Table des matières

Table des figures

Liste des tableaux

Résumé

Nous avons présenté dans ce mémoire les systèmes chaotiques qui sont des systèmes déterministes non linéaires apériodiques et très sensibles aux conditions initiales. Depuis la découverte de Pecorra et Carroll que deux systèmes chaotiques peuvent se synchroniser, un intérêt significatif a été accordé à l'usage de ces systèmes pour sécuriser les transmissions. Cet intérêt est dû à leur imprévisibilité qui dépasse celle des systèmes de transmission conventionnels, et à leur simplicité d'implémentation.

L'objectif principal de ce mémoire est l'exploitation des systèmes chaotiques aux transmissions sécurisées. À ce propos nous avons étudiéles principales techniques de transmission par chaos analogiques et numériques ; d'où vient l'importance des générateurs de nombres pseudo-aléatoires à base de systèmes chaotiques.

Puis, nous avons exploité la combinaison de deux systèmes chaotiques discrets pour créer un nouveau générateur de nombres pseudo-aléatoires. L'algorithme ainsi développé conserve davantage les propriétés naturelles des systèmes chaotiques utilisés, sans perte de robustesse liée à leur implémentation.

Mots clefs : Système chaotique, transmission sécurisée, cryptographie, générateur de nombres pseudo-aléatoires.

Abstract

We have presented in this paper the chaotic systems which are aperiodic nonlinear deterministic systems and very sensitive to the initial conditions. Since the discovery of Pecorra and Carroll, that two chaotic systems can synchronize significant interest has been given to the use of these systems to secure transmissions. This interest is due to their unpredictability, which exceeds of the conventional transmission systems and their simplicity of implementation.

The main objective of this thesis is the use of chaotic systems for secure transmissions. In this regard, we have studied the main techniques of transmission by analogue and digital chaos; fromhere comes, the importance of the pseudo-random number generators based on chaotic systems.

Then, we exploited the combination of two discrete chaotic systems to create a new pseudo-random number generator. The algorithm thus developed retains more the natural properties of the chaotic systems used, without loss of robustness linked to their implementation.

Keywords: ChaoticSystem, Secure transmission, cryptography, Generator of pseudo-random numbers.

ملخص

قدمنا في هذا البحث بعرض الأنظمة الفوضوية التي هي أنظمة غير خطية حتمية دورية وحساسة للغاية للشروط الأولية. منذ اكتشاف كارول وبكورا ان نظامين الفوضى يمكن مزامنتهما. أولى اهتمام كبير لاستخدام هذه الانظمة لتأمين الاتصالات. هذا الاهتمام يرجع إلى عدم القدرة على التنبؤ بها لهذا هي تتجاوز أنظمة الإرسال التقليدية، وايضا لبساطة تنفيذها

والهدف الرئيسي من هذا البحث هو استخدام نظم الفوضى لتأمين الاتصالات. وفي هذا الصدد قمنا بدراسة تقنيات البث الرئيسية التناظرية والفوضى الرقمية؛ أين تأتي أهمية مولد الاعداد شبه عشوائية القائمة على نظم الفوضى

ثم استخدمنا مزيج من اثنين من نظم الفوضى منفصلة لخلق فرص عمل جديدة كمولد اعداد شبه عشوائية. الخوارزمية المتقدمة جيدة حيت تحافظ على الخصائص الطبيعية للنظم الفوضى كما استخدامها لا يؤدي الى فقدان قوة تنفيذها

الكلمات المفتاحية نظام الفوضى. تأمين الاتصالات. كربيتوغرافيا. مولد اعداد شبه عشوائية

« Le chaos est souvent source de vie alors que l'ordre génère les habitudes. »

Henry Brooks Adam

Introduction générale

Depuis l'antiquité, l'homme n'a pas cessé de chercher les différents moyens pour transmettre un message à son correspondant en toute sécurité. Il a fourni, à travers des époques successives, des efforts autant physiques qu'intellectuels pour pouvoir trouver des techniques de transmission efficace et appropriée.

Ces vingt dernières années ont été marquées une évolution de la technologie de l'information avec l'avènement d'internet, la miniaturisation des moyens de communication, comme le téléphone et l'ordinateur portables et les réseaux sans fil. Cette banalisation d'échange d'informations à n'importe quels lieux et moment et de n'importe quelle manière, a causé l'engouement du grand public et même les organismes de pouvoir culturel, financier, politique, militaire et scientifique.

Aujourd'hui, la mondialisation des échanges pose le problème de la sécurité (confidentialité, authenticité, et intégrité) de l'information transmise à travers les canaux publics non sécurisés. Pour résoudre cette problématique, plusieurs travaux de recherche sont déjà réalisés et d'autres sont en cours de réalisation par les chercheurs académiques. L'intérêt d'utilisation des signaux chaotiques pour sécuriser les transmissions sont confirmées par les nombreux travaux internationaux de recherche sur cette thématique, à cause de ces caractéristiques comportements apériodique, déterministe et sensible aux conditions initiales.

L'emploi du chaos pour la transmission sécurisée de l'information a été considéré comme une solution très prometteuse pour augmenter les performances des systèmes de transmission analogique ou numérique. L'inconvénient de la transmission à base de chaos analogique se traduit par le faible degré de confidentialité et la dégradation des propriétés des systèmes chaotiques. D'où vient l'importance spéciale assumée par la cryptographie dans la transmission à base du chaos numérique, à cause de ces avantages l'intégrité des données, la non répudiation et l'authenticité des données en plus de la confidentialité.

Cette techniques apportent certaines originalités par rapport aux transmissions conventionnel, et soulèvent en contrepartie de nombreux défis. Cependant, en comparant les deux modes de transmission par chaos on trouve que les crypto-systèmes numériques, ce qui est divisé on deux type symétriques et asymétriques sont plus convaincants du point de vue de sécurité et par conséquent plus adaptés aux utilisations pratiques.

En effet, les deux types d'algorithmes de chiffrement ont chacun leurs avantages et leurs inconvénients ; les algorithmes de chiffrement asymétriques sont utilisés au chiffrement des messages de petite taille, par contre algorithmes de chiffrement symétriques sont les plus adaptés aux transmissions chiffrées à cause de ces avantages assure la confidentialité des données et algorithme de cryptage performant. Le chiffrement symétrique est réalisé, selon deux modes distincts chiffrement par flux, qui opère sur un flux continu de données, adapté pour la transmission en temps réel et réalisé en général sur des supports matériels et chiffrement par bloc, qui opère sur des blocs de données de taille fixe est réalisé en logiciel et en matériel.

Le standard de chiffrement à base de chaos par bloc ou par flux, présentent des inconvénients comme difficultés de réalisation aussi la dégradation des propriétés des systèmes chaotiques.

Les travaux réalisés et présentés dans ce mémoire concernent l'étude et l'exploitation des systèmes chaotiques aux transmissions sécurisées ; tout en tenant compte des problématiques précitées. Pour résoudre ces problèmes nous allons étudier deux performances de systèmes chaotiques unidimensionnels, qui ont été appliqués au chiffrement, et avant de quantifier la qualité de performance une série de tests doit être appliquée, les tests du NIST, dont nous avons montré que ces systèmes chaotiques ne donnent pas un aspect aléatoire pour une utilisation dans les générations pseudo-aléatoires.

A ce propos, nous allons crées un générateur de nombres pseudo-aléatoires développé à base d'une combinaison de deux systèmes chaotiques précédents ce qui permet d'avoir un générateur plus efficace avec un aspect parfaitement aléatoire.

Chapitre 1

Système de transmission chaotique

I. Introduction

Les systèmes dynamiques étranges (chaotiques) sont depuis longtemps connus dans le domaine des mathématiques mais c'est seulement au cours de la dernière décennie que les applications concrètes se sont multipliées. Notre étude se focalise sur l'usage du chaos pour transmettre de l'information.

Poincaré fut l'un des premiers à entrevoir la théorie du chaos. Il découvrit la notion de sensibilité aux conditions initiales à travers le problème de l'interaction de trois corps célestes.

Le chaos a ainsi trouvé de nombreuses applications dans les domaines tant physiques que biologique, chimique ou encore économique. Ainsi, nous nous intéresserons principalement dans ce chapitre aux systèmes dynamiques chaotiques en nous attardant sur les espaces de phases, les attracteurs étranges et les scénarios de transition vers le chaos (appelés aussi bifurcations), lesquels nous permettront de mieux comprendre la nature du chaos.

II. Système dynamique

En général un système dynamique décrit des phénomènes qui évoluent au court du temps, représenté par un ensemble des variables de façon à la fois :

- Causal, ou son avenir ne dépend que des phénomènes du passé ou du présent ;
- Déterministe, à partir d'une «condition initiale » donnée à l'instant présent qui correspond à un seul état futur possible (à chaque instant ultérieur) [1].

L'évolution d'un système dynamique peut se modéliser à temps continu ou à temps discret**.**

II.1. Système dynamique à temps continu

Un système dynamique en temps continu est décrit par un système d'équations différentielles sous la forme [1] :

$$x'(t) = F(x(t), t)$$

Où$F: R^n \times R^+ \rightarrow R^n$désigne la dynamique du système continu.

L'ensemble des solutions d'un système différentiel constitue un système dynamique. En d'autres termes, la fonction f appelée champ de vecteurs, définit d'une part le système différentiel mais détermine également un système dynamique continu

- Le champ de vecteurs f est non linéaire ;
- La fonction f ne dépend pas explicitement du temps, le champ de vecteur est alors dit autonome ;
- Les systèmes étudiés sont dissipatifs : la divergence du champ de vecteurs est constante négative ou elle est en moyenne négative sur les orbites considérées.

- ***Exemple***

Plusieurs systèmes chaotiques ont été étudiés dans la littérature. Parmi ces systèmes on trouve le système de Lorenz, le système de Rossler, l'attracteur de Chen et la fonction de Jerk.

Prenons comme exemple le système de Lorenz est un des systèmes différentiels les plus connus et étudiés, vérifie ces trois propriétés[2].

$$\begin{cases} \dot{x}=\sigma(y-x) \\ \dot{y}=rx-y-xz \\ \dot{z}=-bz+xy \end{cases}$$

Avec x, y et z sont les variable d'état du système σ, r et $b$sont les paramètres de contrôle. Les paramètres pour l'exemple de trajectoire donné dans la figure I.1 ont été choisis de la manière suivante : $\sigma = 10$, $\rho = 28$, $b = 8/3$ avec la condition initiale

$(x_0, y_0, z_0) = (2, 5, 20)$.

On observe que la dynamique du système de Lorenz donnée par les équations ci-dessus est indépendante de l'instant t considéré, et généralement ce type de système est qualifié d'autonome. La dynamique dans ce cas particulier à la forme suivante :

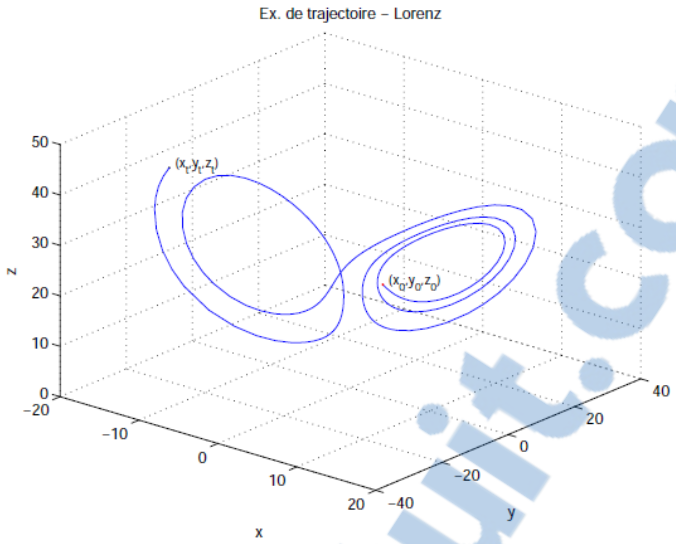

Figure I. 1: Exemple de trajectoire pour le système Lorenz.

II.2. Système dynamique à temps discret

Un système dynamique dans le cas discret est représenté par une équation aux différences finies sous la forme :

$$x_{i+1} = f(x_i, \alpha)$$

Où f est une fonction continue ou au moins continue par morceaux, $x_i \epsilon \mathbb{R}^i$ est le vecteur d'état à l'instant i (i∈ N) et $\alpha \epsilon \mathbb{R}^r$ est celui des paramètres. La fonction f peut, dans certains cas, être inversée, ce qui introduit la notion de réversibilité qui permet de remonter dans le temps [3].

III. Système chaotique

La théorie du chaos est une des très rares théories mathématiques qui ait connu un vrai succès médiatique. Apparue au début des années soixante en météorologie, elle s'est rapidement étendue à peu près toutes les sciences. Certains y ont vu, ou y voient encore, une révolution scientifique d'une importance identique à l'apparition de la mécanique de Newton, de la relativité d'Einstein ou de la mécanique quantique.

En 1963 les premiers comportements chaotiques ont été découverts par le météorologue Edward Lorenz qui a mis en évidence que, dans les systèmes non linéaires, d'infimes différences dans les conditions initiales engendraient à long terme

des systèmes totalement différents [4]. Pour mieux faire comprendre l'importance de cette sensibilité aux conditions initiales, il eut recours à une image qui contribua au succès médiatique de la théorie du chaos : celle de l'effet papillon. Cette métaphore insistait sur la disproportion entre la cause et l'effet soulignant au passage l'imprédictibilité à long terme de l'évolution de tels systèmes.

III.1 Définition

Le chaos est un comportement apériodique à long terme dans un système déterministe, qui présente une dépendance sensible aux conditions initiales.

IV. Caractéristiques d'un système chaotique

Les caractéristique et propriétés suivantes permettent de comprendre qualitativement les points marquants des systèmes chaotiques

IV.1. Comportement apériodique

L'évolution temporelle d'un système chaotique, lorsque le temps tend vers l'infini, ne converge vers aucun régime régulier (point fixe ou orbite périodique) [3]. Ce comportement irrégulier provient des non-linéarités attachées aux systèmes chaotiques.

