REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEURE ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE ABOU-BEKR BELKAID – TLEMCEN

FACULTE DE TECHNOLOGIE

DEPARTEMENT DE TELECOMMUNICATIONS

LABORATOIRE DE TELECOMMUNICATIONS DE TLEMCEN

THÈSE

Présentée pour l'obtention du diplôme de

DOCTORAT

Spécialité : Télécommunications

Par :

ABDERRAHIM Nassiba Wafa

Sur le thème

Étude et conception d'un modèle chaotique dédié aux transmissions chiffrées

Soutenue le 27 Octobre 2015 devant le jury composé de:

Mr CHIKH Mohammed Amine	Pr, Université de Tlemcen	Président
Mr DJEMAI Mohamed	Pr, Université de Valenciennes	Examinateur
Mr LASRI Boumediène	Pr, Université de Saïda	Examinateur
Mr TALEB Nasreddine	Pr, Université de Sidi bel Abbes	Examinateur
Mme CHOUKCHOU-BRAHAM Amal	MCA, Université de Tlemcen	Examinatrice
Mr SEDDIKI Omar	Pr, Université de Tlemcen	Directeur de Thèse
Mme BENMANSOUR F. Zohra	MCB, Université de Tlemcen	Membre invité

Remerciements

Grâce à la volonté d'Allah le tout puissant et bienveillant que ce travail s'est accompli.

Je tiens tout d'abord à exprimer mes sincères remerciements à Mme BENMANSOUR F. Z, maître de conférences à l'université de Tlemcen, pour m'avoir fait découvrir la relation passionnante entre le chaos et la cryptographie, et pour m'avoir soutenue jusqu'au bout. Par sa compétence, ses conseils avisés, ses critiques et sa gentillesse touchante, elle a joué un rôle déterminant dans le développement de mes recherches. Ces quelques mots ne suffisent pas pour lui exprimer toute ma gratitude.

J'adresse toute ma reconnaissance à mon directeur de thèse le Professeur SEDDIKI Omar, pour m'avoir proposé ce sujet de thèse et pour son encadrement. La confiance que vous m'avez accordée, votre sympathie et vos conseils tout au long de ces années, m'ont permis de mener ce travail dans les meilleures conditions.

Je remercie profondément Mr. CHIKH. M. A, Professeur à l'université de Tlemcen, pour m'avoir fait l'honneur de présider le jury de cette thèse.

Mes remerciements s'adressent également aux membres du jury : Mr DJEMAI. M, Professeur à l'université de Valenciennes, Mr LASRI. B, Professeur à l'université de Saïda, Mr TALEB. N, Professeur à l'université de Sidi bel Abbes et Mme CHOUKCHOU-BRAHAM. A, maître de conférences à l'université de Tlemcen, qui ont bien voulu examiner mes travaux en me faisant l'honneur de participer au jury.

Ce travail de thèse s'est déroulé au sein du laboratoire de télécommunications de Tlemcen. Je tiens alors à remercier son directeur, Mr MERIAH. S. M, pour m'y avoir accueillie. Je remercie de même tous les membres du laboratoire, qui ont rendu ces années de thèse très agréables par leur amitié, leur soutien moral et leurs encouragements.

Un remerciement tout particulier à Mme BABA-AHMED. A, pour son aide précieuse et sa gentillesse. J'ai énormément bénéficié de ses conseils en matière de développement des circuits numériques sur les composants FPGA.

Mes dernières pensées se tournent vers ma famille, mon frère, mes sœurs et surtout mes chers parents. Je leur dois en grande partie l'aboutissement de ce travail.

Résumé

Le sujet de recherche abordé dans cette thèse porte sur l'application des systèmes chaotiques aux transmissions sécurisées. Plus particulièrement, nous nous sommes intéressés à une exploitation originale des systèmes chaotiques unidimensionnels les plus performants en tant que générateur de nombres pseudo-aléatoires, destiné au chiffrement par flux.

L'étude menée dans ce contexte s'est centrée autour des aspects communs entre les systèmes chaotiques et la cryptographie symétrique. En premier lieu, nous avons mis en évidence les fortes similitudes entre la description des systèmes chaotiques en dynamique symbolique et le chiffrement par flux conventionnel, dont nous avons souligné le potentiel de l'approche par dynamique symbolique pour résoudre le problème de synchronisation entre l'émetteur et le récepteur dans les transmissions chiffrées par chaos numérique.

Puis, nous avons exploité nos constatations dans la proposition d'un nouveau générateur de nombres pseudo-aléatoires, basé sur l'intégration de deux systèmes chaotiques discrets, adapté au chiffrement par flux synchrone. L'algorithme ainsi développé conserve davantage les propriétés naturelles des systèmes chaotiques utilisés, sans perte de robustesse liée à leur implémentation.

Finalement, nous avons discuté la conception de l'algorithme de chiffrement proposé sur un composant FPGA. Une évaluation des performances et une comparaison avec les principaux standards de chiffrement par flux sont également effectuées, afin de bien situer l'originalité des contributions apportées.

Mots clés: cryptographie, chiffrement symétrique, chaos, synchronisation, système dynamique.

Abstract

The research topic addressed in this thesis concern the application of chaotic systems in secure transmissions. We are particularly interested in an original exploitation of the most performance one-dimensional chaotic systems as a pseudo-random numbers generator, destined to stream cipher.

The study conducted in this context is centered around common aspects between chaotic systems and symmetric cryptography. First and foremost, we have highlighted the strong similarities between the description of chaotic systems using symbolic dynamics and conventional stream ciphers, where we have pointed the potential of the symbolic dynamics approach to resolve the synchronization problem between transmitter and receiver in secure transmissions by digital chaos.

Then, we have exploited our ascertainments in the proposition of a new pseudo-random numbers generator, based on the integration of two discrete chaotic systems, adapted to synchronous stream cipher. The developed algorithm retains more the natural characteristics of the chaotic systems used, without loss of robustness related to their implementation.

Finally, we have addressed the conception of the proposed stream cipher on an FPGA device. Performances evaluation and comparison with the main stream cipher standards are also performed in order to point out the originality of the provided contributions.

Keywords : Cryptography, stream cipher, chaos, synchronization, dynamic system.

ملخص

يتناول موضوع هذه الأطروحة تطبيق أنظمة الفوضى في مجال تأمين الاتصالات. إذ ركزنا اهتمامنا بشكل خاص على الاستغلال الفريد من نوعه لأنظمة الفوضى أحادية البعد الأكثر كفاءة كمولد أعداد شبه عشوائية، موجه للتشفير المتصل.

اعتمدت الدراسة التي أجريت في هذا السياق حول الجوانب المشتركة بين أنظمة الفوضى و الكريبتوغرافيا المتناظرة. تطرقنا أولا لإبراز أوجه التشابه القوية بين تمثيل أنظمة الفوضى بواسطة الديناميات رمزية و التشفير المتصل التقليدي، حيث سلطنا الضوء على إمكانات نهج الديناميات الرمزية في حل مشكلة التزامن بين المرسل و المتلقي في تأمين الاتصالات بالفوضى الرقمية.

ثم قمنا باستغلال النتائج التي توصلنا إليها في اقتراح مولد أعداد شبه عشوائية جديد، يعتمد على دمج نظامي فوضى، ملائم للتشفير المتصل. الخوارزمية المقترحة تحتفظ بكافة الخصائص الطبيعية لأنظمة الفوضى المستخدمة، دون فقدان ميزاتها جرّاء تنفيذها.

أخيرا، ناقشنا تنفيذ الخوارزمية المقترحة على جهاز FPGA (شبكة أبواب قابلة للبرمجة). تقييم للأداء ومقارنة مع أهم خوارزميات التشفير المتصل تمّ أيضا إجراءهم بهدف توضيح مكانة المساهمات المقدمة.

الكلمات المفتاحية : كريبتوغرافيا ، تشفير المتناظر، الفوضى، تزامن، نظام الديناميكي.

Table des matières

Table des figures

Liste des tableaux

Liste des acronymes et abréviations

AES	:	Advanced Encryption Standard
BPSK	:	Binary Phase Shift Keying
CAO	:	Conception Assistée par Ordinateur
CBC	:	Cipher Bloc Chaining
CFB	:	Cipher FeedBack
CSK	:	Chaos Shift Keying
CVES	:	Chaotic Video Encryption Scheme
DES	:	Data Encryption Standard
DSP	:	Digital Signal Processor
ECB	:	Electronic Code Book
FPGA	:	Field-Programmable Gate Array
HDL	:	Hardware Description Langage
HQS	:	Habitat Qualité Service
ISE	:	Integrated Synthesis Environment
IV	:	Initialization Vector
JTAG	:	Joint Test Action Group
LCG	:	Linear Congruential genrator
LFSR	:	Linear-Feedback Shift Register
LUT	:	Look Up table
NIST	:	National Institute of Standards and Technology
OCCULT	:	Optical Chaos Communications Using Laser-Diodes Transmitters
OFB	:	Output FeedBack
PLL	:	Phase-Locked Loop
PRNG	:	Pseudo-Random Numbers Generator
RAM	:	Random Access Memory
RC4	:	Rivest Cipher 4
RSA	:	Rivest, Shamir, Adleman
RTL	:	Register Transfer Level

SDM	:	Symbolic Dynamic based Method
SNR	:	Signal to Noise Ratio
SPN	:	Substitution-Permutation Network
TEB	:	Taux d'Erreurs Binaires
VHDL	:	VHSIC Hardware Description Language
VHSIC	:	Very High Speed Integrated Circuits

Chapitre 1 : Introduction générale

I. Contexte et motivation

Les technologies de communication ont subi un développement remarquable ces dernières années au niveau des infrastructures et des services offerts aux utilisateurs, tels que les communications sans fil, la vidéo à la demande, la télévision à haute définition et la fourniture de contenu multimédia en général. La mise en place de telles technologies impose certaines exigences liées à leur protection contre les exploitations malveillantes visant à manipuler ou communiquer des informations sensibles. D'où, le déploiement des mécanismes de sécurité est devenu indispensable pour protéger l'échange d'informations à travers les canaux publics. Les protocoles de sécurité conçus à cette fin reposent typiquement sur plusieurs primitives cryptographiques, y compris les algorithmes de chiffrement destinés à préserver la confidentialité. En d'autres termes, rendre le contenu d'une communication ou d'un fichier inaccessible aux personnes non autorisées, celles qui ne disposent pas de la clé de déchiffrement valide.

On distingue classiquement deux types d'algorithmes de chiffrement : symétriques et asymétriques. Les algorithmes de chiffrement symétriques utilisent la même clé partagée secrètement pour procéder au chiffrement et au déchiffrement, comme l'algorithme DES (Data Encryption Standard) et ses variantes : Triple-DES et l'AES (Advanced Encryption Standard). Quant aux algorithmes asymétriques utilisent deux clés différentes. Une publique employée pour le chiffrement et une autre privée pour le déchiffrement, comme l'algorithme RSA nommé selon les initiales de ses inventeurs : Rivest, Shamir et Adleman.

En effet, les deux types d'algorithmes de chiffrement ont chacun leurs avantages et leurs inconvénients, ainsi que leurs applications privilégiées. Néanmoins, ils sont souvent utilisés en association au sein des protocoles de sécurité afin de combiner leurs propriétés. D'un côté, les algorithmes de chiffrement asymétriques sont plus adaptés au chiffrement des messages de petite taille. Ils sont couramment employés pour le partage des clés de session, qui doivent

être échangées fréquemment pour éviter les failles de sécurité. Ils servent également à la signature numérique et à l'authentification. D'un autre côté, les algorithmes de chiffrement symétriques sont plus souhaitables au chiffrement de quantités importantes de données, car ils réalisent un excellent compromis entre l'efficacité et la sécurité par le biais de clés secrètes assez courtes (128/256 bits). De plus, les algorithmes de chiffrement symétriques s'adaptent aux différents types de données, en procédant selon deux modes de chiffrement : par bloc et par flux.

En dépit de leur capacité de sécurisation, les algorithmes de chiffrement existants exigent souvent une mise en œuvre logicielle, telle que leur application à certains types de transmissions ne soit pas envisageable. D'autre part, la plupart des algorithmes de chiffrement standardisés, en particulier les algorithmes de chiffrement par flux, se sont avérés irrésistibles contre les attaques académiques, qui sont de plus en plus optimisées pour fonctionner avec une complexité inférieure à la sécurité calculatoire, censée être garantie par la taille de la clé secrète. Pour ces raisons, plusieurs chercheurs tentent à présent de mettre au point de nouvelles alternatives de chiffrement, en exploitant les systèmes non-linéaires en régime chaotique, qui suscitent beaucoup d'attention auprès des cryptographes en raison de leurs caractéristiques attractives.

En effet, l'exploitation de la dépendance sensible des systèmes chaotiques aux conditions initiales et l'ergodicité de leur évolution temporelle dans le cadre de chiffrement ont permis l'émergence d'une nouvelle génération de transmissions chiffrées, qui s'inscrit dans le cadre de la cryptographie symétrique. Cette branche, communément appelée cryptographie chaotique, englobe deux modes de chiffrement, à savoir le chiffrement par chaos analogique et le chiffrement par chaos numérique.

Cependant, malgré la diversité des cryptosystèmes chaotiques proposés dans la littérature, qui varient entre des algorithmes de chiffrement par bloc et par flux, aucun standard de chiffrement par chaos n'a émergé jusqu'à présent, car les études de faisabilité et de robustesse des algorithmes développés remettent en cause leur niveau sécurité qui est souvent indéterminé. Par ailleurs, la plupart d'entre eux présentent des inconvénients communs et partagent les mêmes difficultés de réalisation. Il s'agit d'une part, de la dégradation des propriétés des systèmes chaotiques induite par leur mise en œuvre sur des composants numériques, et d'autre part, les problèmes liés à la synchronisation des systèmes chaotiques, la définition et le partage des clés secrètes sur lesquelles repose entièrement la sécurité de la cryptographie symétrique.

La conception des cryptosystèmes chaotiques exige en fait une connaissance approfondie non seulement des fondements de la cryptographie, mais aussi des comportements dynamiques et la nature des systèmes permettant de générer le chaos, et les éventuels problèmes liés à leur manipulation. Il s'agit donc des mécanismes originaux qui doivent être soigneusement pris en compte, afin de remplir les critères de sécurité et de robustesse imposés par la cryptographie moderne.

II. Contributions

De nombreuses techniques ont été proposées pour masquer des signaux analogiques et numériques en utilisant les propriétés des systèmes chaotiques, à savoir les transmissions sécurisées par synchronisation des systèmes chaotiques et les cryptosystèmes numériques. Ces techniques apportent certaines originalités par rapport aux standards de chiffrement conventionnel, et soulèvent en contrepartie de nombreux défis. Cependant, en comparant les deux modes de chiffrement par chaos on trouve que les cryposystèmes numériques sont plus convaincants du point de vue de sécurité et par conséquent plus adaptés aux utilisations pratiques. Notant que l'exploitation des systèmes chaotiques dans le chiffrement par flux, en tant que générateurs de nombres pseudo-aléatoires, est plus bénéfique par rapport aux standards adoptés actuellement, notamment pour remplacer les registres à décalage qui jouent un rôle dominant dans le chiffrement par flux conventionnel.

L'objectif du travail que nous présentons dans cette thèse est d'étudier l'application des systèmes chaotiques aux transmissions chiffrées, tout en tenant compte des problématiques précitées, afin d'apporter une contribution prometteuse au chiffrement par flux qui connait un manque de standards.

Compte tenu que la majorité des cryptosystèmes chaotiques proposés dans la littérature considère les conditions initiales des systèmes chaotiques employés comme une partie de la clé secrète pour éliminer le problème de synchronisation entre l'émetteur et le récepteur, alors nous avons considéré dans notre étude une approche par dynamique symbolique pour assurer un partage efficace de la condition initiale. Une première partie de ce travail s'est concentrée donc sur la mise en évidence du lien entre la synchronisation des systèmes chaotiques à base de la dynamique symbolique et le chiffrement par flux conventionnel, dont nous avons montré que la dynamique symbolique peut tout aussi bien s'appliquer à la génération de nombres pseudo-aléatoires dédiés au chiffrement par flux. La principale motivation dans cette

contribution provient du fait que la description des systèmes chaotiques au moyen de la dynamique symbolique a été peu abordée dans la littérature.

D'autre part, il est toujours difficile d'établir un compromis entre la sécurité et l'efficacité dans les algorithmes de chiffrement par flux, à cause de leur mode de fonctionnement exigeant des structures simples. Pour cela nous nous sommes orientés vers l'exploitation des systèmes chaotiques unidimensionnels dans la conception d'un nouvel algorithme de chiffrement par flux adapté aux transmissions temps réel. Une étude de tous les aspects liés à la conception des cryptosystèmes chaotiques, y inclus le choix approprié des systèmes chaotiques et la conservation de leurs propriétés suite à la binarisation, le développement des procédures de chiffrement/ déchiffrement robustes et rapides, et l'efficacité de leur implémentation au niveau hardware, a été considérée afin d'atteindre les propriétés de confusion et de diffusion souhaitables pour tout générateur de nombres pseudo-aléatoires destiné à être utilisé dans le chiffrement par flux.

En vue d'approuver expérimentalement la validité de l'algorithme proposé, une seconde partie a été consacrée à l'étude de son implémentation matérielle sur un composant FPGA de type Spartan-XC6LX16 de Xilinx. Les résultats obtenus confirment l'intérêt de l'algorithme mis en place au chiffrement par flux.

III. Organisation de la thèse

Le contenu de cette thèse s'organise autour de cinq chapitres qui traitent d'une part l'intérêt des propriétés naturelles des systèmes chaotiques aux transmissions chiffrées, et d'autre part les mécanismes nécessaires pour pallier aux différents problèmes liés à la représentation binaire des systèmes chaotiques et leur implémentation pratique.

