'équations différentielles soit de récurrences discrètes non linéaire.

Nous avons pris comme exemple l'attracteur de Hénon Lozi dans le cas des équations discrètes non linéaires, les résultats de chiffrement sont satisfaisants. La sécurité de ce principe réside dans l'impossibilité de connaître la clé secrète du ce système chaotique crypto système qui est fonction du nom de l'attracteur utilisé en plus de l'état initiale et de pas d'échantillonnage.

Aussi, il faut noter que les attaques utilise contre se type d'algorithmes sont les mêmes que celles utilise pour le chiffrement continue sauf que dans notre cas, nous avons ajouté d'autres contraintes aux cryptanalyses.

Bibliographies :

[01]http://www.astrosurf.com/luxorion/chaos-inerte-vivant.htm

[02] http://math.cmaisonneuve.qc.ca/alevesque chaos_fract/Galerie/Galerie.html

[03] S. H. Strogatz, Nonlinear Systems and Chaos, Perseus publishing 1994.

[04] http://www.astrosurf.com/cieldaunis/chaos/resumons.html

[05] J. GLEICK 'chaos theory', Albin Michel 1989.

[06] A. Ali-Pacha A, N. Hadj-Said, B. Belmekki, A. Belghoraf, «Chaotic Behaviour for the Secrete key of Cryptographic System», Revue Elsevier Science : Chaos, Solitons & Fractals, Volume 23/5 pp. 1549-1552. Available online October 2004.

[07] A. Ali-Pacha, N. Hadj-Said, A. M"Hamed, A. Belghoraf, «Lorenz's Attractor Applied to the Stream Cipher (Ali-Pacha Generator)», Revue Elsevier Science : Chaos, Solitons & Fractals, Volume 33/5 pp.1762-1766. Available online August 2007.

[08]] http://just.loic.free.fr/chaos/

[09] http://math.cmaisonneuve.qc.ca/alevesque/chaos_fract/chaos/chaos.html

[10] B. Schneier," Applied Cryptography-Protocols, Algorithms and Source Code in C", John Wiley & Sounds, Inc, New York, Second Edition, 1996.