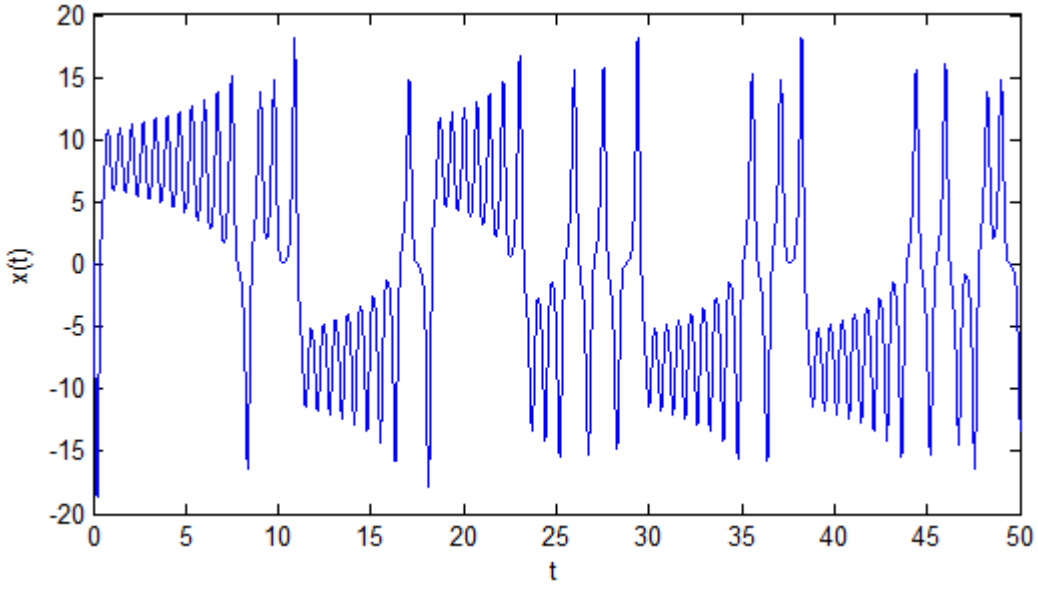

Figure I. 2:Série temporelle x(t) générée par le système de Lorenz, à partir des paramètres : a= 10, b= 8/3, c= 28 et des conditions initiales : x=0.1, y=-10 et z=5.

IV.2. Déterminisme

La notion de déterminisme signifie la capacité de prédire le futur d'un phénomène à partir d'un évènement passé ou présent.

Les systèmes chaotiques obéit à des lois mathématiques qui décrivent son comportement dynamique, à partir de son état initial de ce fait, il est possible de calculer son évolution au cours du temps si on connait exactement son état à l'instant initial, car pour chaque état à un instant donné va correspondre un et un seul état futur.

IV.3. Sensibilité aux conditions initiales

Cette propriété observée par Edward Lorenz est connue sous le nom populaire d'effet papillon. C'est une autre caractéristique permettant de reconnaître un comportement chaotique, puisque la plupart des systèmes chaotiques exhibent la sensibilité aux conditions initiales [1]. En effet, pour deux conditions initiales arbitraires très voisines initialement, les deux trajectoires correspondantes à ces données initiales divergent exponentiellement, par suite les deux trajectoires sont incomparables.

Une autre propriété des phénomènes chaotiques est qu'ils sont très sensibles aux perturbations. Il est clair que la moindre erreur ou imprécision sur la condition initiale interdit de décider à tout temps quelle sera la trajectoire effectivement suivie et, en conséquence, de faire une prédiction sur l'évolution à long terme du système.

Une des propriétés essentielles du chaos est donc bien cette sensibilité aux conditions initiales que l'on peut caractériser en mesurant des taux de divergence des trajectoires. Ceci est présenté par la figure I.3 :

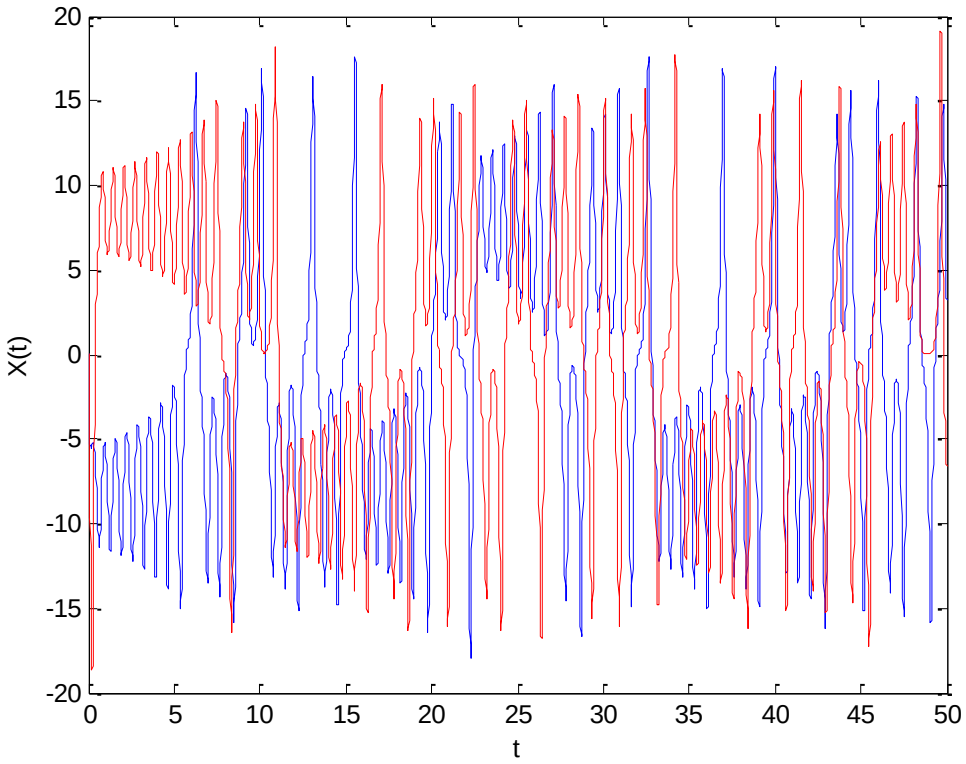

Figure I. 3: Séries temporelles X(t)et X' (t) générées par le système de Lorenz, à partir des conditions initiales : X_0=0.1 et X'_0=0.1001

IV.4. Attracteur étrange

Un attracteur est un objet géométrique vers lequel tendent toutes les trajectoires de l'espace des phases, c'est-à-dire, une situation ou un ensemble de situations vers lesquelles évolue un système, quelles que soient ses conditions initiales [5].

Etrange signifie que la forme de cet attracteur n'est pas une courbe ni une surface et n'est même pas continue mais reconstituée point par point de manière discontinue par la dynamique qui, bien qu'apparemment désordonnée, reconstitue ce type spécial d'ordre. C'est un ordre de type chaos déterministe.

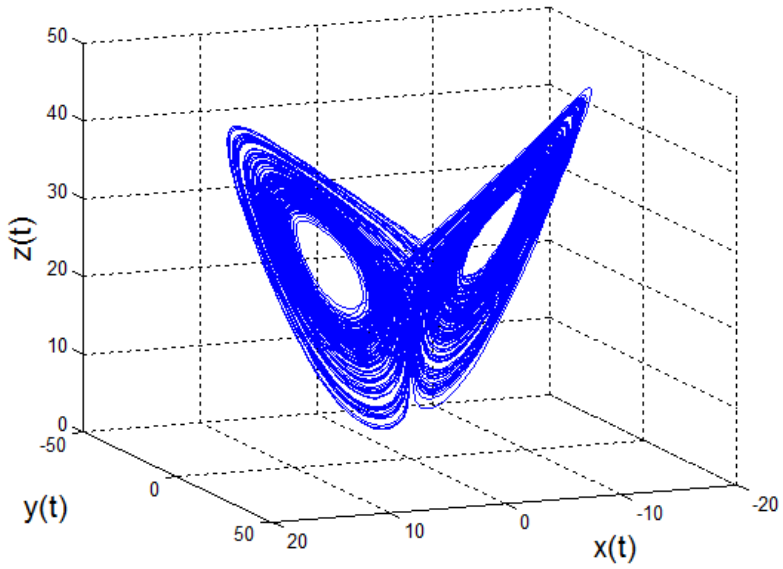

Figure I. 4: Vue en trois dimensions de l'attracteur étrange de Lorenz.

IV.5. Exposants de Lyapunov

L'évolution chaotique est difficile à appréhender car la divergence des trajectoires sur l'attracteur est rapide. Pour cette raison on essaye de mesurer ou bien d'estimer la vitesse de divergence ou de convergence. Cette vitesse est donnée par l'exposant de Lyapunov qui caractérise le taux de séparation de deux trajectoires très proches.

L'exposant de Lyapunov sert à mesurer le degré de stabilité d'un système chaotique et permet de quantifier sa sensibilité aux conditions initiales. Ainsi, le nombre d'exposants de Lyapunov est égal à la dimension de l'espace des phases et ils sont généralement indexés du plus grand au plus petit $\lambda_1, \lambda_2, \lambda_3, \dots, \lambda_n$[2].

L'exposant de Lyapunov se définit alors en fonction de la déformation subie sur la i-ème direction comme :

$$\lambda i = \lim_{t\to\infty} \frac{1}{t} \ln \frac{\delta_i(t)}{\delta_i(0)} \; avec \; i = 1 \dots \dots . n$$

L'existence d'un attracteur nécessite que la dynamique de ce système soit globalement dissipative. Le système doit être caractérisé par une stabilité globale qui correspond à la condition suivante sur le spectre de Lyapunov:$\sum_{i=1}^{n} \lambda_i < 0$.

Pour un attracteur non chaotique, les exposants de Lyapunov sont tous inférieurs ou égaux à zéro et leur somme est négative. Un attracteur étrange possèdera toujours au moins trois exposants de Lyapunov, dont un au moins doit être positif.

V. Routes vers le chaos

Il existe plusieurs types d'évolution possibles d'un système dynamique régulier vers le chaos. Le système peut passer d'un état stationnaire à un état périodique, puis au-delà d'un certain seuil, à partir d'un scénario de transition pour devenir chaotique. On distingue trois scénarios théoriques d'évolution vers le chaos [6] :

V.1 Le doublement de période

Ce scenario est le plus connu qui repose sur l'augmentation du paramètre de contrôle d'un oscillateur, la période de l'oscillateur est multiplier en deux, puis quatre, après par huit…etc. Lorsque la période est infinie, le système devient chaotique.

V.2 L'intermittence

Ce scénario est caractérisé par un mouvement périodique stable entrecoupé par des mouvements chaotiques qui apparaissent de manière irrégulière, lorsqu'on augmente le paramètre de contrôle le chaos apparait.

V.3 Quasi-périodicité

Ce scénario résulte de la concurrence de différentes fréquences dans le système dynamique. Il intervient quand un deuxième oscillateur perturbe un système initial périodique si le rapport des deux oscillateurs en présence n'est pas rationnel, alors le système est dit quasi périodique.

V.4 Bifurcation

La théorie de bifurcation est l'étude mathématique des changements qualitatifs ou topologiques de la structure d'un système dynamique. Elle survient lorsqu'une variation quantitative d'un paramètre du système engendre un changement qualitatif de ses propriétés telles que la stabilité, le nombre de points d'équilibre ou la nature des régimes permanents. Les valeurs des paramètres au moment du changement sont appelées valeurs de bifurcation.

V.4.1 Définition

Une bifurcation marque le passage soudain d'un régime dynamique à un autre, qualitativement différent [2].

Dans les systèmes dynamiques, un diagramme de bifurcation montre les comportements possibles du système, à long terme, en fonction des paramètres de bifurcation. D'une manière générale, l'évolution du point fixe vers le chaos n'est pas progressive mais marquée par des changements discontinus appelés bifurcations. La résolution du système différentiel de Lorenz par exemple, n'apporte pas toujours le chaos. Ce régime n'apparaît que pour certaines valeurs des paramètres de contrôle.

V.4.2 Exemple

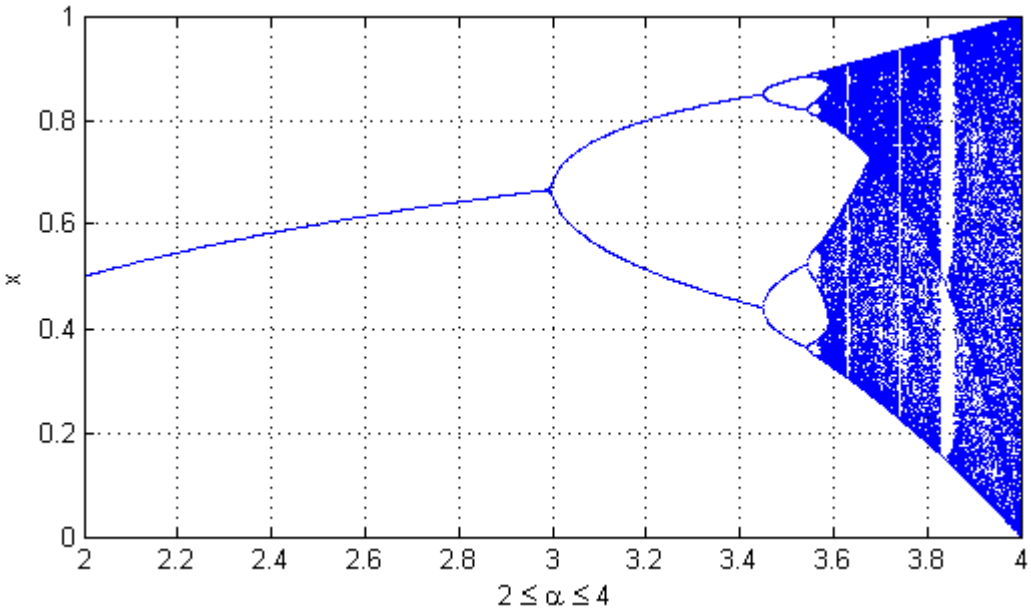

Figure I. 5: Diagramme de bifurcation de la fonction logistique

Un exemple de systèmes dynamiques unidimensionnels discrets, connu dans la théorie des systèmes non linéaires sous le nom de la carte logistique, qui est une fonction itérative définie par la fonction :

$f: [0,1] \rightarrow [0,1] x_{k+1} = f(x_k) = r x_k (1 - x_k)$ ..... (A)

Le paramètre r défini dans [0,4], est responsable du type de comportement de cette dynamique. La figure I.5 représente le comportement du système (A) en fonction du paramètre r:

- ✓ $r = 2$: la tendance de la suite logistique vers un point d'équilibre ;
- ✓ $r = 3.2$: la suite logistique oscille entre deux valeurs ;
- ✓ Pour $r = 3.5$: la suite logistique oscille entre plus de deux valeurs ;
- ✓ Pour $r = 3.9$: la suite logistique a un comportement qui semble aléatoire : c'est le comportement chaotique.

La figure I.5 représente un diagramme dit de bifurcation de Feigenbaum, qui décrit la transition de la suite logistique vers le chaos. Nous avons choisi le temps discret $k = 0,1,2,\ldots,100$ et le nombre de valeurs de r égal à 500 définies dans l'intervalle [4,0] pour notre simulation. Il s'agit dans ce cas d'une bifurcation par doublement de période, dans laquelle nous pouvons constater les caractéristiques suivantes :

-Pour$1 \leq r < 3$, le système possède un point fixe attractif qui devient instable lorsque $r = 3$;

- Pour $3 \leq r < 3.373$ le système se comporte périodiquement, de période 2^m où m est un entier qui tend vers l'infini lorsque r tend vers 3.57 ;

- Pour$3.57 \leq r < 4$ le système présente une succession de bifurcations (doublement de période), alors on aura un comportement chaotique ;

- Dans la région de comportement chaotique du système on peut trouver une fenêtre où il peut présenter des oscillations périodiques.