Le premier chapitre est destiné à introduire le contexte général du travail présenté dans cette thèse et les contributions apportées au chiffrement par chaos, après avoir cerné les principales problématiques rencontrées dans ce domaine;

Le second chapitre dresse un état de l'art des travaux portant sur les transmissions chiffrées par chaos, que ce soit en mode analogique ou numérique. Une synthèse résumant les points forts et faibles de chacun des modes est présentée dans l'optique de mieux mettre en évidence l'originalité des contributions que nous proposerons par la suite;

Le troisième chapitre se focalise sur la description en dynamique symbolique des systèmes chaotiques, et la mise en évidence des fortes similitudes entre la synchronisation des systèmes chaotiques au moyen de la dynamique symbolique et le chiffrement par flux conventionnel ;

Le quatrième chapitre est consacré au développement d'un nouvel algorithme de chiffrement par flux, en tirant profit de la description en dynamique symbolique des systèmes chaotiques et leur capacité de synchronisation. À cet effet, une étude comparative entre plusieurs systèmes chaotiques unidimensionnels est présentée en vue d'en sélectionner les plus adaptés à notre algorithme. Enfin, une analyse permettant d'estimer la sécurité du cryptosystème proposé sera détaillée.

Le cinquième chapitre aborde l'implémentation matérielle du cryptosystème proposé sur une cible FPGA, dont nous essayons d'approuver expérimentalement la validité de l'algorithme mis en place;

Une synthèse des différents travaux présentés dans cette thèse est donnée en conclusion générale, suivie par les perspectives envisagées.

IV. Production scientifique

L'ensemble des travaux présentés et les résultats obtenus tout en long de cette thèse ont fait l'objet des communications listées ci-dessous.

4.1. Publication internationale

N. W. Abderrahim, F. Z. Benmansour and O. Seddiki. "***A chaotic stream cipher based on symbolic dynamic description and synchronization***", Nonlinear Dynamics, vol. 78.1, pp. 197-207, 2014.

4.2. Communications internationales

N. W. Abderrahim , F. Z. Benmansour , O. Seddiki, "***A suitable use of chaotic dynamics in stream cipher***", The International Conference on Telecommunications and ICT in Oran (ICTTelecom-2015) ;

Abderrahim, N. W., F. Z. Benmansour, and O. Seddiki. "***Etude des transmissions chiffrées par synchronisation des systèmes chaotiques***", Conférence Internationale sur l'Intelligence Artificielle et les Technologies de l'Information (ICA2IT'14) ;

W.Abderrahim, F.Z.Benmansour et O.Seddiki, "***Cryptage des images médicales basé sur l'intégration des séquences chaotiques uniformes***", Biomedical engineering international conference (BIOMEIC'12), 2012, TLEMCEN (ALGERIA);

Abderrahim Nassiba Wafa, Benmansour F.Zohra et Seddiki Omar, "***Intégration des séquences chaotiques issues des récurrences discrètes dans le chiffrement d'images***", Conférence Internationale sur le Traitement de l'Information Multimédia (CITIM'12).

4.3. Communications nationales

N. W. Abderrahim, F.Z.Benmansour et O.Seddiki, "***Etude des transmissions chiffrées par discrétisation des systèmes chaotique***", JLTT'2014, TLEMCEN ;

N. W. Abderrahim, F.Z.Benmansour et O.Seddiki, " ***Application des systèmes chaotiques au chiffrement par flux***", JLTT'2015, TLEMCEN.

Chapitre2 : Transmissions sécurisées par chaos

I. Introduction

Un intérêt significatif a été accordé à l'usage des systèmes chaotiques aux transmissions sécurisées au cours des dernières décennies, en raison de l'aspect aléatoire de leur comportement et leur hypersensibilité aux variations. Ces caractéristiques ouvrent de larges perspectives applicatives des systèmes chaotiques, en tant que source d'aléa, dans les transmissions chiffrées en mode analogique ou numérique.

Dans ce présent chapitre, nous allons détailler l'intérêt et l'apport d'utilisation des signaux chaotiques aux transmissions chiffrées, tout en mettant le lien entre les propriétés naturelles des systèmes chaotiques et la cryptographie symétrique. À ce propos, nous entamerons le chapitre par une description du principe des transmissions sécurisées par chaos, suivie par un aperçu général des approches de chiffrement par chaos les plus intéressantes, en les regroupant en deux catégories:

- Les techniques de chiffrement par chaos analogique : fondées sur les mécanismes de synchronisation des systèmes chaotiques;
- Les cryptosystèmes chaotiques : inspirés des notions de la cryptographie conventionnelle.

Notre étude porte principalement sur la validité et la robustesse de ces techniques dans le contexte de transmissions chiffrées, qui nécessitent une optimisation du compromis entre la qualité de transmission et le niveau de sécurité.

II. Principe de la transmission chiffrée par chaos

Depuis l'année 1990, plusieurs similitudes entre les propriétés naturelles des systèmes chaotiques et la cryptographie symétrique ont été constatées par la communauté scientifique, notamment les correspondances entre la nature stochastique des signaux chaotiques et les

deux concepts de confusion et de diffusion formalisés par Claude Shannon dans le cadre de la théorie de l'information [1] [2]:

- Les signaux générés par les systèmes chaotiques possèdent des propriétés statistiques proches de celles des signaux complètement aléatoires en dépit d'être déterministes;
- La forte sensibilité des comportements chaotiques aux variations permet la génération d'un nombre infini de signaux chaotiques non corrélés d'un même système, en utilisant différentes valeurs de conditions initiales ou de paramètres de contrôle;
- Le caractère déterministe des signaux chaotiques permet la reproduction à l'identique de leurs comportements complexes en émission/ réception ;

En raison de ces similitudes, de nombreuses techniques ont été proposées pour masquer une information en utilisant les propriétés du chaos. Le procédé général du chiffrement par chaos repose sur deux facteurs essentiels: la dynamique chaotique et la procédure de chiffrement/ déchiffrement, comme illustré sur la figure (2.1). De ce fait, le développement de telles approches exige une connaissance approfondie non seulement des fondements de la cryptographie, mais aussi des modèles non-linéaires et des comportements dynamiques des systèmes permettant de générer le chaos, et des éventuels problèmes liés à leur manipulation.

2.1. Dynamique chaotique

Qu'ils soient à temps continu ou discret, les systèmes chaotiques sont capables de générer des régimes dynamiques en apparence aléatoire, du fait de leur forte sensibilité aux conditions initiales et leur caractère non-linéaire. Cependant, les systèmes chaotiques étudiés dans la littérature ne sont pas tous équivalents en termes de complexité, de dimension, et de caractéristiques stochastiques. Par conséquent, le choix des systèmes chaotiques utilisés pour le chiffrement doit répondre aux critères suivants [3]:

- Avoir un comportement particulièrement complexe, produit à l'aide de simples fonctions mathématiques continues ou discrètes ;
- Générer des signaux ayant une très faible dépendance statistique et un spectre de puissance à large bande;
- Exhiber une forte sensibilité aux conditions initiales et aux paramètres de contrôle, impliquant une multitude de solutions exploitables en pratique.

En effet, plusieurs systèmes chaotiques, à temps continu et discret, ont été exploités dans les transmissions sécurisées. Toutefois, l'utilisation des systèmes chaotiques à temps discrets est généralement plus fréquente, en raison des propriétés suivantes [4]:

- Les systèmes récurrents les plus simples, même unidimensionnels, peuvent produire des régimes chaotiques assez complexes et riches. Par contre, un système d'équations différentielles doit être de trois dimensions au moins pour pouvoir générer le chaos ;
- L'implémentation des systèmes chaotiques discrets est très efficace que ce soit au niveau matériel ou logiciel, ce qui permet d'optimiser le compromis entre la sécurité et la robustesse dans les cryptosystèmes chaotiques. En revanche, les systèmes à temps continu ont une complexité de conception plus élevée;
- Les séquences chaotiques issues des récurrences discrètes non-linéaires sont en général apériodiques et bornées. Ceci permet de les utiliser comme des séquences pseudo-aléatoires qui ont l'avantage d'être reproductibles à l'identique en émission / réception.

2.2. Procédure de chiffrement/ déchiffrement

Dans le contexte du chiffrement par chaos la procédure de chiffrement désigne la manière de mélanger l'information avec le signal chaotique, qui peut être de nature analogique ou numérique. Tandis que la procédure de déchiffrement désigne l'opération inverse, où le message confidentiel est extrait du signal chaotique reproduit par le récepteur. Ces deux procédures peuvent être réalisées selon plusieurs approches qui tirent leur robustesse principalement des non-linéarités attachées aux systèmes chaotiques et leur imprévisibilité à long terme. Ainsi, il existe une forte correspondance entre ces caractéristiques et le principe du chiffrement symétrique:

- **Chiffrement :** l'aspect aléatoire des comportements chaotiques permet de construire des opérations de chiffrement qui sont non inversibles pour quiconque ne connaît pas exactement les caractéristiques du système chaotique employé;
- **Déchiffrement :** le caractère déterministe des systèmes chaotiques assure le déchiffrement pour le récepteur légitime, qui seul dispose de la configuration paramétrique adéquate permettant la reproduction du même comportement chaotique utilisé lors du chiffrement, afin de pouvoir extraire l'information confidentielle ;
- **Clé secrète :** la dépendance sensible aux conditions initiales et aux paramètres de contrôle des systèmes chaotiques incite leur emploi comme clés secrètes. La

connaissance de celles-ci est indispensable de chaque côté de la transmission pour procéder au chiffrement et au déchiffrement. Notant que la majorité des algorithmes de chiffrement par chaos proposés dans littérature utilise les paramètres des systèmes chaotiques employés comme clé secrète.

La cryptographie par chaos constitue donc une nouvelle branche de la cryptographie symétrique, communément appelée cryptographie fondée sur le chaos ou "chaotique". Néanmoins, la principale différence entre la cryptographie conventionnelle et la cryptographie chaotique est que la première consiste en des transformations définies sur des ensembles finis d'entiers, tandis que la seconde est définie sur des ensembles de réels à virgule flottante.

Par ailleurs, deux modes de chiffrement par chaos ont été inventés en compétition avec les méthodes de chiffrement conventionnelles: le chiffrement par chaos analogique et le chiffrement par chaos numérique [5].

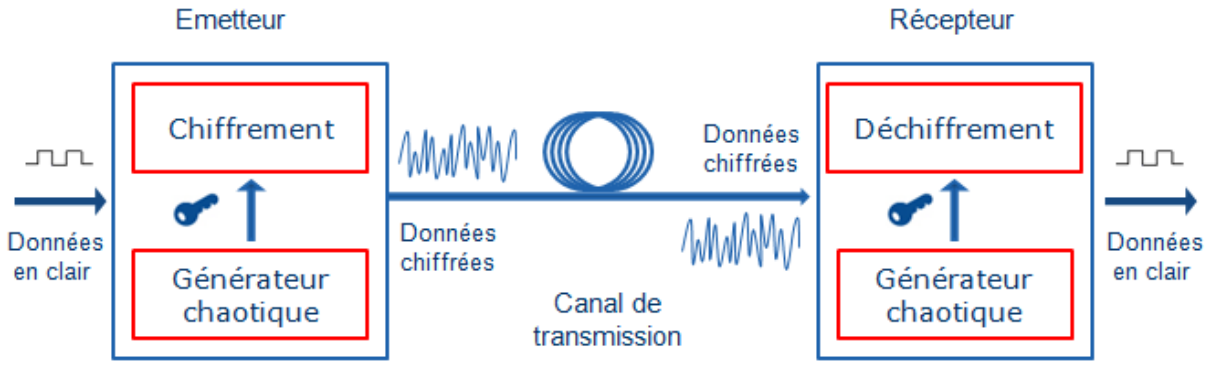

Figure.2.1- Principe du chiffrement par chaos.

III. Chiffrement par chaos analogique

Dans le cadre d'une transmission chiffrée par chaos analogique, un signal confidentiel $m(t)$ est chiffré à l'aide d'un signal chaotique $x(t)$ selon une fonction bien définie. Le signal ainsi produit $y(t)$, contenant le message confidentiel, est transmis directement au récepteur via un canal public.

La difficulté de cette méthode réside entièrement dans le déchiffrement. En effet, lors de la propagation de $y(t)$ à travers un milieu bruité il risque d'être altéré et détruit, de sorte que le signal reçu par le récepteur, $z(t) = y(t) + n(t)$; où $n(t)$ désigne le bruit additif, soit différent du signal émis $y(t)$. Dans ces conditions la restitution du signal informationnel constitue un vrai challenge à cause de la forte sensibilité des systèmes chaotiques aux

variations, et l'application d'un mécanisme de synchronisation devient nécessaire pour pouvoir extraire l'information contenue dans $z(t)$.

3.1. Synchronisation des systèmes chaotiques

L'idée originale des transmissions sécurisées par chaos analogique est rendue possible grâce à la découverte de Pecora et Carroll en 1990 [6]. Les deux chercheurs ont réussi à synchroniser deux systèmes chaotiques identiques par une décomposition en sous-systèmes, pour laquelle on dispose d'un sous-système dominant (maître) qui impose son rythme à un second sous-système esclave. En supposant que les exposants de Lyapunov du système esclave, dits conditionnels, soient négatifs, une convergence parfaite des trajectoires des deux sous-systèmes est ainsi accomplie sans tenir compte de leurs conditions initiales. Suite à cette découverte, la synchronisation des systèmes chaotiques est devenue un thème de recherche très actif, et de nombreuses méthodes de synchronisation ont été proposées et étudiées, y compris l'auto-synchronisation qui se manifeste par des interactions internes entre les systèmes chaotiques considérés, et la synchronisation commandée qui nécessite une intervention externe pour forcer deux ou plusieurs systèmes chaotiques à se synchroniser [7] [8]. Ainsi, la configuration maître-esclave de la synchronisation commandée a suscité beaucoup d'attention dans les transmissions sécurisées par chaos, de part sa robustesse et sa simplicité de mise en œuvre.

Par ailleurs, H. Nijmeijer et I. Mareels ont montré que la synchronisation maître-esclave des systèmes chaotiques peut être traitée comme un problème de synthèse d'observateurs, en mettant en relief les notions communes entre le problème de la synchronisation et celui de l'estimation d'état [9]. Par la suite, diverses approches de synthèse d'observateurs ont été développées et appliquées aux transmissions chiffrées par chaos, en vue de reconstruire l'information noyée dans les signaux chaotiques [10]. Nous nous contentons ici d'une approche généraliste de la synchronisation maitre-esclave à base d'observateurs. Des descriptions plus détaillées des autres approches de synchronisation des systèmes chaotiques sont disponibles dans [11].

Considérant la notation unifiée (2.1) pour décrire un système dynamique non-linéaire S:

$$\dot{x} = f(x,u)$$
$$y = h(x,u) \qquad (2.1)$$

Où $\dot{x}(t), t \in \mathbb{R}^+$ $(x(t+1), t \in \mathbb{N})$ correspond au vecteur d'états dans le cas continu (respectivement discret), $u \in \mathbb{R}^m$ le vecteur d'entrée et $y \in \mathbb{R}^p$ celui de sortie. f et h sont des fonctions supposées de classe C^∞.

L'observateur adapté au système S consiste en un système dynamique auxiliaire O, dont les entrées sont les entrées/sorties mesurées, c'est-à-dire $u(t)$ et $y(t)$, du système S, et la sortie est supposée être l'estimation $\hat{x}(t)$ de x(t) [12], selon une commande par retour d'état comme montré dans le schéma décrit à la figure (2.2).

$$\dot{\hat{x}} = f(\hat{x}, u) + k(\hat{x}, u, y)(y - \hat{y})$$
$$\hat{y} = h(\hat{x}, u) \qquad (2.3)$$

Où k, appelé gain de l'observateur, sert à corriger l'intégration de l'état estimé $\hat{x}(t)$ à partir de l'information fournie par l'erreur d'observation. k doit être déterminé d'une façon à assurer le fonctionnement correct de l'observateur, qui dépend principalement de la convergence de l'erreur d'observation $x(t) - \hat{x}(t)$ vers 0 quand t augmente. Lorsque cette propriété est satisfaite l'observateur est dit asymptotique. Notant que cette formulation reste valide pour les systèmes à temps discret.

Dans ce qui suit, nous allons citer les principales méthodes de chiffrement par chaos analogique. Quatre méthodes seront considérées en fonction de la technique de chiffrement et la façon d'accomplir la synchronisation.

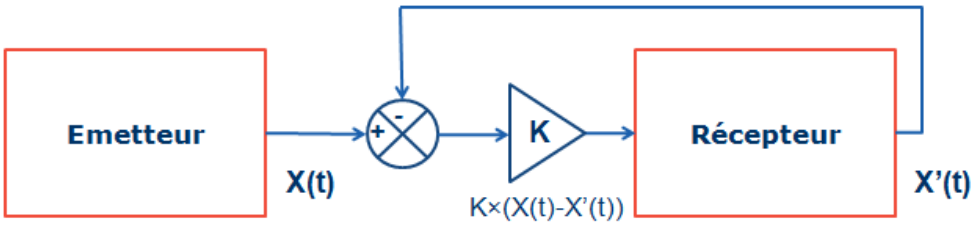

Figure.2.2- Principe de la synchronisation maître-esclave à base d'un observateur.

3.2. Chiffrement par masquage additif

Cette méthode, démontrée expérimentalement dans [13], est l'une des premières applications des signaux chaotiques aux transmissions sécurisées. Son principe consiste à additionner directement le signal confidentiel m(t), qui peut être de nature binaire ou analogique, à un signal chaotique y(t) beaucoup plus large.