VI. Domaines d'application du chaos

La théorie du chaos représente le premier pas vers l'unification des sciences. Le concept moderne du chaos déterministe est de plus en plus utilisé dans les contextes scientifiques variant des mathématiques et physiques des systèmes dynamique et jusqu'aux variations temporelles complexes de tous types (exemples : chimie, biologie, physiologie, économie et même dans la psychologie).

VI.1 Biologie

En biologie la théorie du chaos permet d'expliquer les variations des populations animales, et aussi dans la médecine pour la prévision des crises d'épilepsie.

VI.2 Economie

En économie, les mouvements commerciaux et les marchés financiers, ainsi que les cycles économiques, peuvent être expliqués en partie par la théorie du chaos, quipermet de modéliser des expériences aléatoires complexes, d'où l'utilisation en finance, pour modéliser les variations des cours de la Bourse.

VI.3 Informatique

En informatique, des procédés de compression d'images ont été mis au point à partir des fractales. Des images de synthèse, au cinéma ou dans le domaine des jeux vidéo.

VI.4 Télécommunication

L'utilisation du chaos pour sécuriser les télécommunications est un sujet d'études depuis plusieurs années. Le chaos est obtenu à partir de systèmes non linéaires ; il correspond à un comportement stable, apériodique et éventuellement 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 repose sur la prise en compte des propriétés de signaux chaotiques issus soit d'équations différentielles soit de récurrences discrètes non linéaires [4].

Alors que L'idée d'utilisations du chaos dans les communications sécurisés à multiutilisateurs sont souvent basées sur le contrôle et l'utilisation adéquate des d'orbites périodiques instables, l'idée principale est de se servir du squelette d'un attracteur chaotique comme un réservoir d'ondes potentiels de communications. De cette façon, le nombre d'utilisateurs, pourvus chacun d'un code propre dans le même canal.

L'intérêt des attracteurs multi-plis réside dans leur possibilité de permettre de générer des orbites plus courtes (par un chaos plus compliqué) et donc une

transmission plus rapide des messages, ainsi qu'une meilleure sécurité dans les communications.

VII. Conclusion

Ce chapitre avait comme objectif d'introduction de quelques notions élémentaires concernant les systèmes dynamiques ainsi que l'étude théorique du phénomène chaotique qui a un comportement sensible aux conditions initiales et un aspect semblable à l'aléatoire, par la suite nous avons présenté la route vers le chaos et nous avons cité les domaines d'application des systèmes chaotiques.

Dans le chapitre suivant nous allons présenter les différentes méthodes de chiffrement par chaos analogique ainsi que numérique avec leurs avantages et inconvénients.

Chapitre 2

Transmissions sécurisées à base du chaos

I. Introduction

Le chaos est obtenu à partir des systèmes non linéaires, sensible aux conditions initiales ; il correspond à un comportement stable, apériodique et éventuellement borné, de ces systèmes ce qui fait apparaitre comme du « bruit » pseudo-aléatoire. Donc il peut être utilisé pour masquer ou mélanger les informations dans une transmission sécurisée. Ainsi, l'utilisation du chaos dans les transmissions sécurisées est devenue un domaine de recherche très actif depuis les années 1990 [2]. En effet, le chaos déterministe peut générer des comportements dynamiques d'apparences aléatoires. Il serait intéressant d'utiliser ces derniers comme porteuses d'informations en télécommunications, en particulier pour transmettre des quantités importantes d'information [1].

Dans ce chapitre on va exposer les principales méthodes des transmissions sécurisées à base du chaos que ce soit analogique ou numérique.

II. Transmission par chaos analogique

L'intérêt d'utiliser des signaux chaotiques dans les transmissions analogiques réside dans deux propriétés fondamentales du chaos [3] :

- 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 au départ (sensible aux conditions initial ce qu'on a vu dans le premier chapitre).
- Un système chaotique engendre un signal à large spectre et peut donc permettre de transmettre des signaux très variés.

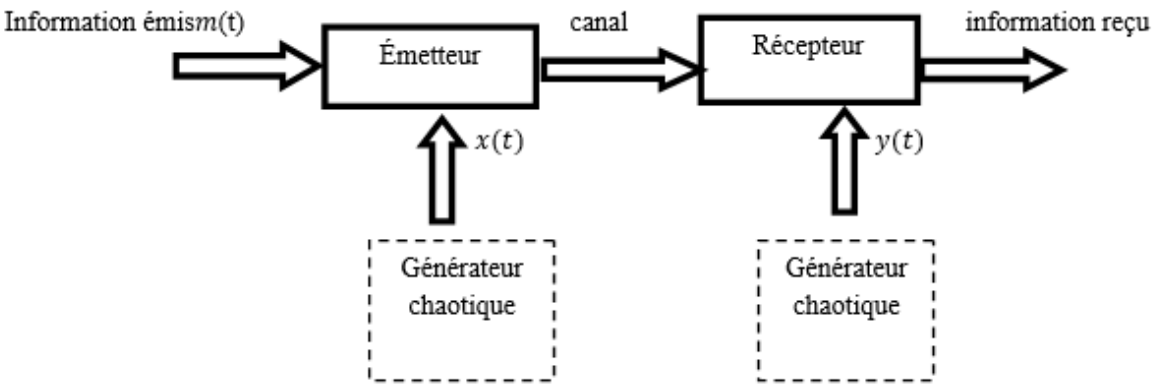

Figure II. 1: Principe de transmission par chaos analogique.

Le principe de transmission par chaos analogique repose sur ces deux propriétés comme indiqué dans la figure II.1.Il consiste à mélanger l'information $m(t)$ avec une séquence chaotique issue d'un système chaotique émetteur, décrit généralement par une représentation d'état t . Seule la sortie $y(t)$ de l'émetteur est transmise au récepteur via un canal public. Ce dernier a pour rôle d'extraire l'information originale à partir du signal reçu $y(t)$. La récupération du signal $m(t)$ exige une synchronisation entre l'émetteur et le récepteur. Cela est possible grâce au comportement déterministe des systèmes chaotiques.

II.1 Synchronisation des systèmes chaotique

Dans les systèmes de transmission, la synchronisation est une clé très importante pour une transmission réussie. La synchronisation classique employée dans les systèmes de transmission cherche à reproduire juste le signal périodique de la porteuse. Par contre, la synchronisation chaotique au niveau du récepteur cherche à dupliquer le signal chaotique généré par l'émetteur selon les travaux de Pecora et Carollen [2], [8]. Les deux chercheurs ont défini la synchronisation chaotique ou synchronisation identique qui consiste à diviser le système d'origine en deux sous-systèmes de telle sorte que les variables dynamiques de départ soient réparties de part et d'autre, dans chacun des sous-systèmes. Il s'agit ensuite de reproduire les sous-systèmes à l'identique et de les mettre en cascade. Le signal issu du système de départ

(système maitre) sert à synchroniser le premier des sous-systèmes dupliqués mis en cascade qui lui-même permet de synchroniser le second sous-système dupliqué. La synchronisation des systèmes chaotiques est devenue un thème de recherche très actif depuis 1990. Plusieurs techniques de synchronisation des systèmes chaotiques ont été proposées et exploitées dans les transmissions sécurisées. Leur fonctionnement consiste à appliquer un couplage aux systèmes chaotiques (émetteur/ récepteur), par la transmission de quelques composantes du vecteur d'états du système maître, en vue d'unifier leurs comportements. Ainsi selon la nature de liens on distingue : le couplage mutuel ou le couplage unidirectionnel (maître-esclave). Ce dernier est le plus convenable aux transmissions sécurisées, car il est plus simple à mettre en œuvre, comme il peut être traité comme un problème de conception d'observateur non linéaire, qui supporte plusieurs configurations adaptées aux différentes classes de systèmes chaotiques [1].

II.2 Techniques de transmission par chaos analogique

Différentes technique d'injection de l'information dans un système chaotique ont été proposées dans la littérature. Nous allons présenter par la suite les principales méthodes proposées pour l'exploitation du chaos dans les transmissions analogiques.

II.2.1 Masquage d'information

Cette technique est considérée comme la première proposition d'utiliser le chaos pour sécuriser les transmissions. Son principe est de brouiller le signal message $m(t)$ dans un signal chaotique $c(t)$, par une opération d'addition directe avant de le transmettre, afin d'avoir un signal crypté $s(t)$. Pour récupérer le signal message au niveau du récepteur autorisé, le même système générateur du chaos est utilisé à la fois à l'émission et à la réception, avec la différence que dans le récepteur ce système est contrôlé par le signal reçu $r(t)$pour obtenir la synchronisation [2].

L'ordre de grandeur du signal message, doit être impérativement très faible par rapport à celui du signal chaotique $c(t)$, pour éviter le risque d'être piraté, sans savoir le signal$c(t)$ exact et pour avoir une bonne synchronisation au niveau du récepteur autorisé.

A la réception, le signal message est reconstitué par la différence entre le signal reçu $r(t)$ et le signal chaotique$c(t)$résultant de la synchronisation. La figure II.2 illustre le principe du masquage d'information par chaos.

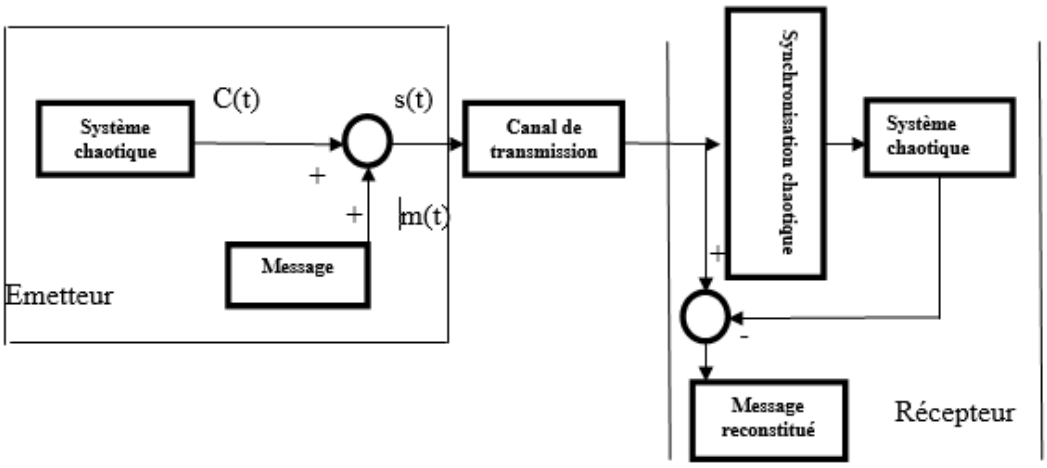

Figure II. 2: Masquage chaotique par addition.

Les avantages du masquage chaotique par addition résident dans sa simplicité deréalisation, inversement on souligne des inconvénients qui limitent l'application de cette technique en pratique, tels que :

- La synchronisation non parfaite entre l'émetteur et le récepteur ;
- Le faible degré de sécurité démontré ;
- La sensibilité à la disparité des paramètres entre les systèmes chaotiques.

II.2.2 Modulation chaotique

Plusieurs méthodes ont été proposées pour moduler un signal informationnel par un signal chaotique. Elles se distinguent par la modification d'états ou des paramètres des systèmes chaotique employés [2].

II.2.2.1 Modulation par commutation « CSK »

L'apparition de cette technique est considérée comme une conséquence des problèmes d'application pratique du masquage par addition. Elle a été proposée par le groupe de Kocarev et sa dénomination actuelle connue par « Chaos shift keying :

CSK », le système de modulation par CSK estconstitué par un modulateur CSK au niveau de l'émetteur et par un démodulateur CSK au niveau du récepteur raccordés par un canal comme il est représenté sur la figure II.3 [2] ; [9].

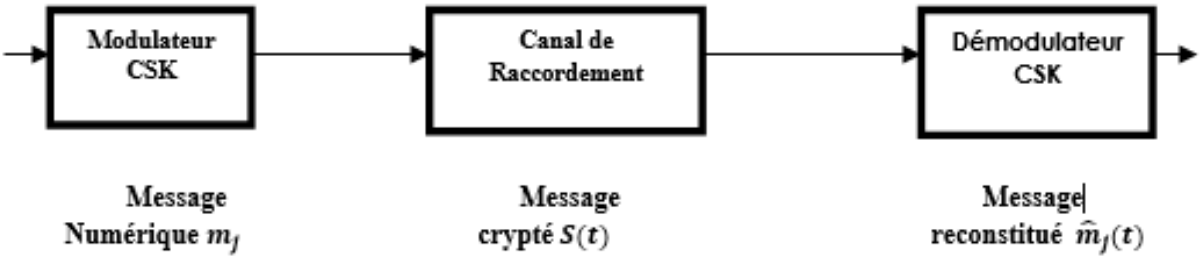

Figure II. 3: Schéma présente la Modulation par commutation « CSK ».

II.2.2.2 Modulation paramétrique

Le principe de cette méthode consiste à utiliser le signal d'information, généralement denature binaire, pour moduler l'un des paramètres du système chaotique émetteur. Le systèmerécepteur synchronise d'une manière adaptative avec l'émetteur chaotique et le signal d'information est restauré par l'intermédiaire d'une loi d'adaptation. Cette méthode à est présentée dans la figure II.4.

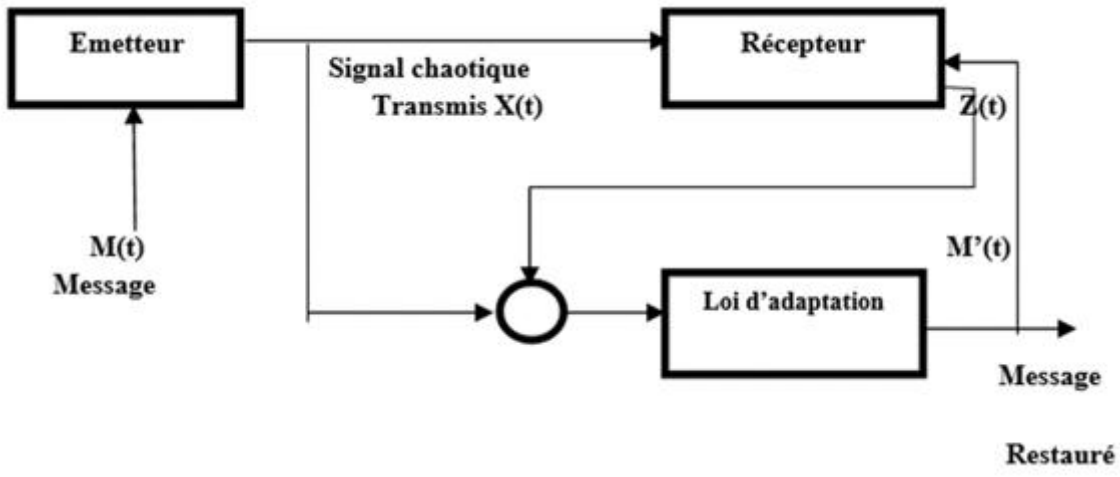

Figure II. 4: Schéma représentatif de la technique de modulation paramétrique.

La modulation paramétrique apporte quelques avantages par rapport aux techniques précédentes, notamment concernant le niveau de sécurité. Elle offre aussi des capacités de multiplexage chaotique, de sorte que plusieurs messages peuvent moduler différents paramètres d'un même système chaotique et par conséquent être envoyés et récupérés en utilisant un seul signal de transmission [9].

Cependant, l'inconvénient majeur de cette méthode s'agit du mécanisme de synchronisation adaptative employé, qui nécessite un temps de convergence pendant lequel les paramètres et l'information sont construits de manière erronée, ce qui dégrade la qualité de la transmission.

II.2.2.3 Modulation par inclusion

Cette technique consiste à injecter le message dans la dynamique chaotique d'émetteur. La synchronisation et la restauration de l'information côté récepteur peut être établie suivant deux techniques, reposantsoit sur les observateurs à entrées inconnues, soit sur l'inversion du système émetteur. La figure II.5 illustre la méthode d'inclusion [3] ; [8].

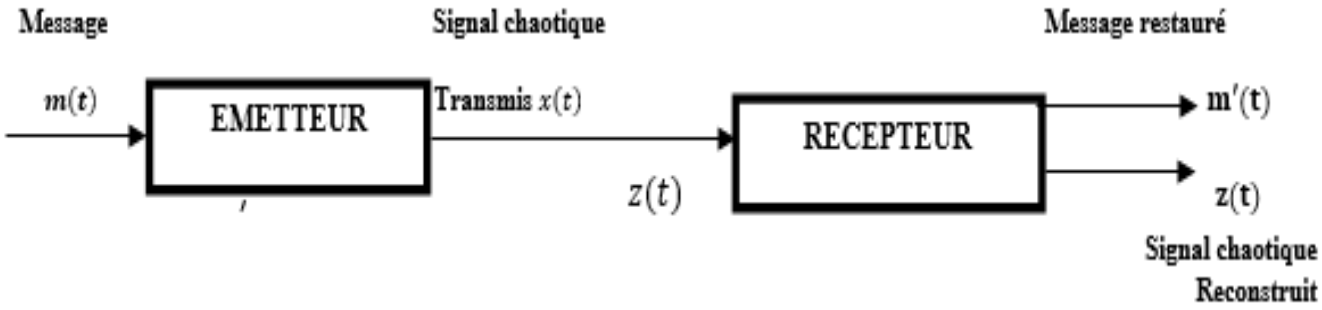

Figure II. 5: Schéma représentatif de la modulation par inclusion.

La modulation par inclusion chaotique présente beaucoup d'avantages qui motivent son exploitation en pratique, principalement à cause de son niveau de sécurité plus élevé par rapport aux techniques précédentes.

II.2.3 Etalement de spectre chaotique

L'étalement de spectre désigne en général un ensemble de techniques de transmission de l'information utilisées pour combattre les effets néfastes de l'interférence produite par un brouillage. L'étalement de spectre est utilisé aussi pour masquer le signal en utilisant une faible puissance d'émission, et par conséquence le signal sera difficile à intercepter par un utilisateur non-autorisé [3].

Les signaux chaotiques peuvent être employés à cet effet. L'idée de base consiste à remplacer le générateur de séquences pseudo-aléatoires employé dans les techniques d'étalement conventionnelles par une dynamique chaotique, puisque les séquences chaotiques possèdent des propriétés similaires aux séquences d'étalement.

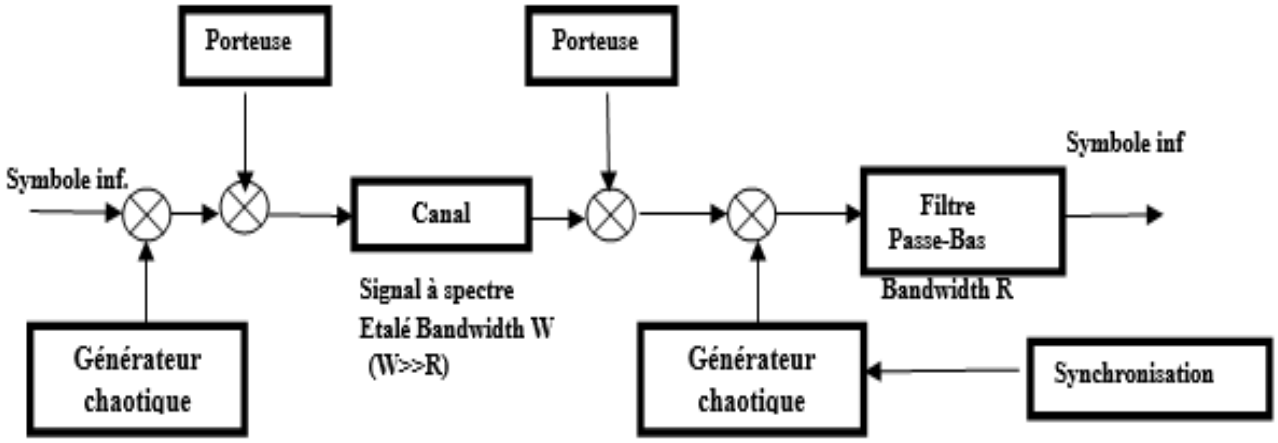

Figure II. 6: Modèle d'un système de communication a étalement de spectre par séquence chaotique.

II.3 Avantages et inconvénients des transmissions par chaos analogique

Les méthodes de transmission à base de chaos analogique permettent de crypter et d'étaler le spectre du signal en même temps dont les informations sont transmises et reçues en temps réel, tout en exigeant des circuits moins compliqués par rapport aux méthodes de transmission conventionnelles. Toutefois, la plupart d'entre elles présentent des inconvénients communs et partagent les mêmes difficultés de réalisation [3] :

•**Faible degré de confidentialité** : l'application d'une synchronisation consiste à transmettre une information suffisante sur le processus chaotique employé au chiffrement. Par conséquent des diverses attaques pourraient être menées à partir de l'exploitation du signal de synchronisation.

•**Dégradation des propriétés des systèmes chaotiques** : la force du couplage appliqué aux systèmes chaotiques lors du processus de synchronisation, sert à tolérer l'effet du bruit de transmission et corriger les éventuelles perturbations dues aux incertitudes des paramètres

•**Faible robustesse contre le bruit** : en présence du bruit les performances de synchronisation dans les transmissions sécurisées par systèmes chaotiques se dégradent.

•**La non-conformité des signaux chaotiques aux infrastructures de télécommunication actuelles** : en raison de leur nature pseudo-aléatoire, qui prend des valeurs réelles continues, exigeant un canal avec une capacité infinie, impossible à satisfaire.

III. Transmission par chaos numérique

L'exploitation du chaos dans ce contexte consiste à étudier les possibilités d'utilisation des signaux chaotique issus des récurrences discrètes pour chiffrer les informations dans une transmission numérique.

III.1 Cryptographie par chaos

La cryptographie désigne l'ensemble des techniques permettant de transmettre des données confidentielles sur un milieu non sécurisé sans qu'un intrus ne puisse découvrir le contenu. Ces données seront déchiffrées seulement par le destinataire ou celui connaissant la clé de déchiffrement [10]. La cryptographie garantit entre autre l'intégrité, la non répudiation et l'authenticité des données en plus de la confidentialité [3] :

- **La confidentialité** : Permet de garantir que seul le destinataire ou le détenant de la clé puisse découvrir le message en clair : accès aux informations est sécurisé.
- **L'intégrité :** Permet le non modification ou non altération des données pendant le stockage ou la transmission
- **L'authenticité :** Permet de garantir l'origine et l'identité de l'émetteur
- **Le non répudiation** : Empêche de nier la participation à un échange ou traitement de données.

Les algorithmes de chiffrement sont classés souvent selon les types de clés utilisées et les procédures de chiffrement comment indiqué dans la figure (II. 7). Notant que les algorithmes de chiffrement symétriques sont les plus adaptés aux transmissions chiffrées à cause de ces avantages [3] :

•Assure la confidentialité des données ;

•Algorithme de cryptage performant ;

•Plus utilisé pour la transmission de long message (débit plus important) ;

•Les clés sont relativement de faible taille et sa primitives de la sécurité qui présente des processus de base sur lesquels tous les mécanismes de protection sont construits. Également les algorithmes cryptographiques vus comme une primitive de sécurité.

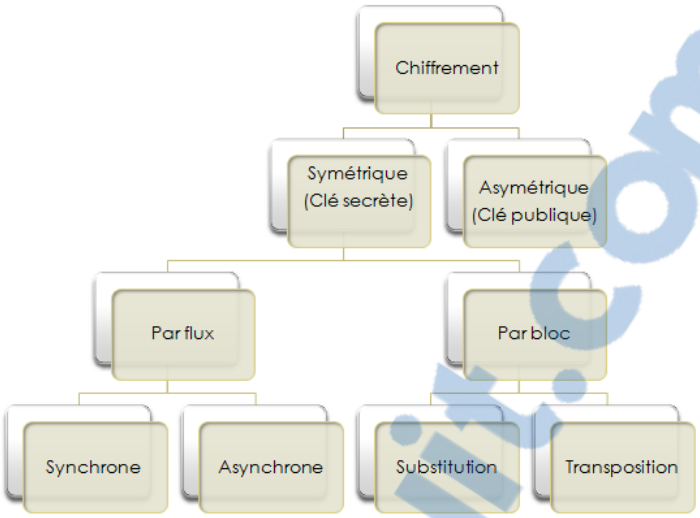

Figure II. 8: Classification des algorithmes de chiffrement.

III.1.1 Chiffrement asymétrique

Le chiffrement asymétrique (appelé aussi à clé publique) a été proposé par Diffie et Hellmanen 1976. Son principe repose sur l'utilisation de deux clés différentes, une clé pour le chiffrement et une autre clé différente pour le déchiffrement [11]. N'importe qui peut utiliser la clé de chiffrement ou la clé publique pour chiffrer un message, mais seul celui possédant la clé de déchiffrement, où la clé privée peut déchiffrer le message chiffré résultant [12].

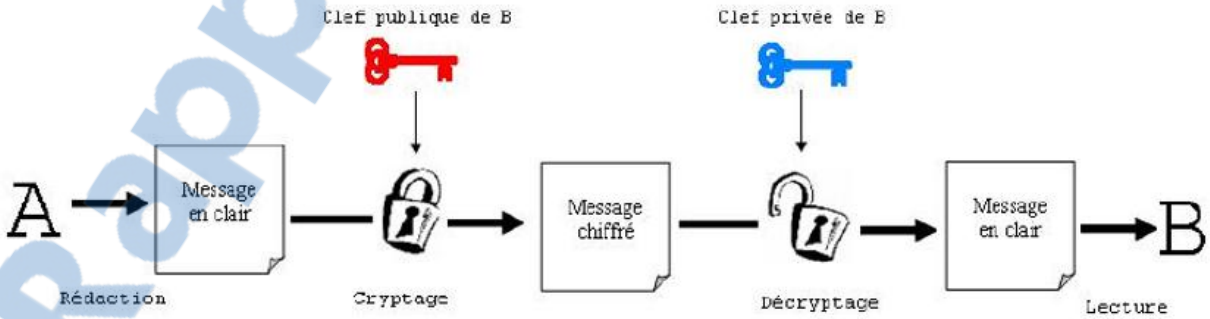

Figure II. 9: schéma présente le principe de chiffrement asymétrique.

.

Le chiffrement à clé publique offre trois services essentiels qui sont :

- le chiffrement/déchiffrement qui assure la fonction de confidentialité
- la création des signatures numériques qui assure l'authentification, l'intégrité et la fonction de non-répudiation
- l'échange des clés symétriques.

III.1.2 Chiffrement symétrique

Le chiffrement symétrique ou à clé secrète est la plus ancienne forme de chiffrement. Le principe du chiffrement symétrique est que l'émetteur et le récepteur partagent une même clé secrète, c'est-à-dire les clés de chiffrement et de déchiffrement sontidentiques [11] ; [13].

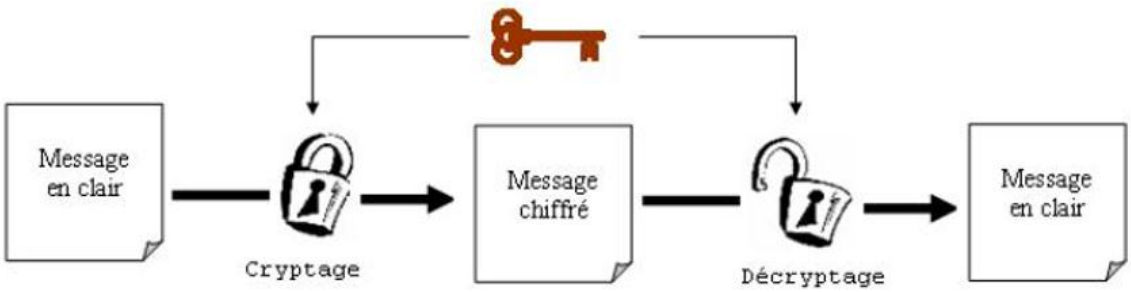

Figure II. 10: schéma présente le principe de chiffrement symétrique.

L'exploitation du chaos dans la cryptographie est orientée beaucoup plus vers la création des crypto-systèmes symétriques. Le principe de tel crypto-système repose sur un système qui compose de [13]

- ✓ **Algorithme de chiffrement** : permet de transformer un message confidentiel afin d'en cacher le sens à tous ceux qui ne sont pas autorisés à la connaitre.
- ✓ **Clé secrète** : est un paramètre utilisé en entrée d'une opération cryptographique chiffrement ou déchiffrement peut se présenter sous plusieurs formes : mots ou phrases.

- ✓ **Algorithme de déchiffrement** : réalise l'opération inverse du chiffrement, il a pour but de récupérer l'information masquée ; comme illustré dans la figure II.10.

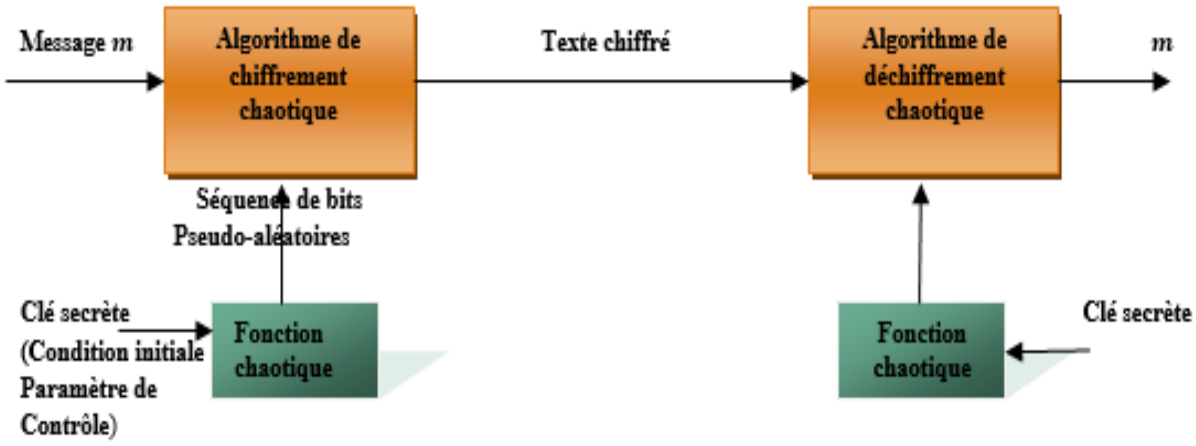

Figure II. 11: Schéma de principe d'un crypto-système basé chaos.