Pour décoder le message au niveau du récepteur, une synchronisation maître-esclave, en faisant appel à un observateur remplissant (2.2) et (2.3), est recommandée. Il s'agit dans ce cas d'une synchronisation identique, dans laquelle le système récepteur dispose d'une configuration paramétrique identique à l'émetteur afin de dupliquer le signal chiffrant, qui sera donc plus proche du signal chaotique original $y(t)$ que de la somme $y(t) + m(t)$. De ce fait, il ne reste plus qu'à soustraire le signal généré localement de celui délivré par l'émetteur pour pouvoir restaurer le message confidentiel. Le schéma descriptif de cette méthode est donné par la figure (2.3).

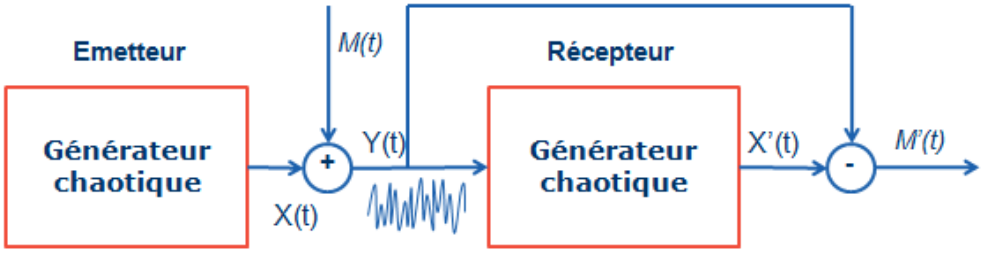

Figure.2.3- Schéma illustrant le principe du masquage additif.

Le principal avantage de cette méthode réside dans sa simplicité d'implémentation, et son adaptabilité aux signaux continus et discrets. En revanche, sa performance se dégrade considérablement en présence du bruit de canal, à cause des contraintes complexes liées au processus de synchronisation identique. D'un côté, bien que les signaux chaotiques présentent une large plage de fréquence, il faut s'assurer que le spectre du signal chaotique soit continu et infiniment plus large que celui du signal confidentiel, qui doit être typiquement de 20 dB à 30 dB plus faible. Dans ces conditions, il serait très difficile pour le récepteur de restituer le signal confidentiel sans bruit [14].

D'un autre côté, cette technique s'est avérée très fragile face aux diverses attaques, comme l'analyses spectrale qui pourrait amener à distinguer la fréquence du signal confidentiel à travers l'interception du signal chiffré, où on remarque que son spectre comporte des fréquences caractéristiques, et la fréquence dominante du message produit un pic par rapport au spectre de la porteuse chaotique. Comme il a été montré dans [15] que les signaux à forte amplitude sont faciles à reconstituer au moyen de simples filtres adaptés.

3 .3. Chiffrement par commutation (CSK)

Cette méthode a été proposée pour la première fois dans [16], principalement dans le cadre des transmissions numériques, où l'émetteur est constitué de plusieurs systèmes chaotiques utilisés en commutation conformément aux symboles du message binaire à coder.

En réception la détection des symboles se fait en mode cohérent ou incohérent. La détection non-cohérente fait appel aux techniques de détection statistique qui n'exigent pas une connaissance parfaite des caractéristiques des systèmes chaotiques utilisés dans le chiffrement. Elle est très utile dans un environnement où la synchronisation entre l'émetteur et le récepteur est difficile à atteindre, mais pas intéressante du point de vue de chiffrement, car elle ne garantit aucune sécurité [17]. Par contre, dans le contexte d'une détection cohérente, le récepteur et l'émetteur doivent disposer d'autant de générateurs chaotiques afin de mener une synchronisation maître-esclave d'une façon transitoire. Celle-ci implique un bloc de comparaison d'observateurs qui détermine le système chaotique adéquat selon le symbole émis, en se plaçant dans une période de symbole de durée T. De ce fait, un des systèmes chaotiques et seulement un se synchronise avec le signal reçu. Celui ayant le même comportement que l'émetteur qui a réellement délivré le signal confidentiel. Le diagramme représentatif du chiffrement CSK cohérent est donné par la figure (2.4).

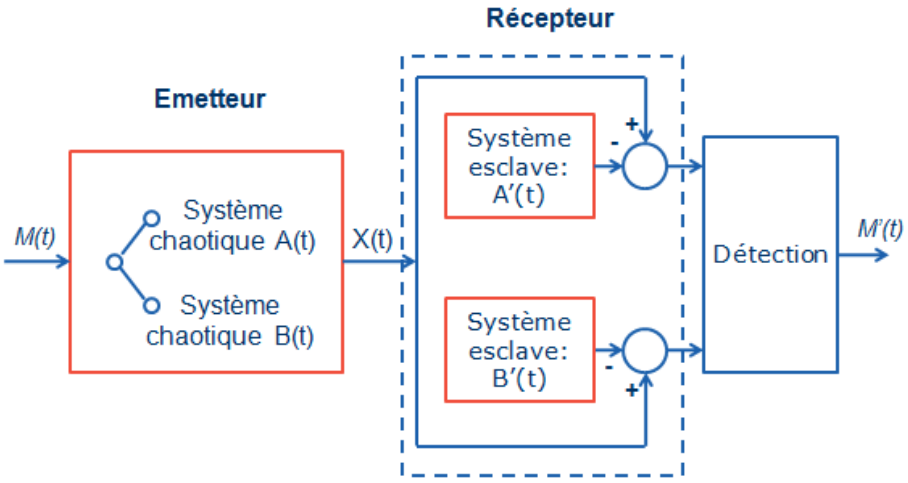

Figure.2.4- Schéma illustrant le principe du chiffrement par commutation (CSK).

Le chiffrement par commutation a l'énorme avantage d'être robuste au bruit, grâce au mécanisme de détection cohérente qui détermine d'une manière exacte les symboles du message binaire, tout en limitant l'influence du bruit sur le processus de synchronisation. En revanche, dans un contexte sans bruit, cette technique est moins intéressante est peu efficace

en terme de débit, du fait que la synchronisation est perdue à chaque fois que le message change de valeur. De plus, le temps nécessaire pour la transmission d'un seul symbole est donné par le temps de synchronisation plus le temps d'estimation, pendant lequel les vecteurs d'observation sont calculés. Par conséquent, le débit de transmission possible est limité par l'inverse du temps de synchronisation, ce qui empêche son application aux transmissions haut débit.

En outre, la nature transitoire de cette méthode de chiffrement laisse observer les changements des systèmes chaotiques émetteurs via le signal transmis, surtout lorsque les deux systèmes chaotiques utilisés au niveau de l'émetteur possèdent deux attracteurs très différents. D'où elle est jugée sensible à plusieurs attaques, telles que les techniques de classification par fonction de retour ou par les réseaux de neurones artificiels détaillées dans [18] et [19] respectivement.

3.4. Chiffrement par modulation paramétrique

L'idée de base de cette méthode est de faire intervenir le signal confidentiel, généralement de nature binaire, dans la génération de la dynamique chaotique par la modulation d'au moins un des paramètres de contrôle du système chaotique émetteur. Elle ressemble dans son principe au chiffrement par commutation, cependant la commutation s'effectue entre les paramètres d'un seul système chaotique et non pas entre des systèmes chaotiques différents.

Des techniques de synchronisation à base d'observateurs adaptatifs sont utilisées pour la restauration du signal confidentiel en réception [20] [21]. Ce genre d'observateur permet l'estimation simultanée des états et des paramètres inconnus des systèmes chaotiques en dépit des variations de paramètres. Le schéma correspondant à la modulation paramétrique est présenté dans la figure (2.5).

Cette approche de chiffrement exploite pleinement les qualités des systèmes chaotiques, en admettant des niveaux de sécurité plus élevés par rapport aux deux approches décrites auparavant. Comme elle offre également 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. Cependant, la convergence de la synchronisation au niveau du système récepteur passe par une période transitoire à chaque changement de symbole, pendant ce temps de convergence les paramètres et donc l'information sont construits de manière erronée, ce qui dégrade la qualité de la transmission. Pour répondre à cette problématique deux solutions sont

envisageables : le signal confidentiel doit rester constant pendant le temps de convergence, ou bien augmenter la durée de transmission des symboles.

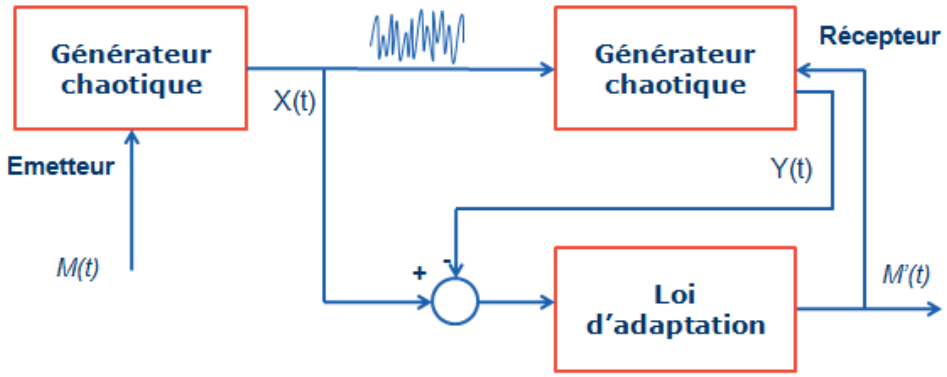

Figure.2.5- Schéma illustrant le principe du chiffrement par modulation paramétrique.

3.5. Chiffrement par inclusion

Cette méthode consiste à injecter le message confidentiel dans la dynamique chaotique, mais sans moduler les paramètres du système chaotique comme c'est le cas pour la modulation paramétrique. Il s'agit en fait d'utiliser le signal confidentiel comme une source de perturbation externe pour entretenir la dynamique du système chaotique émetteur.

En réception, des observateurs à entrées inconnues [22], ou à mode glissant [23] sont requis pour la restauration du signal confidentiel. La convergence en temps fini et le fonctionnement étape par étape de ce genre d'observateurs permettent l'estimation simultanée des états et des entrées inconnues du système chaotique. Le schéma descriptif de cette technique est représenté dans la figure (2.6).

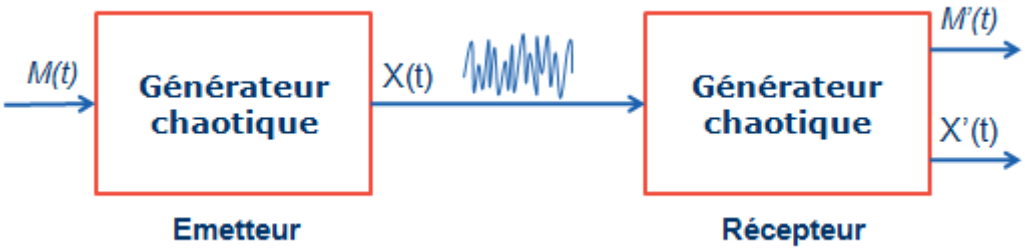

Figure.2.6- Schéma illustrant le principe du chiffrement par inclusion.

Le chiffrement par inclusion chaotique offre un niveau de sécurité nettement plus élevé par rapport aux techniques précédentes, puisque le signal confidentiel est injecté dans la

dynamique du système chaotique émetteur. De ce fait, le signal chaotique disponible dans le canal public ne porte pas l'information d'une manière directe à propos le signal confidentiel comme c'est le cas pour la technique de masquage chaotique. Ainsi, contrairement au chaos qui lui est déterministe, l'information ne répond à aucun critère de prévisibilité et évolue de façon complètement aléatoire ce qui va ajouter un degré de complexité supplémentaire à la procédure du chiffrement. Cependant, le principal inconvénient de la méthode de chiffrement par inclusion c'est qu'elle est moins sensible aux variations des paramètres, ce qui pose le problème du choix des clés secrètes valides.

3.6. Synthèse du chiffrement par chaos analogique

A la différence de la cryptographie conventionnelle, qui relève des mathématiques discrètes et de l'algorithmique, l'originalité des techniques de chiffrement par chaos analogique réside principalement dans le fait qu'elles interviennent au niveau de la couche physique du système de transmission, c'est-à-dire le module de chiffrement agit directement sur le signal confidentiel à transmettre, en particulier pour envisager des transmissions sécurisées en temps réel, tout en assurant les fonctionnalités suivantes:

Faible cout de réalisation: le comportement d'un système chaotique est entièrement décrit par des équations différentielles ou récurrentes. L'implémentation de ces équations au niveau circuit se fait par de simples montages électroniques ayant l'avantage d'une structure réduite à base de fibre dopée à l'erbium et de laser semi-conducteur [24] [25]. Ainsi, la nature et la complexité du chaos généré peuvent être facilement modifiées par le biais de ses équations mathématiques afin d'augmenter la sécurité du chiffrement;

Simplification de la transmission: l'implémentation des techniques de chiffrement par chaos analogique simplifie le schéma de la transmission, de sorte qu'un seul circuit analogique soit suffisant pour réaliser à la fois le codage et la modulation des signaux confidentiels;

Efficacité de synchronisation : les mécanismes de synchronisation utilisés dans les techniques de chiffrement par chaos analogique garantissent une sorte d'auto-synchronisation, qui permet au récepteur de se passer de la connaissance des conditions initiales de l'émetteur, et joindre la synchronisation à n'importe quel moment, en assurant le déchiffrement des signaux transmis en temps réel [26];

Transmission haut débit: certaines techniques de chiffrement par chaos analogique permettent des débits de transmission adaptés aux liaisons haut débit, notamment en fibre

optique. Les études expérimentales menées par le groupe européen de recherche OCCULT[1] ont déjà donné la preuve de faisabilité du chiffrement par chaos analogique, en acheminant des données par une porteuse chaotique à travers un réseau commercial à fibre optique avec un débit qui dépasse 1 Gb/s [27], voir même 10Gb/s pour les dernières architectures de chaos électro-optique en phase [28].

De manière générale, les techniques de chiffrement par chaos analogique présentent une solution très prometteuse pour prévenir l'interception des transmissions analogiques à caractère confidentiel, en particulier les signaux de nature complexe de type parole en téléphonie, musique pour la radiodiffusion ou encore images pour la télévision. Cependant, d'un point de vue sécurité, ces techniques n'ont pas été suffisamment optimisées pour assurer un haut niveau de confidentialité, et leur sécurité n'est pas à la hauteur de celle des standards de chiffrement conventionnel. Ainsi, la plupart d'entre elles partagent des limitations communes concernant la qualité de transmission et le niveau de sécurité:

La nature des signaux à chiffrer : les quatre méthodes de chiffrement par chaos précitées exigent des contraintes sur l'amplitude des signaux confidentiels à chiffrer, qui doit être significativement plus petite par rapport au signal chaotique. Ces restrictions découlent des propriétés structurelles des systèmes chaotiques et les techniques de synchronisation et de chiffrement utilisées;

Faible degré de confidentialité: la synchronisation requise par ces techniques de chiffrement implique la transmission d'une information suffisante à propos la dynamique chaotique employée au chiffrement. Diverses attaques peuvent par conséquent agir sur le signal de synchronisation lors de la transmission. Les plus notables sont: l'analyse des spectrogrammes [29], les techniques de filtrage [30], la fonction de retour [31] et la synchronisation généralisée [32];

Dégradation des propriétés des systèmes chaotiques: les termes correctifs appliqués aux systèmes chaotiques, pendant la synchronisation, servent à limiter l'effet du bruit qui s'ajoute au signal chaotique et à corriger les éventuelles perturbations dues aux incertitudes paramétriques. La robustesse de synchronisation vis-à-vis des conditions initiales et des paramètres de contrôles réduit la sensibilité des systèmes chaotiques aux variations, ce qui met la sécurité du cryptosystème en danger, du fait de permettre à un récepteur non autorisé

[1] Optical chaos Communications Using Laser-Diodes Transmitters http://nova.uib.es/project/occult

de se synchroniser et d'extraire l'information confidentielle sans connaissance parfaite de la clé secrète;

Cette problématique a été mise en évidence par la simulation d'une synchronisation identique en absence d'information de deux systèmes chaotiques configurés en maître-esclave. Nous avons pris comme exemple la récurrence Skew-Tent, qui sera abordée plus en détail dans le troisième et le quatrième chapitre, avec la même condition initiale et deux paramètres différents. En effet, la simulation des deux systèmes chaotiques indépendamment dévoile deux comportements tout à fait distincts (figure 2.7). Cependant, nous constatons à partir de la figure (2.8) que la synchronisation a eu lieu malgré l'utilisation de deux configurations paramétriques différentes pour les deux systèmes chaotiques couplés en maître-esclave. Ce qui implique l'impossibilité de considérer ces paramètres comme clé secrète;

Difficulté de réalisation: la mise en œuvre de ces techniques de chiffrement en pratique soulève de nombreux problèmes liés à l'environnement extérieur et aux imperfections des circuits électroniques. Il s'agit d'incertitudes paramétriques, d'erreurs de modélisation, des sources de perturbations, des dynamiques non modélisées, d'entrées inconnues, du bruit de mesure, du retard…, et plein de problèmes très difficiles à gérer;

Faible robustesse contre le bruit: il a été prouvé dans plusieurs travaux que les performances de synchronisation dans les transmissions sécurisées par chaos se dégradent rapidement en présence du bruit. Ces imperfections surviennent particulièrement lors de la transmission et la restauration des signaux utiles, notamment lorsqu'il s'agit d'une estimation conjointe des états et des entrées inconnues des systèmes chaotiques. Ces transmissions requièrent généralement un rapport signal/bruit plus important par rapport à leurs homologues traditionnels, afin de maintenir le même taux d'erreur;

La non-conformité des signaux chaotiques aux infrastructures de télécommunications: en raison de leur aspect aléatoire, les signaux chaotiques prennent des valeurs réelles et continues qui exigent un canal avec une capacité infinie, impossible à satisfaire en pratique. De plus, les techniques de chiffrement basées sur la synchronisation adaptative ou à grand gain, nécessitant un temps de convergence important, affectent la performance des transmissions en temps réel.