A l'émission Les algorithmes de chiffrement chaotique utilisent des nombres pseudo-aléatoires générés par les fonctions (ou générateurs) chaotiques. Une fonction est dite chaotique, si elle est non linéaire et surtout si elle est sensible aux conditions initiales, même extrêmement faibles de la valeur de la clé secrète qui est formée des conditions initiales et des paramètres du système. La séquence de nombres pseudo-aléatoires générée est utilisée par l'algorithme chaotique pour chiffrer le message en clair à la réception, la même fonction chaotique est utilisée avec la même clé secrète pour générer la même séquence de nombres pseudo-aléatoires. Cette séquence sera utilisée par un algorithme de déchiffrement chaotique afin de récupérer le message en clair qui peut être des données numériques, une image, un texte, etc.

Les crypto-systèmes chaotiques peuvent être classés en deux catégories principales : chiffrement chaotique par flot et chiffrement chaotique par bloc.

III.1.2.1 Crypto-systèmes chaotiques par bloc

La méthode de chiffrement par bloc consiste à diviser le message en blocs de bits de longueur fixe. Chaque bloque est chiffré l'un après l'autre [3]. Le chiffrement peut être effectué selon deux façons :

- **Substitution** : les bits d'un bloc sont substitués par d'autres bits, ce qui permet d'ajouter de la confusion, c'est-à-dire de rendre la relation entre message et le texte chiffré aussi complexe que possible ;
- **Transposition** : les bits d'un bloc sont permutés entre eux, ce qui permet d'ajouter de la diffusion, c'est-à-dire de réarranger les bits de message afin d'éviter que toute redondance dans le message ne se retrouve dans le texte chiffré.

La figure II.11 illustre le principe de chiffrement par bloc [3] :

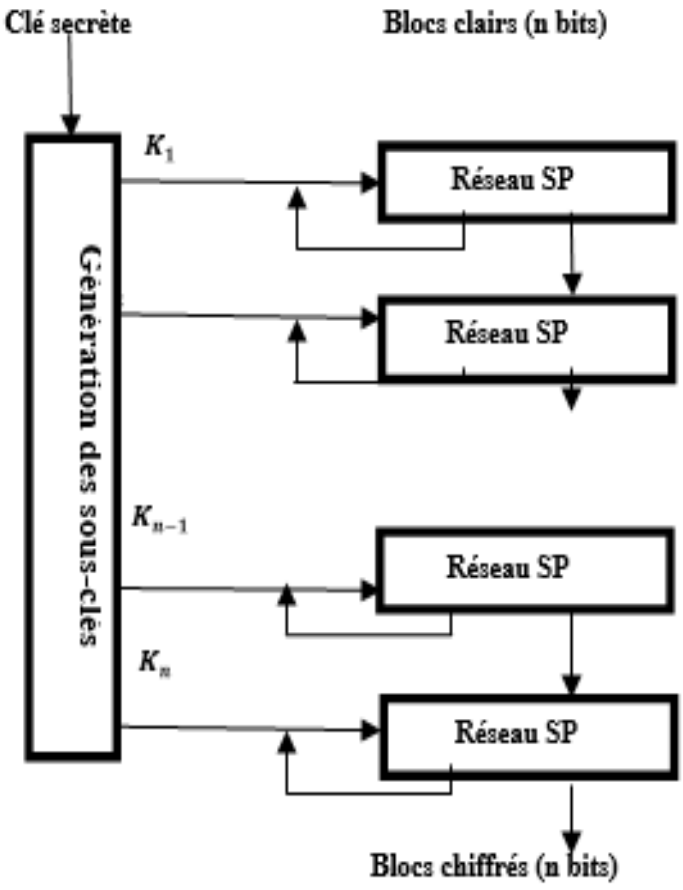

Figure II. 12: Principe du chiffrement par Bloc.

L'utilisation des systèmes chaotiques dans la conception des algorithmes de chiffrement par bloc consiste à créer des procédures de substitution et de transposition à base de séquences pseudo-aléatoires issues des systèmes chaotiques. Ainsi, les données sont cryptées par bloc de longueur qui différent selon l'algorithme employé. Les propriétés de la transformation chaotique et la façon de son implémentation déterminent le niveau de sécurité de tels algorithmes [12].

Il existe plusieurs algorithmes de chiffrement par bloc chaotiquesqui consiste à divisé le domaine de la récurrence logistique a des sous intervalles qu'on a des caractères différents dans le message à chiffrer, avec chaque intervalle est affecté à un seul caractère. Ainsi on trouve Alvarez et Al, ont proposé une nouvelle technique de chiffrement par bloc basée sur le comportement de la récurrence Tente le principe de chiffrement, qui s'opère sur des blocs de taille variable, consiste à itérer la récurrence Tente en sens inverse sur les régions correspondant aux caractères du message à chiffrer.

III.1.2.2 Crypto-systèmes chaotiques par flux ou flot

Les algorithmes de chiffrement par flot tirent leur origine du principal système de chiffrement offrant une confidentialité absolue, le chiffrement de Vernam (ou One Time Pad). Celui-ci consiste à chiffrer un message de n bits à l'aide d'une clé de n bits au moyen d'un simple ou exclusif [3].

La définition des algorithmes de chiffrement par flot induit les propriétés suivantes [4] :

- ✓ La suite chiffrant ne dépend pas du message clair, mais uniquement de la clé secrète ;
- ✓ Il est possible de chiffrer des messages de tailles variables ;
- ✓ Le chiffrement et le déchiffrement s'effectuent de la même manière, puisque le « ou exclusif» est une opération involutive ;
- ✓ L'impact de la modification d'une partie du message chiffré pendant la transmission du message est limité à cette partie du message déchiffré.

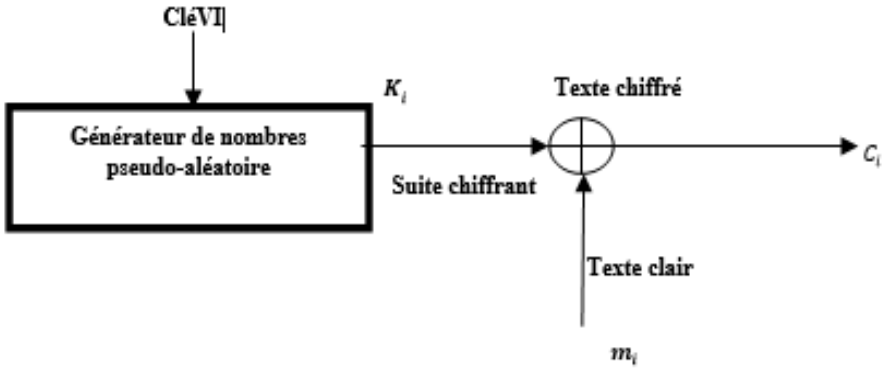

Figure II. 13 : Principe du chiffrement par flux.

Cependant, cela n'est valable que si plusieurs conditions sont vérifiées :

- La clé doit être aussi longue que le message clair.
- La clé doit être une chaîne de bits parfaitement aléatoire.
- La clé ne doit être utilisée qu'une fois.

Ces trois conditions font du chiffrement de Vernam une méthode difficile à utiliser en pratique. En effet, ces conditions imposent que le destinataire d'un message chiffré connaisse préalablement la clé qui est aussi longue que le message. De plus cette clé ne pouvant être réutilisée sans compromettre la sécurité du système. Il est nécessaire donc que le destinataire possède à l'avance suffisamment de clés, ou puisse recevoir les clés utilisées via un canal sûr.

Un chiffrement par flot se présente souvent sous la forme d'un générateur de nombres pseudo-aléatoires avec lequel on opère un XOR entre un bit à la sortie du générateur et un bit provenant des données selon le principe illustré par la figure(II. 14). Grace à leurs propriétés intéressantes, les systèmes chaotiques peuvent jouer le rôle de générateurs de nombres pseudo-aléatoire au sein des algorithmes de chiffrement par flux. .ces générateurs diffèrent selon le genre et le nombre des systèmes chaotiques utilisés, ainsi que la manière d'extraire les bits pseudo-aléatoires.

Une des principales caractéristiques des algorithmes de chiffrement à flot est qu'ils permettent d'atteindre un très haut niveau de performances. Ces performances

s'expriment soit en termes de vitesse de chiffrement soit en termes d'efficacité matérielle. On distingue deux principaux types d'algorithmes à flot :

- ✓ Les algorithmes adaptés à une implantation logicielle, qui peuvent atteindre des vitesses de chiffrement très élevées (de l'ordre de plusieurs Gbits/s sur le processeur d'un ordinateur standard).
- ✓ Les algorithmes adaptés à une implantation matérielle, dont les implantations sont efficaces en termes de taille ou de consommation électrique.

III.1.2.3 Avantages et inconvénients de chiffrement par bloc et par flot

Dans l'algorithme de chiffrement par bloc, on ne peut commencer à chiffrer et à déchiffrer un message que si l'on connait la totalité d'un bloc. Ceci occasionne un délai dans la transmission et nécessite également le stockage successif des blocs dans une mémoire tampon.au contraire dans le chiffrement par flot chaque bit transmis peut être chiffré ou déchiffré indépendamment des autres. D'autre part les chiffrements par flot ne requièrent évidemment pas de padding c'est à dite l'ajoute de certains bits au message clair dont le seul objectif est d'atteindre une longueur multiple de la taille du bloc [10]. Un autre avantage de chiffrement par flot est que contrairement aux chiffrements par bloc le processus de déchiffrement ne propage pas les erreurs de transmission .Par contre dans le cas d'un chiffrement par bloc c'est tout le bloc contenant la position erronée qui devient incorrect après déchiffrement .c'est pour cette raison que le chiffrement par flot est également utilisé pour protéger la confidentialité dans les transmissions bruitées.

IV. Conclusion

Dans ce chapitre on a exposé les principales méthodes des transmissions sécurisées à base du chaos que ce soit analogique ou numérique. Nous avons conclu que chacun de ces techniques offrent de grands potentiels même si on y trouve quelques défauts. Cependant, en comparant entre les deux modes on trouve que les crypto-systèmes numériques sont plus sécurisés et donc plus adaptés aux utilisations réelles. Ainsi quele chiffrement par flux a plus d'avantages par rapport aux chiffrements par bloc.

Ces techniques reposent souvent sur l'utilisation des systèmes chaotiques en tant que générateurs de nombres pseudo-aléatoires, grâce aux fortes similitudes existantes entre les deux mécanismes. D'où nous consacrons le chapitre suivant à l'étude et l'exploitation des systèmes chaotiques dans la génération de nombres pseudo-aléatoires.

Chapitre 3

Utilisation du chaos dans la génération de nombres pseudo-aléatoires

I. Introduction

Les générateurs pseudo-aléatoires acquis une grande importance dans les divers domaines, allant du médical à la sécurisation, et se sont montrés être d'une grande efficacité. Ils sont souvent employés sur des ordinateurs plus précisément dans les jeux d'ordinateurs personnels, dans diverses ou les applications cryptographiques etles systèmes de chiffrement .Mais aussi pour la confidentialité des échanges sur les réseaux sans fils ainsi pour la sécurisation des applications web sans oublié le domaine biomédical.

Ces générateurs sont facile à implanter et permet des débits importants tout en produisant des suites qui ont des bonnes propriétés statistiques [15]. Ils sont donc très adaptés aux applications ne nécessitant pas l'imprévisibilité des suites.

Les générateurs pseudo-aléatoires possèdent malgré leur large popularité des propriétés statistiques assez mauvaises, et ne répondaient pas aux toutes applications de transmission. Plus récemment, des algorithmes robustes vis-à-vis des analyses statistiques ont été élaborés, mais aucun algorithme pseudo-aléatoire ne peut vraiment générer de suite à l'abri de toute analyse statistique. ces générateurs actuels sont donc obligés de faire intervenir une part de hasard qui n'est pas générée par un moyen déterministe : on s'oriente vers des générateurs hybrides ainsi que chaotique , possédant un algorithme de génération de nombres pseudo-aléatoires robuste, et s'initialisant sur un moyen physique de production de hasard.

En effet, pour améliorer la qualité des PRNG la théorie du chaos a joué un rôle actif. L'avantage d'utiliser le chaos dans ce domaine réside dans son comportement désordonné et son imprévisibilité [15]. Ainsi, les séquences construites à partir des systèmes chaotiques possèdent des propriétés statistiques de suites de nombres véritablement aléatoires. Ces systèmes peuvent jouer un rôle dans les transmissions des données.

II. Générateurs de nombres pseudo-aléatoires

II.1. Définition (PRNG)

Un générateur pseudo-aléatoire (pseudorandomnumbergenerator) est un procédé qui, à partir d'une initialisation de taille fixée (une ou plusieurs centaines de bits) appelée graine ou germe, engendre de manière déterministe une suite de très grande longueur de séquences binaires, dite aléatoire car cette suite est arbitraire [16].

II.2. Définition (Suite pseudo-aléatoire)

Une séquence de nombres est dite pseudo-aléatoire si elle est générée de façon déterministe mais semble avoir été produite de façon purement aléatoire. Cette séquence a pour propriété que l'on peut prédire les nombres à venir à partir des nombres déjà connus et de la graine initiale [15].

Un générateur de nombres pseudo-aléatoires présente les caractéristiques suivantes [17] :

- La période de la suite doit être suffisamment grande pour que les sous-suites finies utilisées avec l'algorithme ou le protocole de cryptographique ne soient pas périodiques ;
- Les sous-suites issues du générateur doivent être sur le plan statistique, semblées aléatoire ;
- Le générateur doit être imprévisible.

III. Générateurs de nombres pseudo-aléatoires conventionnels

La génération des séquences binaires pseudo-aléatoires peuvent être implantés au niveau logiciel ou matériel. Nous allons citer dans cette partie quelques types de générateurs de nombres pseudo-aléatoires.

III.1. PRNGs basés sur les méthodes de congruence linéaire

Les générateurs linéaires congruentiels ont été introduits par Lehmer.Lebut de ce générateur est de créer une suite de nombres entiers de manière aléatoire ou plutôt avec aussi peu de régularité que possible.