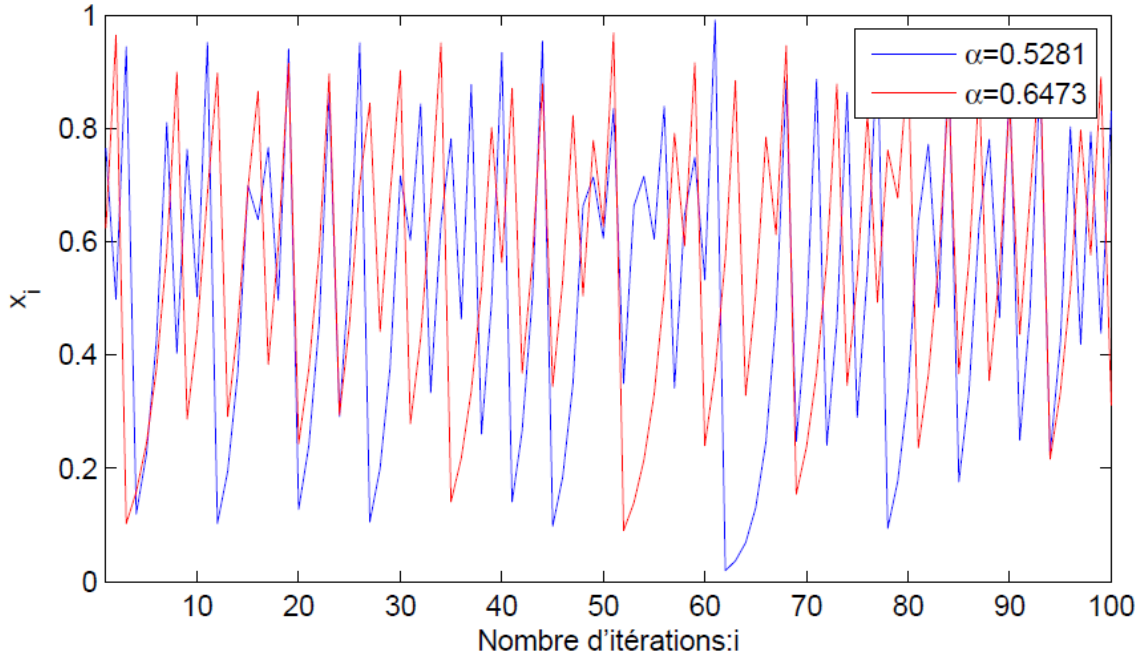

Figure.2.7- Simulation de deux orbites chaotiques générées par la récurrence chaotique Skew-Tent, à partir de deux paramètres différents (p1= 0.6473 et p2= 0.5281).

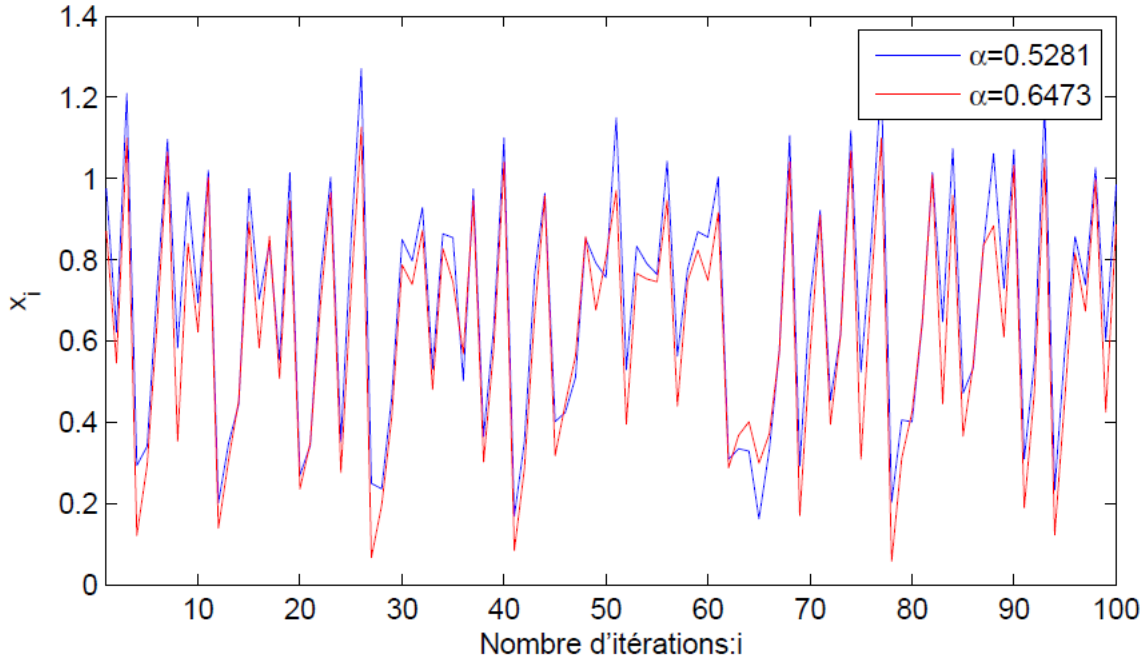

Figure.2.8- Synchronisation par couplage linéaire (k=0.7) de deux orbites chaotiques générées par la récurrence chaotique Skew-Tent, à partir de deux paramètres différents (α= 0.5281 et α= 0.6473), et en présence du bruit.

En conclusion, nous constatons que les techniques de chiffrement par chaos analogique ne peuvent pas servir à des applications réelles. À cause d'une part de leur faible niveau de sécurité, et d'autre part les restrictions imposées concernant la nature des signaux à transmettre.

Comme la plupart de ces limites sont issues des mécanismes de synchronisation employés, qui ne sont pas sécurisés et constituent par conséquent le maillon le plus faible de ces techniques de chiffrement, alors plusieurs solutions et techniques de synchronisation ont été mises au point pour y remédier. Citons à ce titre :

La synchronisation par couplage indirecte: son principe consiste à utiliser plusieurs sous-systèmes chaotiques en cascade et les synchronisés indirectement. Cette approche offre une meilleure sécurité avec une forte sensibilité aux paramètres des systèmes chaotiques. En outre, son application dans le cadre du chiffrement par commutation chaotique a fait preuve d'un haut niveau de sécurité [33];

La synchronisation impulsive : les principaux avantages de cette méthode de synchronisation, qui devient de plus en plus populaire, sont la réduction des informations redondantes dans le signal porteur et la robustesse face aux distorsions [34] [35]. D'où son application dans les transmissions sécurisées par chaos permet d'améliorer considérablement leur performance;

Communication par deux voies de transmission : le principe de cette technique consiste à séparer les tâches de synchronisation et de chiffrement en utilisant deux voies de transmission séparées. En effet, la séparation entre les opérations de chiffrement et de synchronisation permet de concevoir des fonctions de chiffrement complexes sans se soucier de perdre la synchronisation, puisque il va y avoir un autre signal chargé de maintenir la synchronisation entre les systèmes : maître et esclave [36]. Cependant, une transmission incluant deux canaux est peu intéressante pour des liaisons haut débit ;

L'utilisation des systèmes chaotiques à retard : la considération des retards fait augmenter la complexité des dynamiques chaotiques en conférant une dimension infinie à l'attracteur. Ce qui donne lieu à des améliorations notables en terme de sécurité, et permet aussi une réalisation relativement aisée des systèmes dynamiques à comportements hyper-chaotiques de grande complexité [37] ;

L'approche hybride: dans cette approche l'émetteur est composé d'une combinaison de systèmes chaotiques, en faisant intervenir des dynamiques à temps continu et à temps discret

pour complexifier d'avantage la structure du générateur chaotique [38]. Le système générateur ainsi obtenu est de nature hybride;

Transmission numérique à base de convertisseurs A/N: plusieurs chercheurs ont étudié les méthodes de synchronisation du chaos numérique à l'aide des convertisseurs A/N et N/A, pour tirer profit de la robustesse des transmissions numériques conventionnelles [39]. En effet, les convertisseurs disposés à la sortie de l'émetteur (A/N) et à l'entrée du récepteur (N/A) constituent un moyen efficace pour contrôler l'influence du bruit ajouté par le canal de transmission, tout en assurant une certaine compatibilité avec l'infrastructure de télécommunications existante.

Toutefois, la majorité des techniques précitées ont été considérées dans un cadre théorique en se limitant le plus souvent à des simulations numériques, et non pas dans un contexte réaliste de transmissions analogiques, car la mise en œuvre de telles approches reste un défi. De ce fait, il serait très logique d'orienter le développement des systèmes de chiffrement chaotiques vers le chaos discret qui semble plus conforme aux technologies existantes.

IV. Chiffrement par chaos numérique

Les vulnérabilités induites par les techniques de chiffrement par chaos analogique ont motivé l'extension de la cryptographie chaotique au domaine des signaux entièrement numériques, afin de créer une nouvelle génération de chiffrement par chaos indépendante des mécanismes de synchronisation analogiques.

L'intérêt majeur de numériser les signaux chaotiques est la génération plus aisée et de manière reproductible des séquences discrètes, ainsi que le contrôle pertinent de leurs propriétés naturelles:

- Initialisation efficace des systèmes chaotiques sans se soucier des problèmes liés à la synchronisation entre l'émetteur et le récepteur ;
- La binarisation des signaux chaotique implique l'utilisation d'une précision finie (32 bits ou 64 bits), ce qui simplifie la réalisation matérielle et augmente la performance de chiffrement/déchiffrement;
- Mécanismes de mise en œuvre et de contrôle des dynamiques chaotiques efficaces au niveau des calculateurs numériques. Ce qui élimine les effets des perturbations dues aux variations paramétriques;

- La possibilité d'utiliser les conditions initiales et les paramètres comme clés secrètes de tailles convenables.

Etant donné que cette catégorie de chiffrement par chaos est fortement inspirée de la cryptographie symétrique, son principe de base consiste à construire des transformations bijectives par rapport aux conditions initiales et aux paramètres de contrôle des systèmes chaotiques employés, conformément aux deux concepts formalisés par Shannon dans le cadre de la théorie de l'information [1]:

- **La confusion:** sert à cacher la relation entre le clair et le chiffré par l'intermédiaire d'une clé secrète. La méthode la plus courante pour appliquer la confusion est la substitution, souvent non-linéaire comme celle adoptée par l'algorithme AES (Advanced Encryption Standard);
- **La diffusion:** sert à éliminer les redondances dans le message confidentiel et à diffuser l'influence du changement d'un bit de la clé ou du clair sur tout le chiffré correspondant. La diffusion est assurée par une simple transposition ou permutation.

Au cours des deux dernières décennies, de nombreux chercheurs ont mis en évidence les fortes similitudes entre ces concepts et les propriétés naturelles des systèmes chaotiques. C'est ainsi que sont nés de nombreux algorithmes de chiffrement par chaos, trop diversifiés pour être couverts dans ce chapitre. Nous nous contentons dans ce qui suit d'un aperçu général des principales techniques de confusion et de diffusion, qui ont été considérées au sein des algorithmes de chiffrement par bloc et par flux développés dans le cadre de chiffrement par chaos. Une vue plus globale est disponible dans [40] [41].

4.1. Cryptosystèmes chaotiques par bloc

Les algorithmes de chiffrement par bloc, comme leur nom l'indique, traitent les données à chiffrer en blocs d'une longueur fixe, à l'aide des combinaisons de confusion et de diffusion de type réseau de substitution/permutation (SPN) ou schéma de Feistel. Ainsi, des itérations sur plusieurs rondes selon un mode opératoire adéquat, tel que ECB[2], CBC[3], OFB[4] ou CFB[5], sont fortement recommandées pour atteindre un haut niveau de sécurité.

[2] Electronic Code Book.
[3] Cipher Bloc Chaining.
[4] Output FeedBack.
[5] Cipher FeedBack.

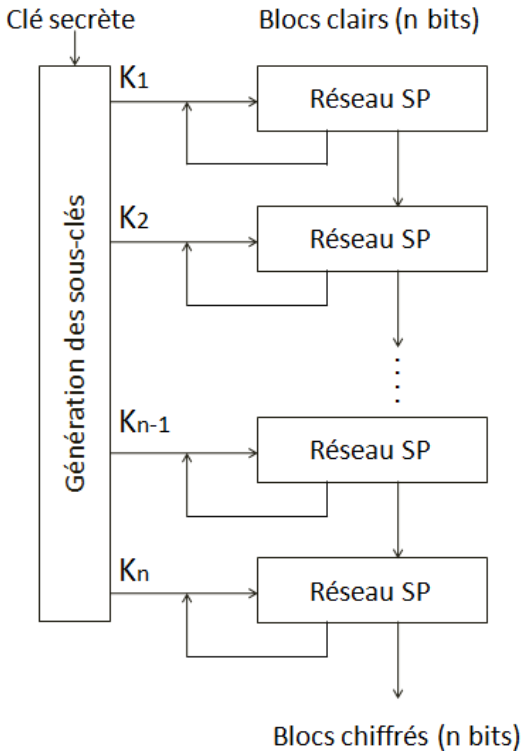

Figure.2.9- Principe du chiffrement par Bloc.

L'idée d'utiliser des systèmes chaotiques dans le chiffrement par bloc revient à créer de nouvelles primitives de confusion et de diffusion, en faisant intervenir des dynamiques chaotiques. En effet, les systèmes chaotiques, grâce à leur nature stochastique et leur aspect aléatoire présentent une source de confusion qualitativement simple, qui peut être intégrée en toute efficacité au sein des algorithmes de chiffrement par bloc, notamment pour la génération des suites chiffrantes et des tables de substitutions (S-Box et P-Box) [42] [43]. Plusieurs contributions ont été menées dans cette optique, afin d'apporter certaines améliorations aux standards de chiffrement par bloc (AES, DES, … etc.). Nous citons à titre d'exemple la contribution d'El-Badawy et Al, qui ont proposé une nouvelle approche de génération de S-Boxs basée chaos, destinée au standard AES. La comparaison de l'approche proposée avec le l'AES a montré une amélioration significative des S-Boxs générées en termes des propriétés statistiques [44]. Une autre contribution concernant l'amélioration de sécurité de l'AES à l'aide des systèmes chaotiques unidimensionnels est disponible dans [45]. Il s'agit de remplacer les S-Boxs statiques utilisées dans l'AES par des S-Boxs dynamiques générées par les récurrences: Logistique et PWLCM (PieceWise Linear Chaotic Map). Par ailleurs, plusieurs méthodes de synthétisation de S-box purement chaotiques ont été développées à base de systèmes chaotiques multidimensionnels, comme le système de Lorenz et celui de

Rossler combinés dans [46], et les récurrences chaotiques : Baker et Chebyshev (à trois et une dimension respectivement) exploitées dans [47].

D'autre part, l'utilisation des paramètres et des conditions initiales des systèmes chaotiques pour paramétrer les cryptosystèmes chaotiques peut produire un grand effet de diffusion, de sorte que la moindre modification appliquée en entrée génère un comportement chaotique tout à fait différent, du fait de la forte sensibilité des systèmes chaotiques aux conditions initiales et aux paramètres de contrôle [48].

Il est donc raisonnable d'exploiter les itérations des systèmes chaotiques pour ajouter de la diffusion aux cryptosystèmes développés, tout en considérant les paramètres et les états initiaux des systèmes chaotiques employés comme clés secrètes.

Une variété de procédures de diffusion et de boites de permutation ont été proposées et appliquées en complément aux procédures de confusion pour l'élaboration des algorithmes de chiffrement par bloc, en faisant appel aux différents systèmes chaotiques étudiés dans la littérature, comme la récurrence Tente qui a été utilisée pour permuter des blocs de données de 64 bits dans [49], la récurrence Logistique qui a été employée pour la permutation des pixels d'images dans [50] ainsi que la récurrence Chebyshev et l'application Chat d'Arnold utilisées également pour la permutation des pixels d'images à travers deux rondes de diffusion [51].

Par ailleurs, il existe dans la littérature plusieurs algorithmes de chiffrement par bloc chaotiques qui ont retenu assez d'attention en raison de leurs procédures de confusion et de diffusion originales, tels que le cryptosystème proposé par Baptista, qui consiste à divisé le domaine de la récurrence logistique en autant de sous intervalles qu'on a des caractères différents dans le message à chiffrer, avec chaque intervalle est affecté à un seul caractère. De cette façon le texte chiffré va correspondre au nombre d'itérations nécessaire pour atteindre l'intervalle adéquat [52]. Alvarez et al, ont aussi suggéré une nouvelle technique de chiffrement par bloc basée sur le comportement de la récurrence Tente. La procédure 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 [53].

Notons également qu'il existe de nombreux cryptosystèmes chaotiques basés sur la combinaison de plusieurs systèmes chaotiques monodimensionnelles et/ ou bidimensionnelles dans le but d'augmenter la complexité des procédures de confusion et de diffusion. Parmi les plus intéressants, nous pouvons mentionner l'algorithme CVES (Chaotic Video Encryption

Scheme) destiné au chiffrement des vidéos [54], ainsi que celui proposé par V. Guglielmi et al, qui repose sur l'intégration de trois séquences chaotiques issues de la récurrence Cubique implémentée sur DSP [55]. Un autre algorithme plus récent est celui de Ling Wanq et al, qui ont proposé d'intégrer la récurrence logistique et la récurrence de Chebyshev dans le chiffrement d'images. L'évaluation de leur algorithme a dévoilé des aptitudes dans la confusion et dans la sensibilité du chiffrement aux paramètres des systèmes chaotiques employés [56]. Quant à Lian et al, ont suggéré d'utiliser la récurence Standard pour la permutation, et la récurrence logistique pour la génération des clés d'addition afin d'atteindre un niveau satisfaisant de sécurité [57].

4.2. Cryptosystèmes chaotiques par flux

Les algorithmes de chiffrement par flux, appelés également à flot ou à la volée, sont généralement inspirés du chiffrement par masque jetable élaboré par Vernam en 1917. Cette technique de chiffrement est considérée inconditionnellement sûre au sens de Shannon.

4.2.1. Définition (chiffrement de Vernam)

Le chiffrement de Vernam repose sur la fabrication des clés aléatoires de n bits $(k_1, k_2, \ldots., k_n)$, appelées suites chiffrantes, aussi longues que le message à coder $(m_1, m_2 \ldots, m_n)$ et qui ne servent qu'une seule fois pour chiffrer et déchiffrer un message, en tant que flux et au moyen d'un simple ou exclusif: $c_i = m_i \oplus k_i$.

4.2.2. Théorème de shannon

Soit un cryptosystème impliquant un texte clair m, un texte chiffré c et une clé secrète k de même longueur, il est dit à sécurité parfaite si et seulement si:

- Toutes les k_i sont équiprobables;
- Pour chaque k_i et chaque c_i, il existe une unique clé k_i vérifiant $E(m_i, k_i) = c_i$.

En effet, l'utilisation de clés purement aléatoires dans le chiffrement de Vernam assure un chiffrement à sécurité parfaite au point que l'interception du message chiffré ne dévoile aucune information utile sur le message confidentiel. Cependant, le cryptosystème de Vernam n'est pas applicable en réalité, car la génération et le partage des suites chiffrantes requises par l'algorithme sont très délicats, voire impossible à assurer en pratique. De ce fait, les algorithmes de chiffrement par flux utilisés actuellement, qu'ils soient synchrone ou asynchrone, ont recours à des générateurs dits pseudo-aléatoires employés selon le même principe du chiffrement de Vernam. Dans la suite du chapitre l'accent sera mis sur les

algorithmes de chiffrement par flux chaotiques en mode synchrone, qui sont particulièrement adaptés aux transmissions temps réel.

4.2.3. Définition (générateur de nombres pseudo-aléatoires)

Un générateur de nombres pseudo-aléatoires (PRNG) permet de générer à partir d'une clé statique de petite taille, partagée secrètement entre des utilisateurs légitimes, une suite chiffrante de taille plus grande remplissant les critères suivants:

- Avoir une apparence aléatoire sur le plan statistique;
- Être suffisamment grande pour que les sous-suites finies utilisées par l'algorithme de chiffrement ne soient pas périodiques;
- Être imprévisible au sens où il doit être impossible de prédire le prochain aléa à partir des aléas précédents.

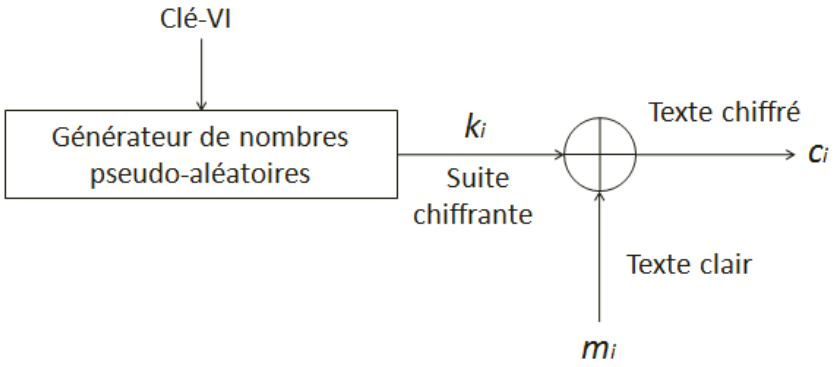

Figure.2.10- Principe du chiffrement par flux synchrone.

En effet, le caractère non-linéaire et déterministe des systèmes chaotiques permet la génération efficace des suites chiffrantes 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 à usage cryptographique, notamment pour remplacer les registres à décalage (LFSR) qui sont largement utilisés dans le chiffrement par flux conventionnel. 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.

Les algorithmes de chiffrement par flux chaotiques les plus simples utilisent généralement un seul système chaotique en tant que générateur de nombres pseudo-aléatoires, comme la récurrence Logistique [58] et la récurrence de Bernoulli (Sawtooth map) [59], qui génèrent

des séquences souhaitables au chiffrement. Ainsi, les bits de la suite chiffrante sont extraits totalement ou partiellement des états des orbites chaotiques générées sans près-traitement. Il existe, en outre, d'autres algorithmes qui extraient les bits pseudo-aléatoires par le biais d'un seuil. Ce dernier permet une simple conversion des états chaotiques en symboles binaires comme l'algorithme suggéré dans [60]. Par contre, d'autres générateurs ont été proposés en incluant des procédures de près-traitement en vue d'améliorer les propriétés statistiques des séquences produites, tel que l'algorithme décrit dans [61].

Des générateurs chaotiques plus complexes ont été suggérés par la suite, reposant sur l'intégration de plusieurs systèmes chaotiques. Citons à titre d'exemple l'algorithme CCS-PRBG (Coupled Chaotic Systems Based PRBG) qui génère des bits pseudo-aléatoires en comparant deux orbites chaotiques différentes issues de deux systèmes chaotiques discrets asymptotiquement indépendants [62]. Un autre générateur basé sur le mélange des séquences chaotiques issues de la récurrence Tente et la récurrence Cat de trois dimensions a été proposé dans [63].

Par ailleurs, certains générateurs de nombres pseudo-aléatoires chaotiques ont été optimisés pour fonctionner avec les standards de chiffrement par flux existants. Une étude a été menée dans ce sens par R. U. Ginting et R. Y. Dillak, qui ont créé un générateur de nombres pseudo-aléatoires à base de la récurrence Logistique pour l'algorithme RC4, en vue de l'adapter au chiffrement d'images. Les résultats expérimentaux montrent que le RC4 modifié fournit un moyen sûr pour le chiffrement d'images [64].

4.3. Synthèse du chiffrement par chaos numérique

La numérisation des signaux chaotiques et leur application au chiffrement ont contribué à l'émergence d'une nouvelle branche de la cryptographie symétrique, qui se fonde sur des combinaisons de confusion/diffusion originales, en exploitant efficacement les propriétés d'un ou de plusieurs systèmes chaotiques. Cette nouvelle catégorie de chiffrement tire sa robustesse principalement de l'aspect aléatoire des dynamiques chaotiques et leur imprévisibilité à long terme, et assure donc une meilleure sécurité par rapport aux techniques de chiffrement par chaos analogique:

- La quasi-totalité des cryptosystèmes chaotiques sont indépendants des mécanismes de synchronisation des systèmes chaotiques, car leurs clés secrètes sont essentiellement basées sur les conditions initiales et les paramètres de contrôle des systèmes chaotiques employés;

- La variété des systèmes chaotiques existants donne lieu aux diversifications des architectures de génération des séquences chaotiques. En outre, le niveau de confidentialité peut être beaucoup plus élevé que ce que l'on pensait possible jusqu'à présent, du fait des fonctions non-linéaires très complexes avec lesquelles les cryptosystèmes peuvent fonctionner ;
- Cette génération de cryptosystèmes a été fortement optimisée en vue d'apporter des solutions au chiffrement d'informations complexes telles que les images et les vidéos. Notant que plusieurs algorithmes de chiffrement basés chaos ont prouvé leur robustesse dans ce contexte [65] ;
- En comparaison aux générateurs de tables de substitutions et de nombres pseudo-aléatoires conventionnels, les générateurs chaotiques sont plus simples à mettre en œuvre et disposent des non-linéarités intrinsèques.

Cependant, malgré la variété des cryptosystèmes proposés dans la littérature, à savoir les algorithmes de chiffrement par bloc et par flux, aucun standard de chiffrement par chaos n'a vu le jour. Car les études des algorithmes proposés indiquent que ce genre d'algorithme ne sont pas encore à la hauteur des standards de chiffrement conventionnel, dont certains sont jugés peu sûrs et / ou inefficaces en terme de performance, et soulèvent par conséquent un nombre important de problèmes qui ne sont pas encore résolus. De ce fait, beaucoup de recommandations ont été mises à la disposition des cryptographes pour l'élaboration des algorithmes de chiffrement par chaos cryptographiquement sûrs au sens de Shannon, en tenant compte des principaux facteurs suivants [66] [67]:

Dégradation des dynamiques chaotiques : la représentation en nombres finis des signaux chaotiques entraine certaines dégradations de leurs propriétés statistiques. Il s'agit de la distribution non-uniforme des séquences générées, la redondance et l'apparition des cycles courts et prévisibles. Ce qui cause une perte d'information en conduisant le système à tourner dans un nombre réduit de valeurs.

Le procédé de binarisation des signaux chaotiques adopté doit donc maintenir leur aspect aléatoire, comme la sensibilité aux conditions initiales et la non-convergence vers une seule valeur;

La taille de la clé secrète : la clé secrète, qui dépend souvent des paramètres de contrôle et des conditions initiales des systèmes chaotiques employés, doit être de taille convenable aux applications de chiffrement symétrique. En outre, le caractère déterministe des systèmes

chaotiques exige le changement régulier de la clé secrète pour éviter son estimation, ce qui pose le problème de sa gestion et son partage;

Choix des systèmes chaotiques : la nature des systèmes chaotiques utilisés affecte considérablement la sécurité du cryptosystème, d'où un choix non pertinent peut causer de nombreuses failles de sécurité;

Procédure de chiffrement : la fragilité des procédures de chiffrement laisse, dans certains cas, exploiter le déterminisme des systèmes chaotique à des fins de cryptanalyse. En contre partie la complexité de la conception affecte la performance du chiffrement en rendant certains cryptosystèmes très couteux en matière des ressources et du temps d'exécution. De ce fait, un compromis entre la sécurité et l'efficacité doit être établi dans les cryptosystèmes chaotiques.

V. Conclusion

Nous avons exposé au cours de ce chapitre le principe du chiffrement par chaos, avec ses principaux axes proposés dans le contexte de la cryptographie symétrique, à savoir les approches de chiffrement par chaos analogique et par chaos numérique. Nous avons pu constater que ces techniques offrent chacune de grands potentiels même si on y trouve quelques défauts, en particulier les cryptosystèmes numériques, qui sont plus convaincants du point de vue de chiffrement et donc plus adaptés aux utilisations réelles.

Toutefois, la majorité des cryptosystèmes chaotiques proposés jusqu'à présent considère les conditions initiales des systèmes employés comme clés secrètes pour éliminer le problème de synchronisation entre l'émetteur et le récepteur. La définition et le partage de telles clés secrètes méritent d'être soigneusement pris en compte lors du développement d'un cryptosystème chaotique.

Dans le chapitre suivant la description et la synchronisation des systèmes chaotiques au moyen de la dynamique symbolique seront introduites pour répondre à ces préoccupations. Cette approche sera considérée dans le cadre de chiffrement par flux chaotique, étant plus avantageux par rapport aux standards adoptés actuellement, notamment pour remplacer les registres à décalage qui jouent un rôle dominant dans le chiffrement par flux conventionnel.

Chapitre3 : Étude de la représentation en dynamique symbolique des systèmes chaotiques

I. Introduction

Les techniques de chiffrement par chaos numérique évoquées dans le chapitre précédent apportent certaines originalités par rapport aux standards de chiffrement conventionnel, en matière de procédures de confusion, de diffusion et de génération de nombres pseudo-aléatoires. Cependant, l'étude de faisabilité et de performance des cryptosystèmes proposés indique que la plupart d'entre eux présentent des limitations concernant le niveau de sécurité et d'efficacité, comme ils partagent les mêmes difficultés de réalisation. D'un côté, le problème de dégradation des propriétés théoriques des systèmes chaotiques suite à leur implémentation sur des composants numériques. D'un autre côté, la majorité des cryptosystèmes chaotiques proposés considère les conditions initiales des systèmes chaotiques employés comme une partie de la clé secrète pour éliminer le problème de la synchronisation entre l'émetteur et le récepteur. La définition et le partage de telles clés secrètes n'ont pas été suffisamment traités dans la littérature.

Dans ce chapitre, nous abordons le principe de binarisation des signaux chaotiques, ainsi que les faiblesses qui en découlent. En revanche, nous montrons que la description et la synchronisation des systèmes chaotiques au moyen de la dynamique symbolique peuvent apporter des contributions prometteuses à la cryptographie par chaos, en particulier pour répondre aux problématiques précitées.

Par ailleurs, nous allons montrer que la dynamique symbolique peut tout aussi bien s'appliquer à la génération de nombres pseudo-aléatoires destinés au chiffrement par flux, dont nous envisagerons de faire le lien entre la synchronisation des systèmes chaotiques par la dynamique symbolique et le chiffrement par flux conventionnel.

II. Codage des signaux chaotiques

À la différence de la cryptographie conventionnelle, qui relève des mathématiques discrètes et de l'algorithmique, la cryptographie par chaos repose sur l'utilisation des nombres réels, qui ne peuvent pas être appréhendés correctement en pratique. D'où le passage par un procédé de binarisation est nécessaire lors de l'implémentation des systèmes chaotiques sur machine.

2.1. Définition (*Représentation binaire des signaux chaotiques*)

La représentation binaire, ou binarisation, des signaux chaotiques consiste à transformer les états générés le long des orbites chaotiques en codes binaires ayant un nombre borné de bits selon une précision donnée.

La figure (3.1) montre une description schématique d'une orbite typique d'un système chaotique discret. Etant donné, que pour chaque condition initiale correspond une orbite chaotique formée de deux parties reliées : une branche transitoire de longueur l : x_1, $x_2 \ldots . x_l$, et une partie récurrente de période n : x_{l+1}, $x_{l+2} \ldots . x_{l+n}$, pour une précision de N bits, le nombre d'états binaires possibles est largement plus petit de 2^N, et l'orbite qui en résulte constitue dans ce cas une version tronquée et arrondie, dont rien ne garantit que cette version reste chaotique [68] [69]. De manière générale, l'approximation d'une orbite chaotique par des nombres flottants se fait selon la norme IEEE 754 [70].

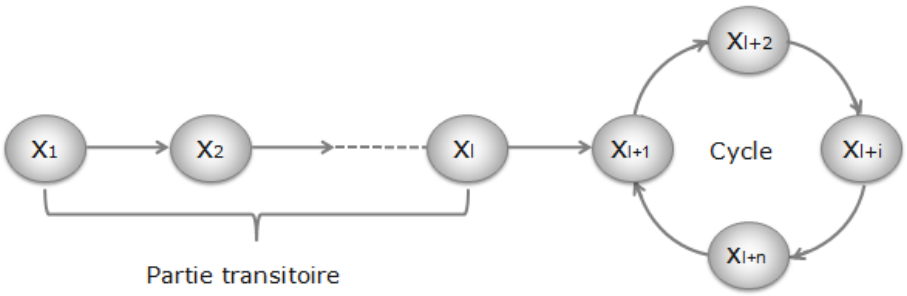

Figure.3.1- Orbite chaotique de longueur $\boldsymbol{l + n}$.

2.1. Représentation IEEE 754

La norme IEEE 754 décrit la manière de stocker les nombres à virgule flottante sur la mémoire d'un ordinateur. Elle est donnée par le format général suivant:

$$(-1)^s \times M^F \times 2^{E-B} \qquad (3.1)$$

Où S désigne le bit du signe, F la partie fractionnaire de la mantisse, E l'exposant biaisé et B le biais de l'exposant. La figure (3.2) regroupe les principaux types de nombres à virgule flottante, qui varient en fonction du nombre de bits alloués à chaque partie en mémoire, comme suit:

- **Le signe (S):** il correspond au bit de poids fort, et il sert à déterminer le signe du nombre flottant, dont il vaut 0 si le nombre est positif et 1 s'il est négatif ;
- **L'exposant (E) :** représente la puissance à laquelle il faut élever 2. Le nombre E de bits qu'il occupe dépend de la taille du type considéré;
- **La mantisse (M)** : représente la partie décimale en notation binaire scientifique du nombre flottant.

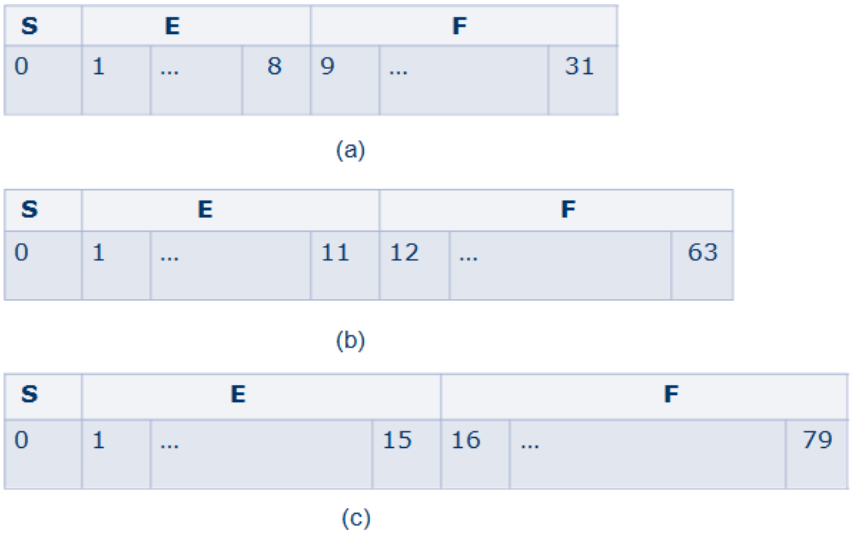

Figure.3.2- Format IEEE 754 des chiffres flottants: (a) simple précision, (b) double précision, (c) expansion de la double précision.