III.2. PRNGs basés sur les registres à décalage linéaire

Les séquences à registres à décalage aussi appelés LFSR (Linear Feedback Shift Register) sont constitués d'un registre de n bits et d'une boucle à rétroaction intégrant une fonction linéaire de ces bits. À chaque décalage du registre (un cran vers la droite) le bit b1 est ajouté à la séquence générée et un nouveau bit est créé dans $b_n$en combinant tous les bits dans le registre par la fonction de rétroaction linéaire.

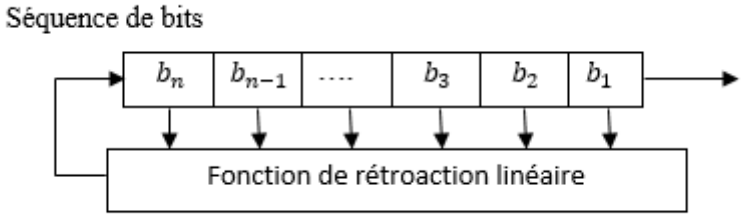

Figure III. 1: Principe de fonctionnement d'un registre à décalage à rétroaction linéaire

III.3. Générateur Blum-Blum-Shub

Générateur Blum-Blum-Shubou générateur à résidu quadratique, puisque la théorie sous-jacente à ce générateur est liée aux résidus quadratiques modulo unentier $n = p * q$, où p et q sont deux grands nombres premiers. Ce générateur est très robuste mais il est très lent comparé aux autresgénérateurs.

III.4. Générateur carré-médian

Générateur carré-médian été proposé en 1946 par John Von Neumann c'est un générateur pseudo-aléatoire connu sous le nom de la méthode middle-square. C'est un générateur très simple consiste à prendre un nombre, à l'élever au carré et à prendre les chiffres au milieu comme sortie.

IV. Générateur de nombres pseudo-aléatoires basés sur le chaos

Le caractère non-linéaire et déterministe des systèmes chaotiques permet la génération efficace des séquences de nombres pseudo-aléatoires souhaitables, à partir d'un jeu de paramètres de petite taille, qui peuvent être échangés et partagés facilement. Les systèmes chaotiques offrent donc un grand potentiel pour la génération

de nombres pseudo-aléatoires, notamment pour remplacer les registres à décalage (LFSR) qui sont largement utilisés dans ce contexte. Dans cette perspective, plusieurs PRNG chaotiques ont été créés et intégrés au sein des algorithmes de chiffrement par flux. Ils diffèrent selon le genre et le nombre des systèmes chaotiques utilisés, ainsi que la manière d'extraire les bits pseudo-aléatoires à partir des orbites chaotiques.

Parmi les systèmes chaotiques les plus adaptés à la génération de nombres pseudo-aléatoires nous citions la récurrence de Bernoulli (A) et la récurrence Skew-Tent (B), qui appartiennent aux systèmes chaotiques linéaires par morceau. Ces récurrences présentent l'intérêt d'avoir une expression mathématique très simple, tout en conduisant aux régimes dynamiques variés. Nous présentons dans ce qui suit l'étude des propriétés statistiques des séquences issues des deux récurrences chaotiques, à savoir la densité de probabilité, la fonction de corrélation et les tests de NIST (National Institute of Standards and Technology) [17].

$$x_{i+1} = (\alpha \times x_i) mod\ 1 \quad \text{.....A}$$

$$f(x_i) = \begin{cases} \frac{x_i}{\alpha} six_i \leq \alpha \\ \frac{(1-x_i)}{1-\alpha} six_i > \alpha \end{cases} \quad \text{.....B}$$

IV.1. Densité de probabilité

La densité de probabilité, connue aussi par l'entropie est cruciale pour les sources de pseudo-aléa utilisées pour le chiffrement, sont principe est de tout suite de n bit ont associé une certain quantité dont on peut déterminer la densité de probabilité ainsi que les trajectoires chaotiques doivent parcourir tous les états de l'espace des phases de façon équiprobable [10].

Nous observons d'après les courbes de densité de probabilité illustrées dans les figures (III.2 et III.3) que les histogrammes visualisés possèdent un comportement uniforme avec une densité invariante qui s'approche d'une distribution uniforme quand

N tend vers l'infini. Ce qui signifie que les séquences chaotiques issues de ces deux récurrences donne un haut niveau de confusion.

IV.2. Analyse de corrélation

L'analyse de corrélation détermine la dépendance statistique des états qui composent les trajectoires chaotiques à long terme. Une faible dépendance statistique indique que la séquence chaotique est imprévisible et reflète un aspect important de confusion. Ce qui est d'un grand intérêt pour le chiffrement de données [3].

Nous observons d'après les courbes de corrélation données dans les figures (III.2 et III.3) que les résultats de simulation sont très proches pour les récurrences Bernoulli et Skew-Tent, il n'existe aucune autocorrélation significative quel que soit le décalage temporel, à l'exception d'un seul pic très étroit au décalage zéro. D'autre part, l'inter-corrélation est très faible.

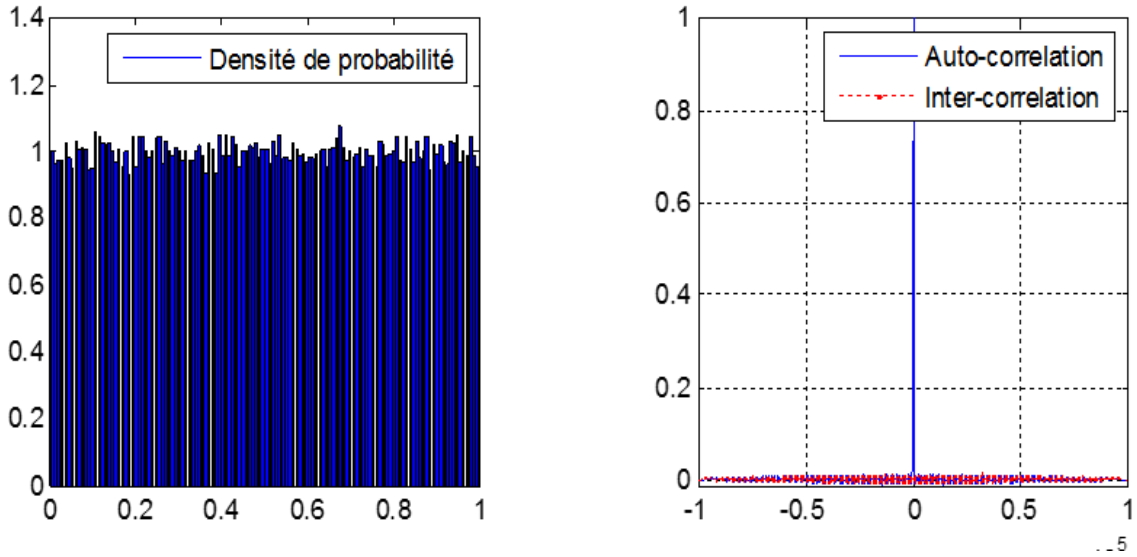

Figure III. 2: Simulation de la densité de probabilité et les fonctions d'auto/ inter-corrélation de la récurrence Skew-Tent

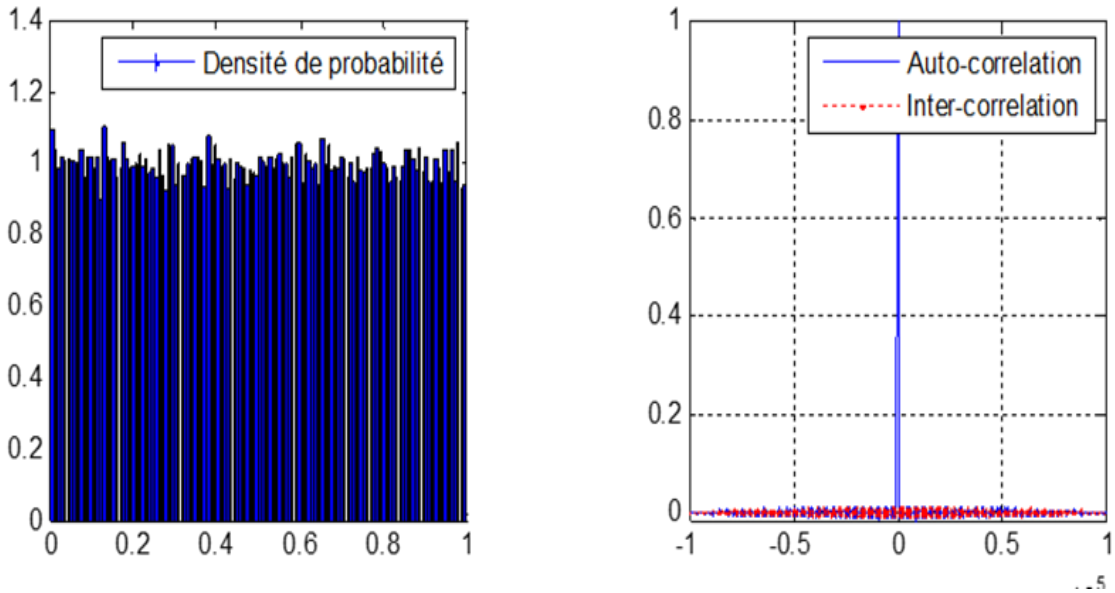

Figure III. 3: Simulation de la densité de probabilité et les fonctions d'auto/ inter-corrélation De la récurrence Bernoulli.

IV.3. Les tests du NIST

Les tests du NIST [NIST SP 800-22, 2008] forment un paquetage statistique de tests qui sont conçus pour détecter l'aspect aléatoire des séquences binaires à la sortie des générateurs de nombres pseudo aléatoires utilisés dans desgénération pseudo-aléatoire, l'ensemble des résultats de ces tests donne une idée du degré de l'aléatoire des signaux produits[12].

Nous donnons dans le tableau ci-dessous, les résultats des quinze tests de NIST sur les deux récurrences Bernoulli et Skew-Tent, en considérant des séquences binaires de longueur égale à 1Mbits, générées en double précision (64 bits). Les valeurs nommées « P-Value » représente la probabilité qu'un générateur de nombre aléatoire parfait produise une séquence moins aléatoire que la séquence testée.

On distingue que chaque test possède des propriétés différentes :

-Si P-valeur est >0 : le teste a réussi, la séquence apparait aléatoire ;

-Si P-valeur est ≤0 : le teste est raté, la séquence est non aléatoire.

Nous concluons d'après les valeurs obtenues que le comportement des récurrences Skew-Tent et Bernoulli ne donne pas un aspect aléatoire parfait.

Tests statistiques	Bernoulli (P-Value)	SkewTent (P-Value)
Approximateentropies	0.000004	×
Block frequency	0.000811	0.124693
Cumulative sums	×	×
FFT	×	×
Frequency	×	×
Linearcomplexity	0.151762	0.251555
LongestRun	0.114270	0.070370
No overlappingtemplates	✓	✓
Overlappingtemplates	0.000129	0.010173
Random excursions	×	×
Randomexcursions variant	×	×
Rank	0.034109	0.744490
Runs	×	×
Serial	0.288882	0.812006
Universal	0.066369	0.000104

Tableau 1 : Résultats des tests statistiques NIST SP 800-22 appliqués sur les deux récurrences Bernoulli et SkewTent de taille1 Mb, générés par ces paramètres (SkewTent ci=0.4185 ; p=0.5097, Bernoulli ci=0.5813, p=2.9999).

V. Conclusion

Dans ce chapitre, nous avons présenté les générateur de nombre pseudo-aléatoire d'ordre générale, en suite nous avons défini le générateur pseudo-aléatoire basés sur le chaos, par la suite nous avons proposé deux performances de systèmes chaotiques parmi d'autres, les récurrences Skew-Tent et Bernoulli.

Ces deux systèmes unidimensionnels étudiés sont capables de générer des comportements chaotiques ayant une très faible dépendance statistique (auto/inter-

corrélation).Ces récurrences Bernoulli etSkew-Tent, possèdent de meilleures propriétés qualitatives et quantitatives, Ilsgénèrent des comportements uniformes sur l'intervalle [0,1], qui demeurent chaotiques pour toutes les valeurs de leurs paramètres de contrôle comprises dans les intervalles : [0.1, 1] et $\alpha>1$ respectivement.

Cependant les tests de NIST appliqués sur ces récurrences ont montré certaines failles de ces séquences.

A ce propos, dans le chapitre suivant un nouveau générateur de nombres pseudo-aléatoires sera développé, crée à base d'une combinaison des deux récurrences précédentes Bernoulli et Skew-Tent ce qui permet d'avoir un générateur plus efficace avec un aspect parfaitement aléatoire.

Chapitre 4

Implémentation d’un générateur de nombres pseudo-aléatoires chaotique sur FPGA

I. Introduction

Les générateurs de nombres pseudo-aléatoires chaotiques ont attiré beaucoup d'attention dans les divers domaines de recherche, tels que les communications et la physique.

En effet, les systèmes chaotiques génèrent des comportements en apparence aléatoire, mais restent totalement déterministes selon une loi de développement mathématique [18]. Par conséquent, toute proposition visant à utiliser le chaos dans les générateurs de nombre pseudo-aléatoire doit prendre en compte le choix du système chaotique, de l'état initial et des paramètres de contrôles.

Nous avons montré dans le chapitre précédent qu'on ne peut pas exploiter les systèmes chaotiques en tant que générateurs de nombres pseudo-aléatoires directement puisque la plupart ne passer pas les tests statistiques de NIST avec succès.

La solution que nous proposons dans ce chapitre est de combiner plusieurs systèmes chaotiques unidimensionnels pour créer un générateur de nombres pseudo-aléatoires plus robuste. Par ailleurs, une implémentation matérielle sur un circuit reconfigurable FPGA (Field-Programmable GateArrays) est également effectuée afin de valider le générateur chaotique proposé. Plus précisément, nous avons choisi la carte Spartan-XC6LX16 de Xilinx qui représente une famille de composants programmables depuis un programme appelé "bitstream".

II. Description VHDL du générateur proposé

Les FPGAs (Field-Programmable GateArrays) ou réseaux logiques programmables son rôle est de configurer les portes logiques et les relier entre elles selon une logique d'interconnexion ; lesFPGAs sont devenus les plus populaires pour l'implantation des circuits numériques [3].

Cependant, pour réussir à implanter un système sur un composant FPGA de manière efficace, il est indispensable de bien connaître sa structure interne et ses limites du point de vue performance.

En ce qui concerne l'implémentation de notre générateur nous avons affaire à un FPGA Spartan-XC6LX16, qui appartient à la famille Xilinx. Cette gamme de FPGA offre un environnement de conception adapté au prototypage d'applications variées, dont celles des systèmes numériques à usage général et des systèmes embarqués.

II.1. Définition de langage VHDL

VHDL (VHSIC1 Hardware Description Language) est un langage de description de matériel destiné à représenter le comportement ainsi que l'architecture d'un système électronique numérique.

La structure mathématique des systèmes chaotiques sélectionnés pour le générateur de nombres pseudo-aléatoires proposé nous impose l'utilisation de l'approche textuelle basée sur le langage de description matériel VHDL, liée d'avantage aux processus algorithmiques.

L'intérêt d'une telle approche réside dans son caractère exécutable : une spécification décrite en VHDL peut être vérifiée par simulation, avant que la conception détaillée ne soit établie. En outre, les outils de conception assistée par ordinateur (CAO) permettant de passer directement d'une description fonctionnelle en VHDL à un schéma en porte logique ont révolutionné les méthodes de conception des circuits numériques, ASIC ou FPGA.

II.2. Représentation binaire des systèmes chaotiques

Notre générateur de nombres pseudo-aléatoires chaotiques proposé est produit par deux systèmes chaotiques Bernoulli et Skew-Tent ; qui sont des systèmes déterministes apériodiques et sensibles aux conditions initiales.

Ce générateur est produit par un XOR entre les sorties de deux systèmes chaotiques Bernoulli et Skew-Tent, cetopérateur XOR est défini par sa table de vérité :

A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

L'arithmétique à virgule fixe est largement recommandée lors de l'implémentation des systèmes chaotiques sous des composants numériques, afin d'accélérer la vitesse du d'exécution et veiller à la simple réalisation matérielle.

Pour l'implémentation de notre PRNG, nous avons utilisé le navigateur de projet ISE Design Suite.14.5. Cet outil, téléchargeable depuis le site de Xilinx7, constitue un environnement de conception extrêmement efficace, qui regroupe tous les mécanismes nécessaires à l'implémentation d'un circuit numérique, allant de la description comportementale en VHDL jusqu'à la génération du schéma correspondant en portes logiques.

III. Conception du PRNG

En ce qui concerne la conception du générateur proposé, nous avons opté pour une description comportementale sous forme d'instructions séquentielles, afin de mettre en valeur la simplicité de son chemin critique modélisé par l'entité PRNG suite à la synthèse comme présenté dans la figure (IV.1).

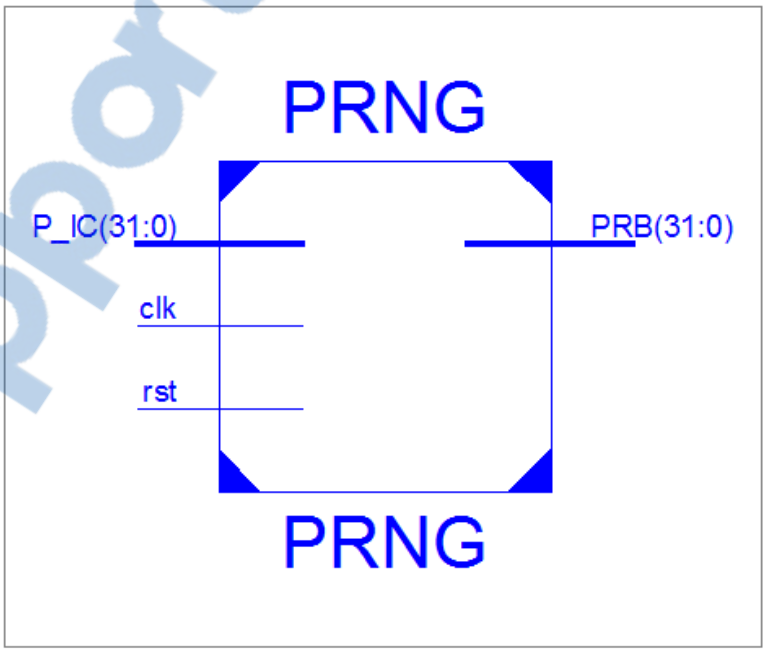

Figure IV. 1: Architecture externe du générateur de nombres pseudo-aléatoires proposé.

L'architecture interne de l'entité « PRNG » englobe deux sous-entités : Bernoulli et Skew-Tent qui correspondent aux systèmes chaotiques employés. Notant que, nous avons considéré une représentation binaire en virgule fixe à 32 bits (2Q30), pour l'implémentation binaire des deux systèmes chaotiques.

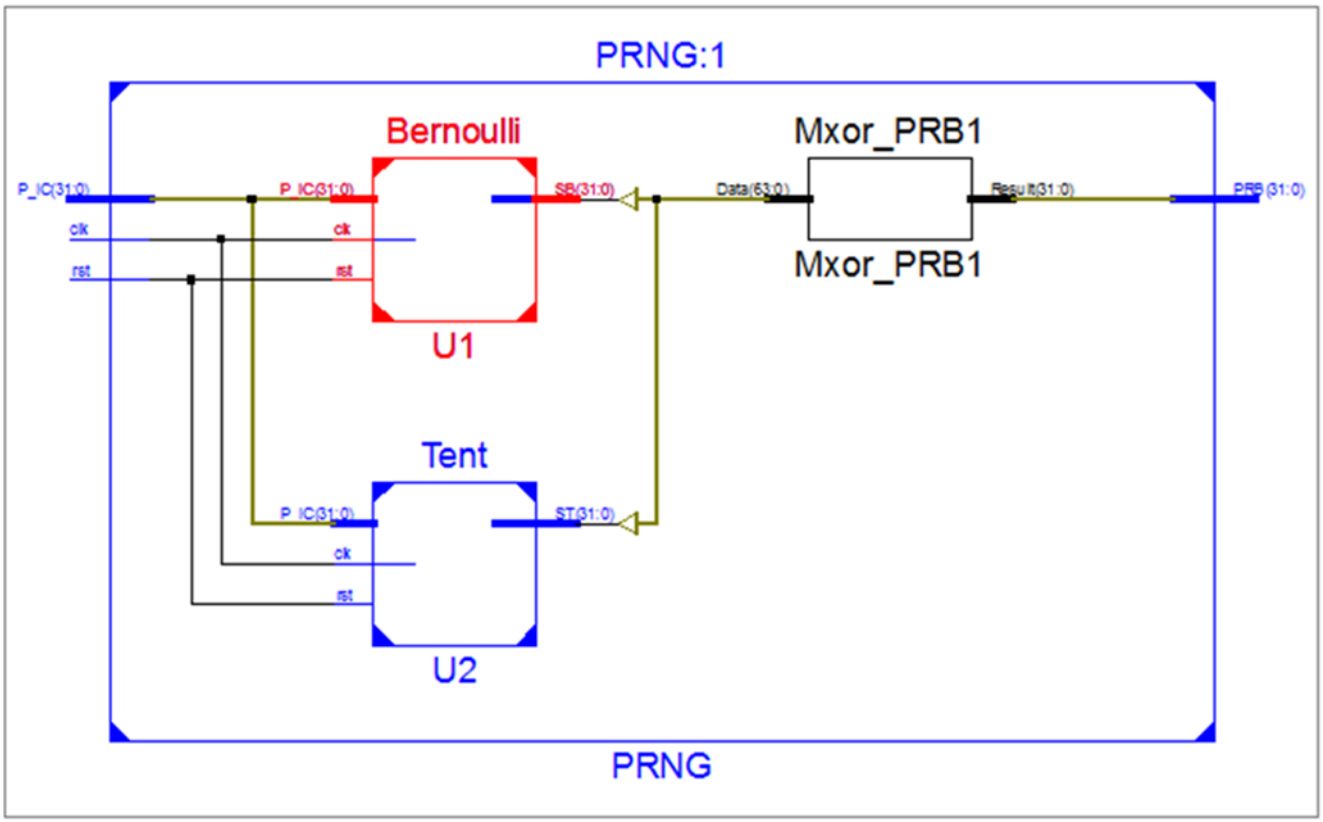

Figure IV. 2: Architecture interne du générateur de nombres pseudo-aléatoires proposé.

Toutes les opérations internes effectuées au sein de l'entité « PRNG » sont soumises aux contrôles des différents signaux d'entrée/sortie décrits dans le tableau 2 :

Nom	Direction	Description
Clk	**Entrée**	**Signal d'horloge du système**
Rst	**Entrée**	**Signal de réinitialisation asynchrone du système.**
P_IC (31 :0)	**Entrée**	**Bus de chargement des Paramètres de contrôle et des conditions initiales**
PRB (31 :0)	**Sortie**	**Flux de bits pseudo-aléatoires, 32 bits**

Tableau 2 : Description des signaux intervenant à l'entité PRNG.

En effet, la description sous forme séquentielle de notre générateur assure une forte connectivité entre les signaux internes et externes intervenant à l'entité « PRNG », sachant que les procédures d'initialisation des systèmes chaotiques et d'extraction des bits pseudo-aléatoires sont opérées au sein d'un même processus. Ce qui permet une gestion efficace des différents états et transitions liés à son fonctionnement. De cette façon, à chaque front montant d'horloge tous les signaux d'états des systèmes chaotiques se voient assignés un état suivant, et par conséquent une nouvelle séquence de bits pseudo-aléatoires de 32 bits est générée suivant la simulation fonctionnelle établie dans la figure (IV.3).

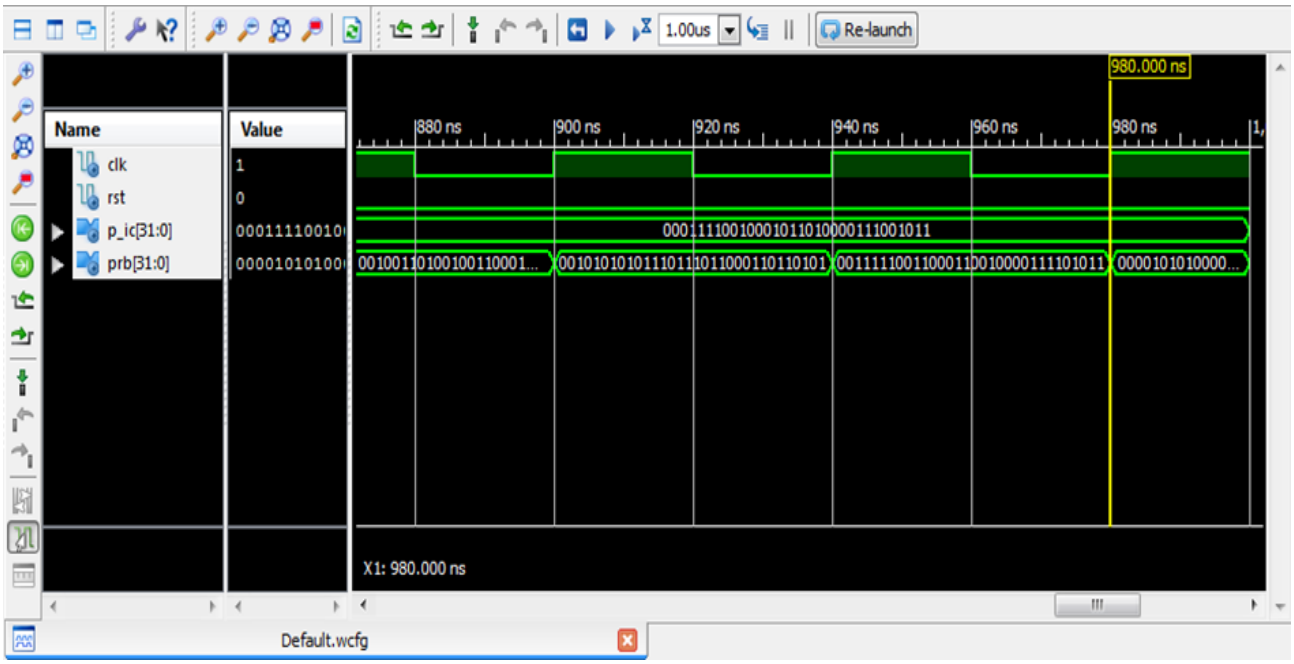

Figure IV. 3: Simulation de l'algorithme PRNG.

IV. Test statistique

La sortie des générateurs de nombre pseudo-aléatoires doit être imprévisible en ignorant l'entrée. D'où la force de tout générateur de nombres pseudo-aléatoires est basée sur une qualité indéniable de ses sorties.

A ce sujet, nous avons utilisé les tests standards NIST SP 800-22 pour évaluer les propriétés statistiques de notre générateur de nombres pseudo-aléatoires l'ensemble des tests a été appliqué sur 50 séquences pseudo-aléatoires de taille 10^6 bits, générées à partir des conditions initiales et des paramètres aléatoires.

Les résultats présentés dans le tableau 3 dessous indiquent que les séquences produites par le générateur de nombres pseudo-aléatoires proposé passent tous les tests statistiques avec succès (toutes les proportions des tests dépassent le niveau de confiance= 98 %) ; ainsi on remarque que le P-valeur>0 qui indique que l'aspect est parfaitement aléatoire.

Ce qui signifie que le générateur de nombres pseudo-aléatoires proposé produit des séquences indistinguables de vraies séquences aléatoires.

Tests statistiques	P_Valeur	Taux de succès(%)
Frequency	**0.534146**	**100**
Block frequency	**0.739918**	**100**
Cumulative sumsforward	**0.534146**	**100**
Cumulative sums reverse	**0.739918**	**100**
Runs	**0.350485**	**98**
Longes runs	**0.911413**	**100**
Rank	**0.739918**	**100**
FFT	**0.534146**	**100**
Nonover lapping Template	**0.66882**	**100**
Over lapping Template	**0.534146**	**100**
Universel	**0.350485**	**100**
Approximateentropy	**0.534146**	**100**
Random excursions	**0.927083**	**100**
Random excursions variant	**0.494392**	**100**
Serial P_value1	**0.534146**	**100**
Serial P_value2	**0.122325**	**98**
Linearcomplexity	**0.739918**	**100**

Tableau 3 : Résultats des tests statistiques de NIST SP800-22.

V. Evaluation de performances

L'efficacité d'un PRNG réside sur la qualité de ce dernier, pour cela un bon PRNG nécessite les critères suivants [16] :

- ✓ Bonnes propriétés statistiques et d'uniformité : les séquences de nombres obtenu doivent passer avec sucées la plupart des tests statistiques raisonnables ;

- ✓ Longue période : supposons que l'on ait besoin de N valeurs aléatoires pour une simulation, alors il faut que la période des valeurs produites soit beaucoup plus grande que N.
- ✓ Efficacité : le temps de calcul nécessaire afin de produire les valeurs doit être le plus petit possible par rapport au temps de la simulation.
- ✓ Répétition : l'utilisateur doit être capable de reproduire la même séquence de nombres facilement.
- ✓ Facilité d'implantation et séparabilité : le générateur doit pouvoir être exécuté sur tous les types d'ordinateurs standards [18].

Le Tableau ci-dessous récapitule les ressources hardwares occupées par le générateur de nombres pseudo-aléatoires proposé. Cette occupation réduite de ressources s'explique par le choix judicieux des systèmes chaotiques ainsi que la simplicité du chemin critique denotre générateur de nombres pseudo-aléatoires.

Device Utilization Summary (estimated values)			[-]
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice Registers	122	18224	0%
Number of Slice LUTs	5022	9112	55%
Number of fully used LUT-FF pairs	88	5056	1%
Number of bonded IOBs	33	232	14%
Number of BUFG/BUFGCTRL/BUFHCEs	1	16	6%
Number of DSP48A1s	4	32	12%

Figure IV. 4 : Taux d'occupation en ressources de l'algorithme de générateur de nombres pseudo-aléatoires proposé pour le FPGA ciblé (Spartan- XC6LX16).