Le passage d'une représentation réelle continue à une représentation binaire ayant un nombre borné de chiffres, lors de l'implémentation des systèmes chaotiques sur machine, ne peut qu'altérer l'aspect chaotique des séquences générées, qui deviennent quasi-chaotiques dans ce cas, et perdent par conséquent quelques particularités mathématiques. Il s'agit de la dégradation de l'uniformité de distribution des séquences chaotiques d'une part, et

l'apparition des cycles courts et prévisibles d'autre part [71] [72]. Ce qui conduit le système chaotique à tourner dans un nombre réduit de valeurs.

Toutefois, il a été montré dans [73] que le choix de la représentation binaire des signaux chaotiques a un impact considérable sur la qualité des séquences générées. Il est évident qu'une précision plus élevée permet de mieux garder l'aspect chaotique des séquences générées. En contrepartie, la manipulation des valeurs représentées en grande précision affecte la performance des calculateurs numériques. De ce fait, un compromis entre la qualité des séquences générées et l'efficacité de leur traitement doit être établi.

En effet, il est recommandé de coder les signaux chaotiques en virgule fixe en raison d'optimisation en espace mémoire et en temps. Ainsi, il est possible dans certains cas de minimiser le nombre de bits réservés par l'élimination des bits inutiles comme celui du signe. Par exemple, pour les systèmes chaotiques qui prennent des valeurs dans l'intervalle [0, 1], une représentation en virgule fixe à 32 bits: 1Q31 (1 bit pour la partie entière et 31 bits pour la partie décimale) est très efficace en matière de performance.

Par ailleurs, des traitements supplémentaires et des manipulations spécifiques sont appliqués aux séquences chaotiques après leur binarisation afin d'améliorer leurs propriétés statistiques, spécialement pour des usages cryptographiques. Nous montrons dans la suite du chapitre que la description des systèmes chaotiques en dynamique symbolique peut servir à cet effet, en permettant une exploitation judicieuse des potentiels des systèmes chaotiques.

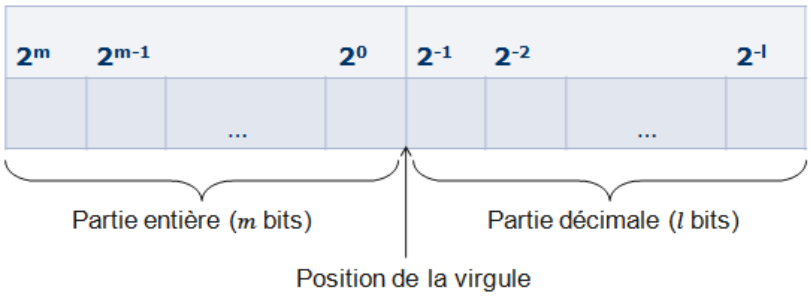

Figure.3.3- Représentation des réels en virgule fixe.

III. Description en dynamique symbolique des systèmes chaotiques

La dynamique symbolique est un outil de description et d'analyse des systèmes dynamiques, introduit par Hadamard en 1898 pour étudier les propriétés de codage des systèmes dynamiques et la codification des orbites périodiques, et comprendre ainsi la diversité et la complexité des trajectoires engendrées par des lois simples. Depuis 1989, cette approche a été largement considérée dans l'étude des dynamiques chaotiques [74],

principalement dans le cadre des transmissions numériques, dont plusieurs contributions ont été développées dans cette optique, comme les techniques de modulation basées sur le contrôle approprié des systèmes chaotiques [75], les techniques de synchronisation de haute qualité (HQS) [76] et la compression d'information [77].

3.1. Définition (*Description en dynamique symbolique*)

La description d'un système chaotique en dynamique symbolique consiste à convertir les valeurs réelles continues des signaux chaotiques en séquences de symboles, en partitionnant l'espace des phases en intervalles, dont chacun est un homéomorphisme, soit $f|I_i: I_i \rightarrow f(I_i)$ [78].

En associant à chaque intervalle I_i un symbole distinct S_i, une séquence symbolique peut être définie comme étant l'ensemble de régions que le signal chaotique visite durant son évolution temporelle [79]. Etant donné que chaque orbite chaotique est représentée par une infinité d'états $\{x_0, x_1, x_2, .. x_n, ..\}$, déterminés par une condition initiale x_0, il peut être démontré que pour chaque point de l'espace des phases est associée une séquence symbolique : $\{s_0, s_1, s_2, .. s_n, ..\} \in S$, de longueur N, où S représente l'alphabet des symboles.

Le principal enjeu de la description en dynamique symbolique est donc l'attribution des symboles aux états chaotiques. Celle-ci implique un partitionnement adéquat de l'espace des phases, de manière à assurer une simple correspondance entre les trajectoires des points et les suites symboliques, tout en maintenant les propriétés essentielles du système modélisé.

3.2. Partition génératrice

Une étape cruciale lors de la description en dynamique symbolique d'un système chaotique est le partitionnement de l'espace des phases qui agit fortement sur la nature des séquences générées, notamment en terme de distribution uniforme. Ainsi, il a été montré dans [79] que la bonne description en dynamique symbolique est obtenue par une partition génératrice, dans laquelle une relation un-à-un est assurée entre l'espace de symboles $S = \{S_i\}$ et l'espace d'états $I = \{I_i\}, i = 1..N$, par le partitionnement de ce dernier en un nombre fini d'intervalles juxtaposés et disjoints deux à deux, tels que :

$$I = \cup_{i=1}^{N}\{I_n\}\ , I_i \cap I_j = \emptyset,\ \forall\ i \neq j$$

D'un point de vue théorique, l'existence de la partition génératrice est garantie pour tout système chaotique, mais sa détermination est généralement très difficile. Néanmoins, pour la classe des systèmes chaotiques unimodals considérés dans notre étude, la partition génératrice

est donnée par : $\{[0, x_c),\ [x_c, 1]\}$, où x_c dénote le point critique du système chaotique [68]. De ce fait, l'association des symbole S_i aux intervalles I_i se fait selon la position relative de chaque x_i par rapport à l'état critique x_c.

3.3. Définition (*Application unimodale*)

Soit φ: U → U, où U = $[a;\ b] \subset \mathbb{R}$ et $a < b$, une fonction continue ou continue par morceaux. φ est dite unimodale s'il existe $c \in [a;\ b]$ tel que :

- $\varphi(a) = 0$ et $\varphi(b) = 0$;
- $\varphi_{|[a;c]}$ est de classe C^1 et strictement croissante ;
- $\varphi_{|[c;b]}$ est de classe C^1 et strictement décroissante.

c est alors appelé le point critique de φ, et la partition obtenue par rapport à c dans ce cas est absolument génératrice [68].

Notant que le choix des systèmes chaotiques qui admettent une partition génératrice comprenant deux intervalles de partitions (à l'unique point critique) est très judicieux aux transmissions numériques. Cela permet une convention standard des orbites chaotiques en symboles binaires, en considérant chaque symbole codé $s_i = \theta(x_i)$ en tant que bit d'information :

$$\theta(x_i) = \begin{cases} 0 & si\ \ x_i < x_c \\ 1 & si\ \ x_i \geq x_c \end{cases} \qquad (3.2)$$

En effet, le fait d'arrondir les états d'une orbite chaotique par tronquer leurs parties décimales suivant (3.2), permet de conserver davantage son aspect aléatoire de façon plus pertinente par rapport aux représentations binaires de la norme IEEE 754 dans certains cas.

L'évaluation statistique des séquences binaires issues de la récurrence Skew-Tent par les tests standards NIST SP 800-22, élaborés par le NIST[6] [80], indique que la représentation en dynamique symbolique exhibe de meilleures propriétés statistiques du fait qu'elle réussisse tous les tests. Contrairement à la représentation en double précision qui échoue quatre tests significatifs. Ce qui encourage l'emploi de la représentation en dynamique symbolique de la récurrence Skew-Tent aux transmissions chiffrées, qui reposent principalement sur les générateurs de nombres pseudo-aléatoires. Une description plus détaillée des quinze tests statistiques NIST SP 800-22 est disponible dans l'annexe A.

[6] American National Institution of Standard and Technology Information

Tests statistiques	Double precision	Dynamique symbolique
Frequency	0.000016	0.296963
Block frequency (m = 128)	0.827429	0.247308
Cumulative sums Forward	0.000017	0.449055
Cumulative sums Reverse	0.000021	0.325081
Runs	0.000000	0.199049
Long runs of one's	0.159720	0.644274
Binary Matrix Rank	0.013137	0.512135
Spectral DFT	0.568708	0.198762
No overlapping templates (m = 9)	Succès	Succès
Overlapping templates (m = 9)	0.083618	0.396014
Universal (L = 7,Q = 1280,K = 41577)	0.122180	0.596270
Approximate entropy (m = 10)	0.342191	0.312608
Random excursions	Succès	Succès
Random excursions variant	Succès	Succès
Serial (m=16) P-value1	0.250454	0.142705
Serial (m=16) P-value2	0.256616	0.390614
Linear complexity (M = 500)	0.466157	0.501126

Tableau.3.1- Résultats des tests statistiques NIST SP 800-22 appliqués sur deux flux binaires de taille 1 Mb, générés par le même jeu de paramètres (CI = 0,72859, α = 0,50063).

IV. Synchronisation basée sur la dynamique symbolique

Un autre potentiel de l'utilisation de la description en dynamique symbolique des systèmes chaotique dans les transmissions chiffrées réside dans la simplification du problème de synchronisation entre l'émetteur et le récepteur, à l'aide d'une approche par itération en arrière. L'idée générale de cette approche s'articule autour de l'exploitation efficace de l'unique correspondance entre l'état initial d'un système chaotique et sa séquence dynamique symbolique [81].

4.1. Approche par itérations en arrière

Le principe de l'approche par itérations en arrière (backward iterations en anglais) repose sur l'estimation de l'état initial d'un système chaotique à partir de la séquence dynamique symbolique correspondante comme suit [82] :

$$f:[0;\ 1] \rightarrow [0;\ 1]; \quad x_{n+1} = f^n(x_0, \alpha) \quad (3.3)$$

Considérant la récurrence chaotique unimodale de la forme (3.3), dotée d'une partition génératrice à seulement deux intervalles de symboles: $I_i, i = 1, 2$. Où x_0 et α correspondent à la condition initiale et le paramètre critique de la récurrence chaotique respectivement.

En supposant que pour chaque intervalle I_i de l'espace des phases, le système chaotique lui associe une fonction linéaire $f_i : I_i \rightarrow I$, bijective sur son intervalle de définition I_i, et par conséquent inversible. Alors on peut affirmer que $f_i^{-1}: I \rightarrow I_i$, la fonction inverse de f_i, existe pour tous $i = 1 \ldots N$, avec pour expression l'équation générale (3.4).

$$x_i = f^{-\mathrm{i}}(S_{i+1}) \quad (3.4)$$

D'un côté, le fait d'opter pour une partition génératrice, lors de description en dynamique symbolique de la récurrence chaotique (3.3), implique que pour n'importe quelle valeur dans I lui correspondra juste une valeur dans S et vice versa. Ce qui conduit à l'unique correspondance entre la condition initiale et sa séquence symbolique.

$$x \neq x' \Rightarrow f(x) \neq f(x') \quad (3.5)$$

D'un autre côté, la relation bijective entre l'ensemble $I = \bigcup_{i=1}^{N} I_i$, qui représente l'espace d'états du système chaotique, et l'alphabet $S = \bigcup_{i=1}^{N} S_i$, permet la contraction des itérations successives de la fonction inverse (3.4) dans l'intervalle (3.6). De ce fait, plus la longueur de la séquence symbolique augmente, plus l'intervalle qui contient la condition initiale diminue jusqu'à l'obtention d'un point unique [83].

$$I = \bigcap_{i=1}^{N} f^{-\mathrm{i}}(S_i) \quad (3.6)$$

L'unicité de la solution induite par (3.5) et (3.6) justifie l'efficacité de l'approche par itération en arrière dans l'estimation de la condition initiale inconnue de toute orbite chaotique issue de (3.3), à partir de la séquence symbolique correspondante, de sorte qu'au bout d'un certain nombre d'itérations le processus d'estimation se stabilise sur la valeur adéquate. Nous allons montrer par simulation numérique l'estimation d'une condition initiale à partir de sa séquence symbolique suivant l'approche par itérations en arrière.

4.2. Exemple :

Prenons la séquence dynamique symbolique (3.7), associée à l'orbite chaotique tracée sur la figure (3.4), générée par la récurrence Skew-Tent (3.8). La séquence $S(n)$ a été obtenue en considérant la partition génératrice de l'espace des phases au point critique $x_c = \alpha$.

$$S(n) = \{0,1,1,1,1,0,1,1,0,0,1,0,0,1,0,1,0,1,1,0,0,0,0,1,1\} \quad (3.7)$$

$$f(x_i) = \begin{cases} \frac{x_i}{\alpha} & si \quad x_i \leq \alpha \\ \frac{(1-x_i)}{1-\alpha} & si \quad x_i > \alpha \end{cases} \quad (3.8)$$

La récurrence Skew-Tent appartient à la classe des systèmes chaotiques unimodals, pour lesquels l'existence de l'application inverse $f_i^{-1}: I \to I_i$ est évidente pour tout $i = 1 \ldots N$, avec pour expression la fonction récurrente (3.9).

$$f^{-1}(s_i) = \begin{cases} \alpha * y_{n-1} & si \quad s_i = 0 \\ 1 - \left((1-\alpha) * y_{n-1}\right) & si \quad s_i = 1 \end{cases} \quad (3.9)$$

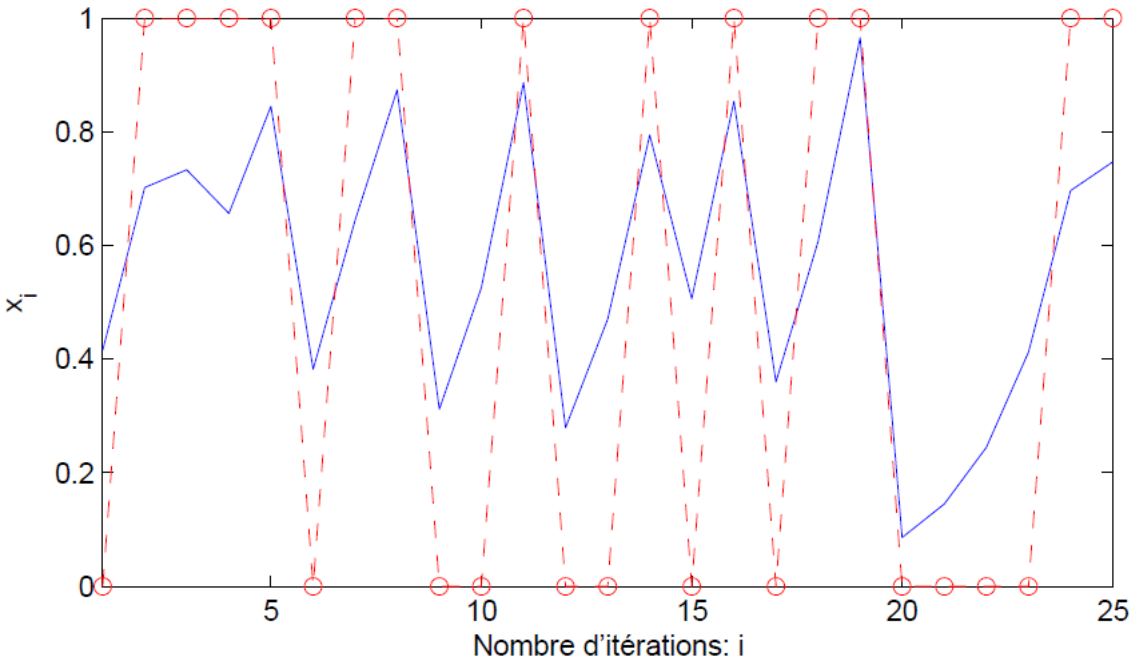

Figure.3.4- La séquence symbolique associée à l'orbite chaotique de la récurrence Skew-Tent.

Pour estimer l'état initial ($x_0 = 0.4158$) générant la séquence (3.7) selon l'approche par itérations en arrière, il suffit d'itérer l'application inverse (3.9) de la récurrence Skew-Tent à partir d'une initialisation aléatoire, en parcourant la séquence dynamique symbolique (3.7) en sens inverse, puisqu'il s'agit d'itération en arrière.

En lançant la simulation avec la même valeur du paramètre utilisée dans la génération de la séquence $S(n)$: $\alpha = 0{,}5927$ et $x_0' = 0{,}7500$ comme condition initiale, nous obtenons les valeurs affichées dans le tableau (3.2).

Nous constatons d'après les valeurs calculées, que l'approche par itérations en arrière permet d'estimer la condition initiale avec succès après seulement 25 itérations. Par ailleurs, il a été montré dans [84] que l'estimation exacte de la condition initiale est proportionnelle au nombre de symboles M de la séquence dynamique symbolique, avec une précision de l'ordre de $1/2^M$.

i	s_i	x_i
1	1	0.7500
2	1	0.6938
3	0	0.4105
4	0	0.2429
5	0	0.9008
6	0	0.6322
7	1	0.7419
8	1	0.4390
9	0	0.8208
10	1	0.4856
11	0	0.8017
12	1	0.6727
13	0	0.3980
14	0	0.2355
15	1	0.1393
16	0	0.0825
17	0	0.9663
18	1	0.6054
19	1	0.7528
20	0	0.4454
21	1	0.8181
22	1	0.6660
23	1	0.7281
24	1	0.7027
25	0	0.4158

Tableau.3.2- Exemple de simulation numérique de l'approche par itération en arrière

i	s_i	x_i
1	1	0.7500
2	1	0.6925
3	0	0.4086
4	0	0.2411
5	0	0.9012
6	0	0.6305
7	1	0.7415
8	1	0.4375
9	0	0.8206
10	1	0.4842
11	0	0.8015
12	1	0.6714
13	0	0.3961
14	0	0.2337
15	1	0.1379
16	0	0.0814
17	0	0.9666
18	1	0.6037
19	1	0.7525
20	0	0.4440
21	1	0.8180
22	1	0.6646
23	1	0.7275
24	1	0.7017
25	0	0.4140

Tableau.3.3- Sensibilité de l'estimation de la condition initiale au paramètre de contrôle.

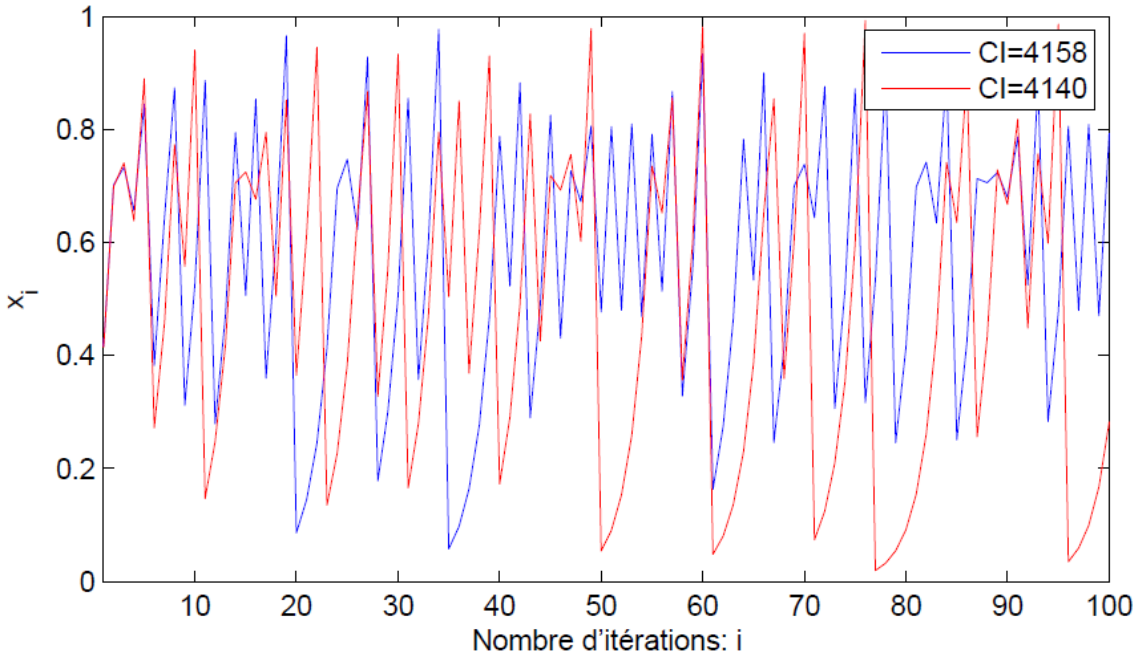

Figure.3.5- Comparaison des orbites chaotiques générées par deux conditions initiales différentes.

Par conséquent, l'approche par itération en arrière, communément appelée SDM (symbolic dynamic based method) permet d'établir la synchronisation dans les transmissions sécurisées par chaos, car la faisabilité de l'estimation de la condition initiale avec exactitude permet la reconstitution d'une séquence chaotique peu importe sa longueur. De plus, le nombre de symboles nécessaires à l'estimation de la condition initiale garantit une synchronisation très rapide entre les systèmes chaotiques de l'émetteur et du récepteur, ce qui rend cette méthode très intéressante pour des applications en temps réel, tant du point de vue de la performance que de la robustesse.

Cependant, l'estimation ne peut pas être précise sans connaissance exacte du paramètre de contrôle. Le tableau (3.3) montre l'erreur commise dans l'estimation de la même condition initiale, à partir d'une valeur de paramètre erronée : $\alpha = 0{,}5900$. Vue la forte sensibilité des systèmes chaotiques aux conditions initiales, la moindre erreur dans l'estimation de la condition initiale conduit à deux trajectoires tout à fait distinctes comme montré par la comparaison des orbites chaotiques de la figure (3.5).

V. L'intérêt de la synchronisation par dynamique symbolique aux transmissions chiffrées

La première exploitation de la description en dynamique symbolique des systèmes chaotiques dans le cadre du chiffrement a été proposée par E. Alvarez et all en 1999. Il s'agit d'un algorithme de chiffrement par bloc, basé sur le contrôle approprié du comportement

chaotique de la récurrence Tente afin d'obtenir des séquences symboliques qui conviennent à l'alphabet des données confidentielles [85]. L'algorithme en question n'était pas très convaincant du point de vue de sécurité, comme il a été cryptanalysé dans [86], principalement à cause de la mauvaise exploitation de la dynamique symbolique et la fragilité de la procédure de chiffrement.

D'autres études plus récentes ont confirmé qu'il n'est pas faisable d'utiliser les séquences symboliques issues directement des systèmes chaotiques dans le chiffrement, puisqu'il est possible d'estimer la condition initiale, ainsi que les paramètres des systèmes chaotiques à travers des séquences de longueur adéquate [87] [88]. Suite à ces faiblesses de sécurité, peu d'intérêt a été accordé à l'usage des dynamiques symboliques au chiffrement par chaos. Néanmoins, les conditions de synchronisation et de mise en œuvre aisées de la SDM présentent un grand potentiel pour les transmissions chiffrées par chaos en temps réel, car d'une part, la SDM permet de résoudre le problème de synchronisation entre l'émetteur et le récepteur via le partage efficace de la condition initiale. Sachant que deux conditions initiales égales (la même valeur présentée avec la même précision et le même arrondissement) conduisent forcément aux mêmes séquences chaotiques. Ce qui garantit le déterminisme nécessaire à la procédure de déchiffrement.

D'autre part, la nécessité de connaître le générateur chaotique employé dans la génération des séquences dynamiques symboliques utilisées dans le chiffrement assure un certain degré de confidentialité, vu que la synchronisation est conditionnée par la connaissance parfaite du système chaotique employé. Par conséquent, tout autre générateur employé à la réception ne peut pas servir à l'estimation de la condition initiale. Cette particularité peut être à l'origine du développement de très forts algorithmes de chiffrement, y inclus le chiffrement par flux, dont il existe de fortes similitudes entre les deux concepts.

5.1. Similitudes entre la synchronisation par dynamique symbolique et le chiffrement par flux

Il est évident, dans le contexte du chiffrement par flux, que pour un algorithme particulier, une même clé secrète produira toujours la même suite pseudo-aléatoire, ce qui implique le changement fréquent de la clé secrète pour éviter les failles de sécurité. C'est pourquoi un vecteur d'initialisation de longueur m bits, dénoté IV, est utilisé en pratique pour créer des clés secrètes dynamiques afin de diversifier la sortie du générateur de nombres pseudo-aléatoires pour une clé donnée. Ainsi, plusieurs messages peuvent être chiffrés par la même clé secrète, à condition de ne pas employer deux fois la même paire (clé, IV).

L'utilisation de la SDM dans les transmissions chiffrées par chaos permet de même l'usage à la fois efficace et sécurisé de clés secrètes dynamiques suivant le mécanisme présenté à la figure (3.6), dans lequel plusieurs similitudes sont constatées entre la synchronisation des systèmes chaotiques au moyen de la dynamique symbolique et le chiffrement par flux conventionnel:

- Les premiers M symboles (bits) $S(x_i), i = 1..M$, qui correspondent au vecteur d'initialisation, doivent être transmis directement au récepteur via un canal publique, pour établir la synchronisation;
- Par la suite, les séquences dynamiques symboliques servent de suites chiffrantes, qui doivent être mélangées avec l'information confidentielle, selon différentes fonctions de chiffrement;
- Chaque système chaotique peut générer un très grand nombre de suites chiffrantes de longueurs désirées, en changeant simplement son état initial ou son paramètre critique, ce qui permet la réutilisation à la fois efficace et sécurisée de la clé secrète;
- En réception, même si le signal reçu est corrompu par un bruit blanc gaussien additif: $S(x) = S(x + w)$, tel que w est de moyenne nulle et variance σ_2, la séquence dynamique symbolique reste détectable, de sorte que l'utilisation d'un filtre adapté est suffisante pour estimer correctement le vecteur d'initialisation, puis l'utiliser dans la récupération de la condition initiale;
- Toutefois, le déchiffrement n'est pas possible sans une connaissance précise des paramètres critiques des systèmes chaotiques employés, étant la clé secrète du crypto-système.

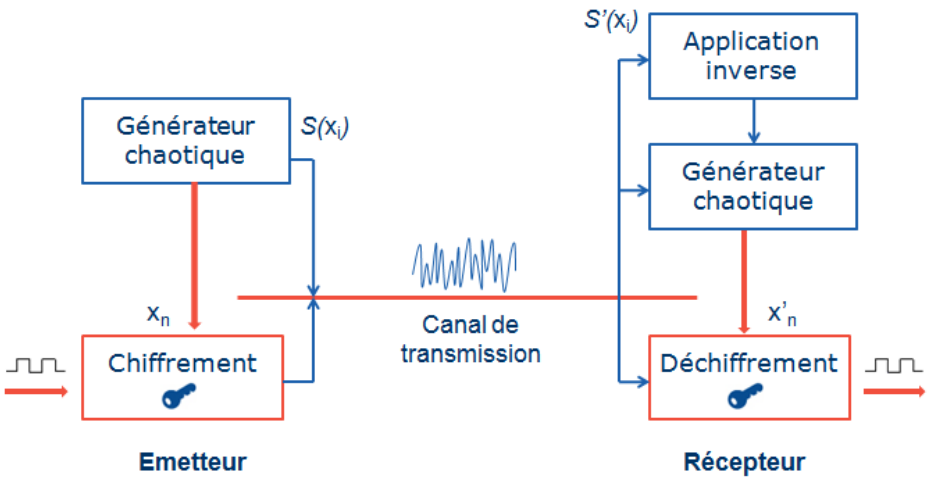

Figure.3.6- Mécanisme général du chiffrement par la SDM.

L'originalité du chiffrement par flux à base de la SDM par rapport au chiffrement par flux conventionnel réside dans la dépendance sensible des systèmes chaotiques aux conditions initiales et aux paramètres de contrôle. Cette sensibilité apporte un degré de confidentialité supplémentaire de façon que seul l'utilisateur légitime, qui connaît le générateur chaotique, soit en mesure de se synchroniser avec l'émetteur par l'estimation correcte de la condition initiale, même si le vecteur d'initialisation est partagé en clair.

Cependant, pour tirer profit de la SDM dans le chiffrement par flux, une attention particulière doit être accordée aux générateurs de nombres pseudo-aléatoires basés chaos adoptés, tout en considérant les mécanismes nécessaires pour remédier la dégradation des dynamiques chaotiques due à leur représentation binaire. Plusieurs solutions ont été utilisées pour étendre la période des séquences chaotiques générées et améliorer leurs propriétés statistiques. Nous citons à titre d'exemple [89] :

- ***Utilisation des précisions plus élevées***: la présentation des états chaotiques avec une précision plus élevée permet de mieux conserver leur aspect aléatoire et étendre la période des séquences binaires générées ;
- ***Cascader plusieurs systèmes chaotiques***: la combinaison de plusieurs systèmes chaotique en cascade augmente la complexité du générateur de nombres pseudo-aléatoires, ainsi que la taille de la clé secrète ;
- ***Perturbation des systèmes chaotiques:*** l'application d'une perturbation présente une solution efficace pour éviter la redondance et étendre les cycles des séquences chaotiques. Plusieurs sources de perturbation sont envisageables, telles que les LFSRs (linear-feedback shift registers) ou bien LCGs (Linear Congruential genrators), qui peuvent agir sur les états ou les paramètres de contrôle des systèmes chaotiques employés.

VI. Conclusion

Nous avons abordé au cours de ce chapitre la représentation binaire des signaux chaotiques et les problèmes qui en découlent. Toutefois, nous avons montré que la description des systèmes chaotiques au moyen de la dynamique symbolique nous offre de nouvelles opportunités pour exploiter leurs comportements dans la cryptographie, en particulier pour la création de nouveaux algorithmes de chiffrement par flux, du fait qu'il existe de fortes similitudes entre la synchronisation des systèmes chaotiques par la dynamique symbolique et le chiffrement par flux conventionnel.

Ces constatations nous seront très utiles par la suite, dont nous envisageons d'exploiter la description en dynamique symbolique des systèmes chaotiques dans la conception d'un nouvel algorithme de chiffrement par flux, qui fera l'objet du chapitre suivant. À ce propos, un nouveau générateur de nombres pseudo-aléatoires sera développé, avec une structure originale basée sur l'intégration de plusieurs systèmes chaotiques unidimensionnels sélectionnés d'après leur aspect aléatoire et leurs propriétés statistiques.

Chapitre 4 : Contribution à l'application du chaos au chiffrement par flux

I. Introduction

Nous avons tenté d'expliquer aux chapitres précédents l'avantage du chiffrement par chaos numérique par rapport au chaos analogique, notamment la description en dynamique symbolique des systèmes chaotiques. Nous reprenons dans ce chapitre nos explications, en les adaptant au contexte particulier du chiffrement par flux. Plus précisément, nous allons décrire l'exploitation de la description et la synchronisation des systèmes chaotiques au moyen de la dynamique symbolique dans la conception d'un générateur de nombres pseudo-aléatoires, basé sur des récurrences chaotiques unidimensionnelles, et son intégration au sein d'un nouvel algorithme de chiffrement par flux.

Des mécanismes originaux sont considérés au cours de la conception de notre cryptosystème afin de combler les faiblesses déjà décelées dans les techniques existantes, en y incluant le choix judicieux des systèmes chaotiques et la procédure de génération de nombres pseudo-aléatoires, sans perte de robustesse liée à l'implémentation des systèmes chaotiques sur machine, ainsi que la résolution du problème de synchronisation entre l'émetteur et le récepteur suivant l'approche par dynamique symbolique.

Par ailleurs, nous allons mener une étude destinée à quantifier le niveau de sécurité du cryptosystème proposé en tenant compte des tests statistiques les plus significatifs, et des attaques spécifiques aux algorithmes de chiffrement par flux.

II. Choix des systèmes chaotiques

Le noyau de tout cryptosystème par chaos est le choix des systèmes chaotiques adéquats à la structure de chiffrement adoptée. Cependant, bien que les systèmes chaotiques génèrent des comportements en apparence aléatoire, mais restent totalement déterministes selon une loi de développement mathématique. D'où l'exploitation directe des régimes chaotiques au chiffrement est risquée, de sorte qu'un mauvais choix du système chaotique, de l'état initial ou

des paramètres de contrôles peut causer de graves failles de sécurité [90]. Par conséquent, toute proposition visant à utiliser le chaos pour le chiffrement doit prendre en compte une série de recommandations, afin d'éviter les exploitations malicieuses des dynamiques chaotiques à des fins de cryptanalyse. Il s'agit d'un côté du choix appropriés des systèmes chaotiques, et d'un autre côté des mécanismes de chiffrement qui répondent aux critères de robustesse et d'efficacité.

Nous allons présenter dans cette section une étude comparative des performances d'un ensemble de systèmes chaotiques discrets, qui ont été appliqués au chiffrement. L'étude envisagée porte sur les propriétés statistiques et l'aspect aléatoire (la densité de probabilité, fonction de corrélation, exposant de Lyapunov) des séquences chaotiques issues des récurrences unidimensionnelles listées dans le tableau (4.1), pour en sélectionner les plus convenables à notre algorithme de chiffrement.

Les systèmes considérés dans notre étude présentent l'intérêt d'avoir une expression mathématique très simple, tout en conduisant aux régimes dynamiques variés. Il est à noter cependant que l'évolution temporelle de ces récurrences, à partir des valeurs initiales arbitraires et des valeurs de paramètres de contrôles appartenant aux intervalles indiqués dans le tableau (4.1), fait apparaitre des comportements chaotiques dans l'intervalle [0, 1].

Récurrence chaotique	**Formule mathématique**	**Paramètre critique**
Bernoulli	$x_{i+1} = (\alpha \times x_i) mod\ 1$	$\alpha >= 1$
Cubique	$x_{i+1} = \alpha x_i (1 - x_i^2)$	$\alpha \in [2.3, 3]$
Logistique	$x_{i+1} = \alpha x_i (1 - x_i)$	$\alpha \in [3.57, 4]$
Sine	$x_{i+1} = \alpha \times \sin(\Pi\, x_i)$	$\alpha \in [1, 3]$
Skew-Tent	$x_{i+1} = \begin{cases} \frac{x_i}{\alpha} & si \quad x_i \leq \alpha \\ \frac{(1 - x_i)}{1 - \alpha} & si \quad x_i > \alpha \end{cases}$	$\alpha \in [0,1]$

Tableau.4.1- Systèmes chaotiques discrets unidimensionnels.

2.1. Densité de probabilité

L'étude de la densité de probabilité, connue aussi par l'entropie ou encore la mesure invariante, est cruciale pour les sources de pseudo-aléa utilisées pour le chiffrement. Elle réfère immédiatement à la notion d'ergodicité, qui implique que les trajectoires chaotiques doivent parcourir tous les états de l'espace des phases de façon équiprobable.