Par ailleurs, le débit de notre générateur de nombres pseudo-aléatoires peut être estimé suivant ()

$$Débit = N \times fréquence\ d'horloge$$

Pour N= 32 bits, le débit atteint = 193 bps pour une fréquence d'horloge = 6.041 MHz. Ce débit est largement suffisant pour répondre aux besoins des transmissions sécurisées. En outre, il y a toujours la possibilité d'améliorer la vitesse de génération des bits pseudo-aléatoires jusqu'à l'ordre de quelques Gbps, en augmentant le nombre de bits extraits à chaque cycle d'horloge.

VI. Génération du fichier de configuration

La mise en œuvre de générateur de nombre pseudo-aléatoire s'achève par l'étape « générateurprogramming file » qui produit un fichier binaire pour la configuration physique du FPGA ciblé dans son état par défaut. Il devient ainsi possible de lancer une interface de reconfiguration à travers l'outil Adept, en permettant au FPGA de s'auto-reconfigurer de manière totalement autonome, à partir du fichier binaire généré.

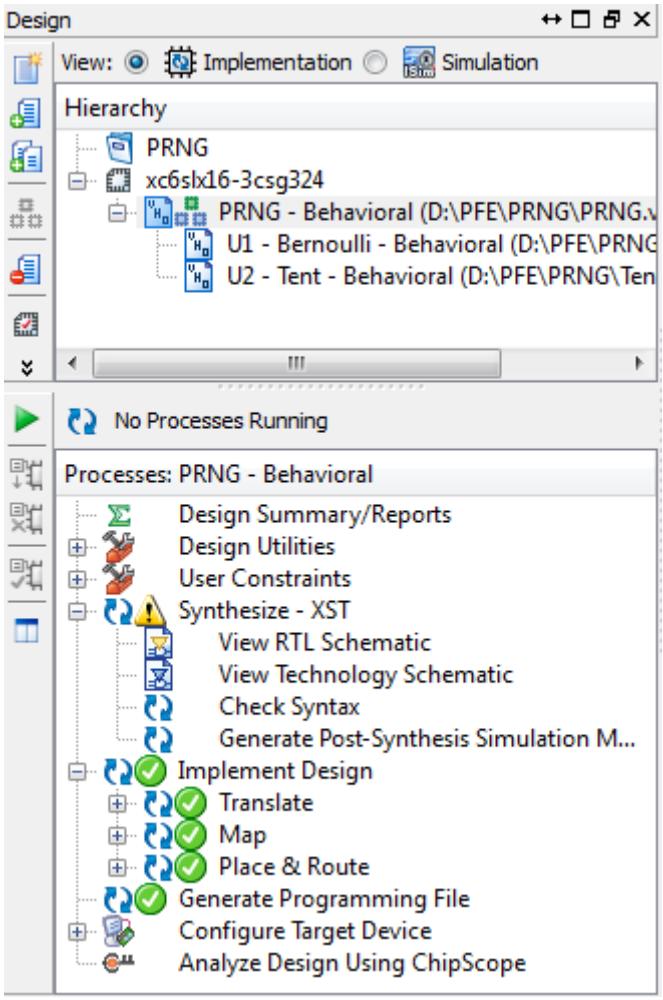

Figure IV.5 : Génération du fichier binaire de configuration.

VII. Conclusion :

Dans ce chapitre le but principal était de créer un générateur chaotique parfaitement aléatoire pour cela nous avons combiné deux systèmes chaotiques unidimensionnels Bernoulli et Skew-Tent que nous avons choisi en raison de leurs bonnes performances.

La conception a était établie en utilisant le langage VHDL et la qualité de sa séquence de sortie a été aussi testée par le test de NIST.

De là ce générateur intégré des récurrences Bernoulli et Skew-Tent crée donne des meilleures propriétés et un niveau élevé de l'aléatoire qui on Peut être utilisée dans les transmissions sécurisées.

Conclusion générale

Dans ce mémoire nous avons abordé l'exploitation des systèmes chaotiques aux transmissions sécurisées ; qui malgré les nombreuses études et les avancées marquées dans ce domaine soulèvent encore de nombreux défis.

Nous avons essayé à travers les recherches effectuées d'apporter des solutions pour l'exploitation de ces systèmes chaotiques aux transmissions sécurisées dans les chapitres de ce document, à savoir celles dues à la représentation binaire des signaux chaotiques et leurs implémentations matérielles.

A ce niveau notre travail a été débuté par une description du phénomène chaotique qui repose sur un comportement aléatoire, déterministe et sensible aux conditions initiales , Il existe plusieurs types d'évolution possibles d'un système dynamique régulier vers le chaos à partir d'un scénario de transition. Aussi nous avons parlé de différents domaines d'applications du chaos.

Dans le deuxième chapitre nous avons exposé les principales méthodes des transmissions sécurisées basé sur le chaos que ce soit analogique ou numérique ; ainsi leurs avantages et inconvénients .de là nous avons conclu qu'aucun standard de transmission par chaos n'a émergé jusqu'à présent, car les études de faisabilité et de robustesse des algorithmes développés remettent en cause leur niveau de sécurité qui est souvent indéterminé.

Par la suite dans le troisième chapitre, nous avons étudié la génération de nombre pseudo-aléatoire ; qui sont utilisées dans les transmissions basées sur le chaos. A ce propos, nous avons étudié les performances de deux systèmes chaotiques unidimensionnels Bernoulli et SkewTent, ces derniers sont les meilleurs mais ne peuvent pas passer le test de NIST avec succès ; les séquences de ces systèmes ne sont pas parfaitement aléatoires, donc on ne peut pas les utilisées directement comme générateur de nombres pseudo-aléatoires.

Pour résoudre ce problème nous avons traité dans le dernier chapitre une solution consiste à combiner la récurrence Bernoulli et la récurrence Skew-Tentpour créer un nouveau générateur de nombres pseudo-aléatoires et son implémentation sur une carte FPGA de type Spartan- XC6LX16. Nous avons passé par la suite au test de NIST ; le générateur de nombres pseudo-aléatoires proposé passent tous les tests statistiques avec succès de là on confirme l'aléatoire de notre générateur .Cette étude nous a prouvé que la combinaison des systèmes

chaotiques choisis peut être utilisée comme un générateur de nombre pseudo-aléatoire dans les transmissions sécurisées.

Annexe

Les tests du NIST (National Institute of Standards and Technology) forment un paquetage statistique de tests qui sont conçus pour détecter l'aspect aléatoire des séquences binaires à lasortie des générateurs de nombres aléatoires ou pseudo-aléatoires.

Le résultat de chaque test est donné par une P-Value qui représente la probabilité qu'ungénérateur de nombre aléatoire parfait produise une séquence moins aléatoire que la séquencedéjà testée.

- ✓ P-Value = 1 : aspect aléatoire parfait.
- ✓ P-Value = 0 : aspect non aléatoire.

On présente par la suite les 15 tests du NIST.

➢ Propriétés d'une séquence aléatoire testée

Les hypothèses suivantes ont été mises en œuvre en ce qui concerne la séquence binaire aléatoire à tester :

1- Uniformité : L'occurrence de 0 ou de 1 est probablement égale,

2- Extensibilité : Tout test applicable à une séquence peut être aussi appliqué à une sous-séquence extraite aléatoirement. Si une séquence est aléatoire, alors toute sous-séquence extraite doit être aléatoire. Ainsi, toute sous-séquence doit passer tout test de l'aspect aléatoire.

3- Cohérence : Le comportement d'un générateur doit être constant à travers les valeurs initiales (seeds). Il est inadéquat de tester un PRNG basé sur une sortie d'un seul seed, ou un RNG basé sur une sortie produite d'une seule sortie physique.

➢ Test de fréquence

Le but de ce test est de déterminer si le nombre de 0 et de 1 dans une séquence est Approximativement le même comme il est prévu pour une séquence réellement aléatoire.

➢ Test de fréquence par bloc

Le but de ce test est de déterminer si la fréquence des 1 dans un bloc de M bits est Approximativement 1/2. Pour un bloc de taille M = 1, on revient au test de fréquence.

- **Test de somme cumulative (inverse)**

  Le but de ce test est de déterminer si la somme cumulative dans une séquence est trop grandeou trop petite (somme de 1 et -1). Ceci indique la présence de nombre important de 0 ou de 1.

- **Test de série**

  Le « Runs Test » permet de déceler des oscillations entre les 0 et les 1 trop rapides ou troplentes.

- **Test de longues séries de 1**

  Ce test consiste à déterminer si la distribution de longues séries de 1 est conforme avec lesprobabilités théoriques.

- **Test de rang**

  Calculer le rang des sous matrices de la séquence et vérifier leur dépendance linéaire**.**

- **Test de Non overlapping template Matching**

  Ce test consiste à détecter des générateurs qui produisent trop d'occurrence d'un mot apériodique donné (Template).

  Une fenêtre de m-bits est utilisée. Si le mot n'est pas trouvé, la fenêtre est décalée d'un bit. Sile mot est trouvé, la fenêtre décale jusqu'au bit qui suit le mot trouvé.

- **Test de overlapping template Matching**

  Le but de ce test est identique à celui du 8ème test, calculer le nombre d'occurrences de B dans chacun des N blocs. On crée une fenêtre de m bits qui traverse la séquence en comparant les bits de la fenêtre avec B. Un compteur s'incrémente quand il y a une égalité.

- **Test statistiqueuniversel**

  Le but de ce test est de déterminer si la séquence est compressible ou non sans perted'information. Une séquence nettement compressible est considérée comme non aléatoire

- **Test d'entropieapproximative**

  On s'intéresse aux fréquences d'occurrences de toutes les sous-séquences possibles de Longueur m fixée. Nous allons comparer les fréquences obtenues avec les longueurs m etm+1. L'entropie mesure le degré de désordre d'un système.

  Pour une séquence de bits donnée, il faut ajouter les m-1 bits de la fin de la séquence à sondébut.

- **Test Random excursion**

  Un cycle d'une marche aléatoire (excursion) est une séquence de pas aléatoires qui commenceet finit à son origine.

- **Test Random excursion variant**

  Le but de ce test est de calculer le nombre de fois où un état particulier est visité, et de détecter la déviation par rapport au nombre de visites attendu à différents états de la marchealéatoire.

- **Serial Test**

  Ce test est basé sur la fréquence de tous les m-bits de chevauchement tout au long de laséquence. Le but de ce test est de déterminer si le nombre d'occurrences des 2^m des modèlesde chevauchement des m bits est identique à celui d'une séquence aléatoire (m est le nombrede bits dans chaque bloc**).**

- **Test Linearcomplexity**

  Ce test est basé sur la longueur d'un registre à décalage à rétroaction linéaire. Le but de ce testest de déterminer si la séquence est assez complexe pour être considérée comme aléatoire**.**

Bibliographie

[1] : MEGHERBI Ouerdia. Etude et réalisation d'un système sécurisé à base de système chaotique. Mémoire de magister, UNIVERSITE MOULOUD HAMMERI, TIZI-OUZOU, 2013.

[2] **:** Kihal Ahmed Ridha. Systèmes chaotiques pour la transmission sécurisée de données. Université Mohamed Khider – Biskra, 2013.

[3] : ABDERRAHIM NassibaWafa. Étude et conception d'un modèle chaotique dédié aux transmissions chiffrées, thèse de doctorat, UNIVERSITE ABOU-BEKR BELKAID, 2015.

[4] : Kassem Ahmad. Protocoles, gestion et transmission sécurisée par chaos des clés secrètes. Applications aux standards : TCP/IP via DVB-S, UMTS, EPS. Electronique. Thèse de doctorat, UNIVERSITE DE NANTES ; UNIVERSITE LIBANAISE, 2013.

[5] : Georges KADDOUM. Contributions à l'amélioration des systèmes de communication multiutilisateurs par chaos : synchronisation et analyse des performances. Thèse de doctorat, UNIVERSITÉ DE TOULOUSE, 2008.

[6] : TayebHamaizia. Systèmes Dynamiques et Chaos « Application à l'optimisation à l'aide d'algorithme chaotique ». Thèse de doctorat, UNIVERSITE CONSTANTINE– 1, 2013.

[7] : Zaraoulia ELHADJ. Etude de quelques types de systèmes chaotiques : généralisation d'un modèle issu du modèle de Chen. Thèse de doctorat, UNIVERSITE MENTOURI CONSTANTINE, 2006.

[8] : Hamid HAMICHE. Inversion à gauche des systèmes dynamiques hybrides chaotiques « Application à la transmission sécurisée de données, Thèse de doctorat », UNIVERSITE MOULOUD HAMMERI, TIZI-OUZOU, 2011.

[9] : Brahim AKBIL. Optimisation des performances des techniques d'accès multiple par l'initialisation des systèmes chaotiques et par regroupement des utilisateurs. Thèse de doctorat, UNIVERSITE MOHAMMED V, 2016.

[10] : KOUADRI Mostefai. Tests de validation pour les crypto-systèmes chaotiques. Magister, UNIVERSITE MOHAMED BOUDIAF, ORAN, 2013.

[11] : ANSTETT Floriane. Les systèmes dynamiques chaotiques pour le chiffrement : synthèse et cryptanalyse. Thèse de doctorat, UNIVERSITE HENRI POINCARE, 2006.

[12] : Hassan Noura. Conception et simulation des générateurs, crypto-systèmes et fonctions de hachage basés chaos performants. Electronique. UNIVERSITE DE NANTES, 2012.

[13] : GhadaZaibi. Sécurisation par dynamiques chaotiques des réseaux locaux sans fil au niveau de la couche MAC. Autre [cs.OH]. UNIVERSITE TOULOUSE le Mirail - Toulouse II, 2012.

[14] : TAREK OULD BACHIR. Génération de nombres pseudo-aléatoires suivant une distribution non-uniforme par circuits intégrés, UNIVERSITÉ DE MONTRÉAL, 2008.

[15]:Mickael Francois, David Defour. A Pseudo-Random Bit Generator Using Three Chaotic Logistic Maps. [Research Report] LIRMM. 2013.

[16]: FRANCOIS Michael. AFastChaos-BasedPseudo-RandomBitGeneratorUsingBinary64 Floating-Point Arithmetic. Thèse de doctorat, UNIVERSITÉ PERPIGNAN VIA DOMITIA ,2013.

[17] : Christophe Guyeux, Qianxue Wang, Jacques Bahi. A Pseudo Random Numbers Generator Based on Chaotic Iterations. Application to Watermarking. WISM 2010, Int. Conf. on Web Information Systems and Mining, 2010.

[18] : KRIM Mohamed. Implémentation des générateurs pseudo-aléatoires : Etudes et applications. Thèse de doctorat, UNIVERSITE MOHAMED BOUDIAF, 2010.