Soit X une variable aléatoire continue à valeurs dans l'intervalle [a, b], alors il est possible de caractériser son comportement en introduisant la densité de probabilité $p(x)$, telle que $\int_a^b p(x)dx$ représente le nombre de fois ou l'intervalle [a, b] est visité. Cette densité de probabilité possède deux propriétés importantes, et permet de déterminer la fonction de répartition F_X [91]:

$$\begin{cases} p(x) \geq 0 \\ \int_{-\infty}^{+\infty} p(x) = 1 \end{cases}$$

$$F(X \, \epsilon \, [a,b]) = F_X(b) - F_X(a) = \int_a^b p(x)dx \qquad (4.1)$$

En supposant que l'espace des phases U= [0, 1] est divisé en M intervalles disjoints pour chacun des systèmes étudiés, et en faisant générer des séquences de langueur N=100000 (calculées en double précision), à partir des conditions initiales et des paramètres aléatoires, la densité de probabilité $p(x)$ des récurrences chaotiques étudiées est facilement déterminée en vertu de leurs histogrammes de répartition.

Nous observons d'après les courbes de densité invariante illustrées ci-dessous que les histogrammes visualisés soulignent une différence importante entre les récurrences chaotiques étudiées. En effet, les récurrences : Skew-Tent et Bernoulli 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 reflètent un haut niveau de confusion. Quant au reste des récurrences : Cubique, Logistique et Sine, les états qui composent leurs trajectoires sont distribués à peu près de la même manière, dont nous remarquons que les intervalles des extrémités sont les plus visités, avec une fonction de répartition qui diffère de la distribution uniforme.

2.2. 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, notamment pour éliminer la relation statistique entre les données en clair et chiffrées.

Les résultats de simulation des fonctions d'auto-corrélation (4.2) et d'inter-corrélation (4.3) des systèmes chaotiques étudiés, pour des séquences de longueur N=100000, sont donnés dans les figures ci-dessous.

$$C_x = \frac{E[(x_i - \bar{x})(x_i + k - \bar{x})]}{\sigma^2} \quad (4.2)$$

$$C_{xy} = \frac{1}{n}\sum_{i=1}^{n-k}(x_i - \bar{x})(y_{i+k} - \bar{y}) \quad (4.3)$$

Où E est l'espérance mathématique, k est le décalage temporel et σ^2 est la variance.

Nous remarquons que les résultats de simulation sont très proches pour la majorité des récurrences. D'une part, il n'existe aucune auto-corrélation 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. Par conséquent nous pouvons conclure que les séquences générées à partir des récurrences étudiées sont complètement imprévisibles et de nature typique des processus dits à bruit blanc.

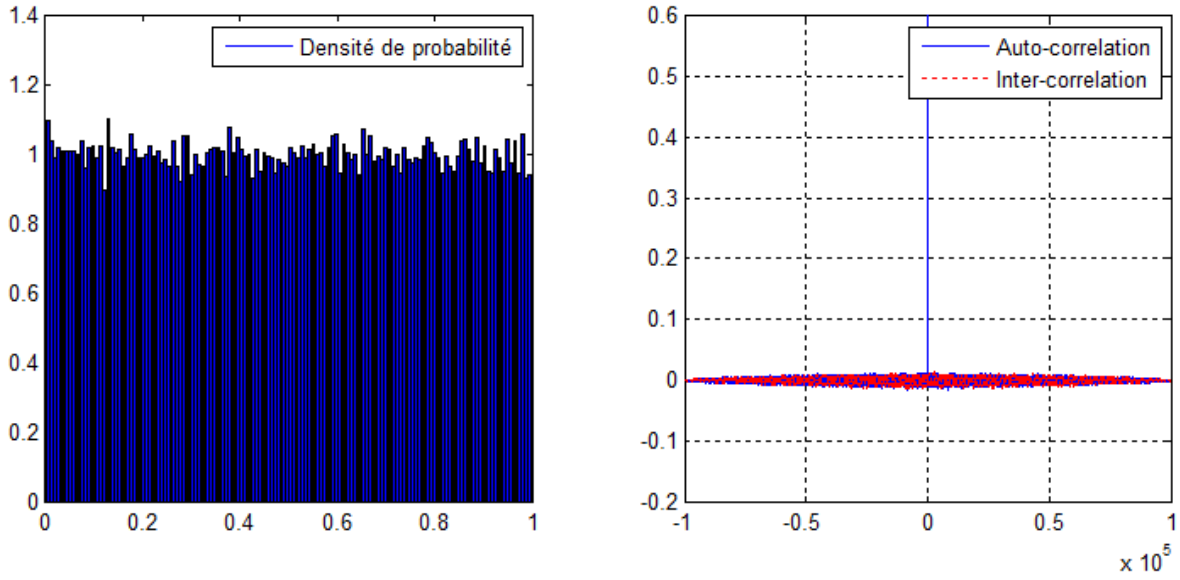

Figure.4.1- Simulation de la densité de probabilité et les fonctions d'auto/ inter-corrélation de la récurrence Bernoulli.

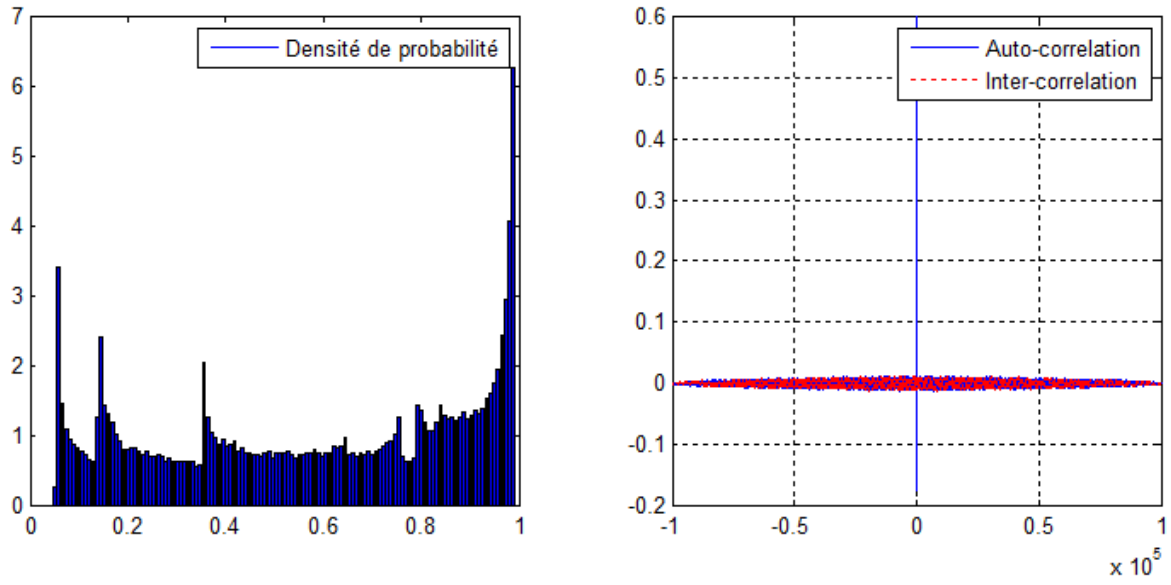

Figure.4.2- Simulation de la densité de probabilité et les fonctions d'auto/ inter-corrélation de la récurrence Cubique.

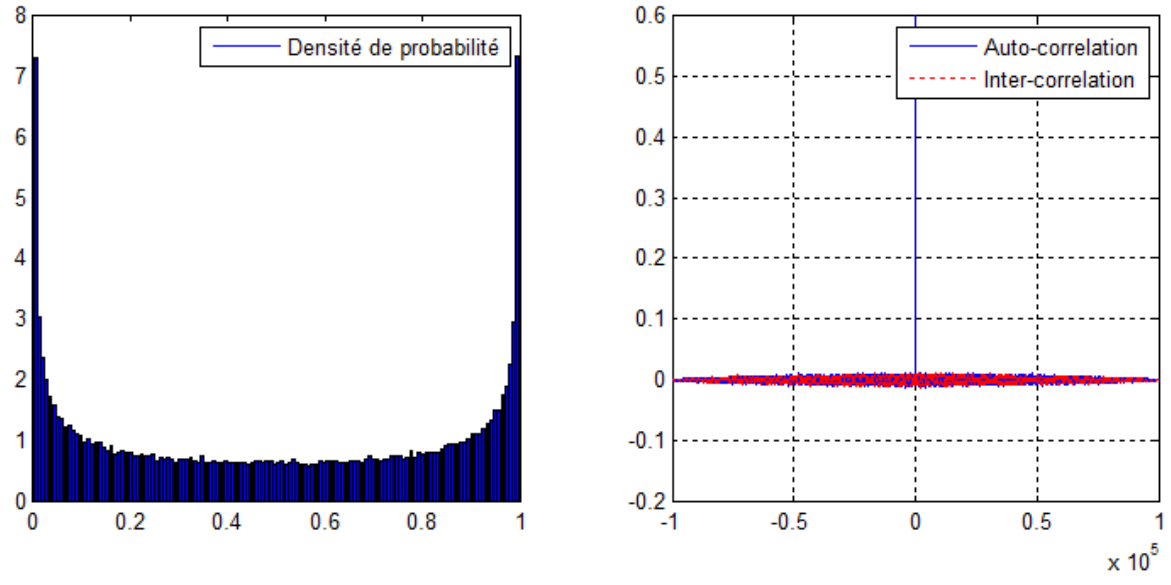

Figure.4.3- Simulation de la densité de probabilité et les fonctions d'auto/ inter-corrélation de la récurrence Logistique.

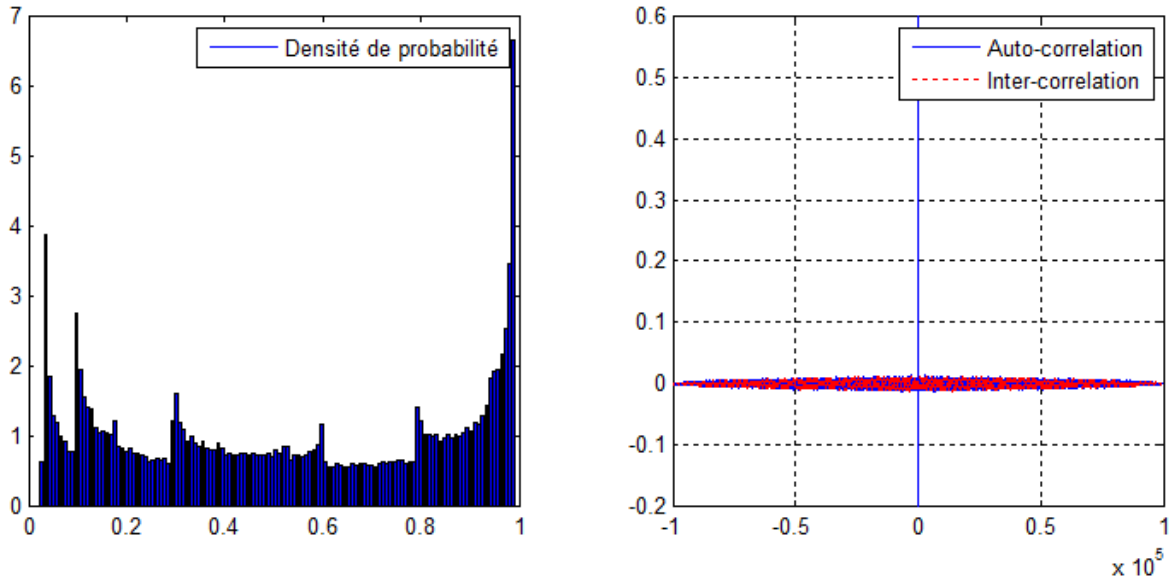

Figure.4.4- Simulation de la densité de probabilité et les fonctions d'auto/ inter-corrélation de la récurrence Sine.

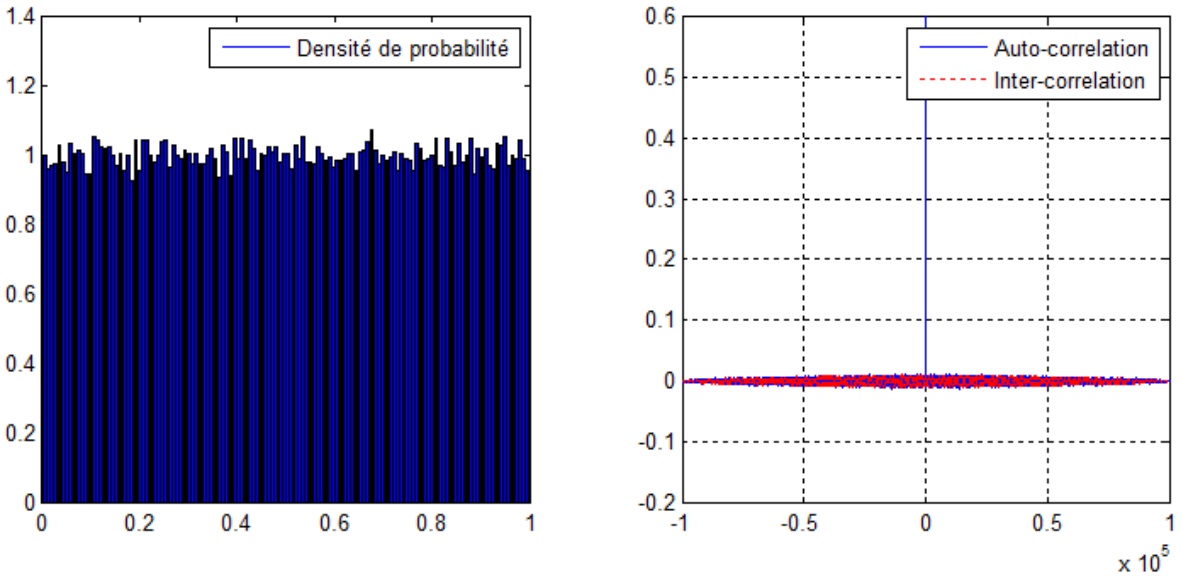

Figure.4.5- Simulation de la densité de probabilité et les fonctions d'auto/ inter-corrélation de la récurrence Skew-Tent.

2.3. Analyse du spectre de Lyapunov

Les systèmes dynamiques non-linéaires sont capables à générer plusieurs régimes dynamiques, y compris le chaos. Du point de vue de la cryptographie par chaos, seules les valeurs des paramètres de contrôle pour lesquelles le système dynamique se comporte chaotiquement sont retenues. L'identification des paramètres valides pouvant exhiber un comportement chaotique est effectuée à l'aide du spectre de Lyapunov.

En effet, la nature du spectre de Lyapunov d'un système dynamique caractérise quantitativement ce dernier. Ainsi, selon que le signe de l'exposant caractéristique de Lyapunov est négatif ou positif, il y'a stabilité ou instabilité locale des orbites issues de l'intégration du système. Si cet exposant est positif ($\lambda > 0$), alors il y a une sensibilité aux conditions initiales et le régime généré est chaotique.

Dans le cas des récurrences chaotiques considérées dans notre étude, l'exposant de Lyapunov λ est facilement calculable en fonction du paramètre de contrôle α, à partir de la formule (4.5), où f' est la dérivée de la i^{ème} itération de f [92].

$$\lambda = \lim_{t \to +\infty} \frac{1}{n} ln \sum_{i=0}^{n-1} ln\,|f'(x_i)|, \qquad i = 1 \dots n \qquad (4.4)$$

En faisant varier les valeurs des paramètres de contrôles dans les intervalles indiqués dans le tableau (4.1), avec un pas de 0.001, nous obtenons les spectres de lyapunov temporels illustrés dans les figures ci-dessous.

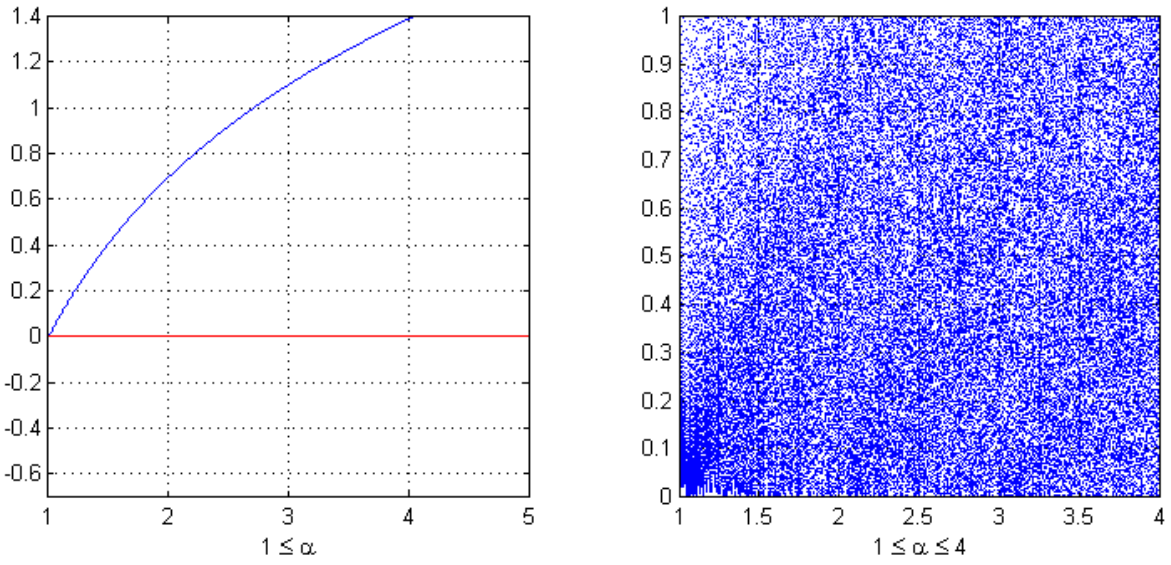

Figure.4.6- Spectre de Lyapunov et diagramme de bifurcation de la récurrence Bernoulli.

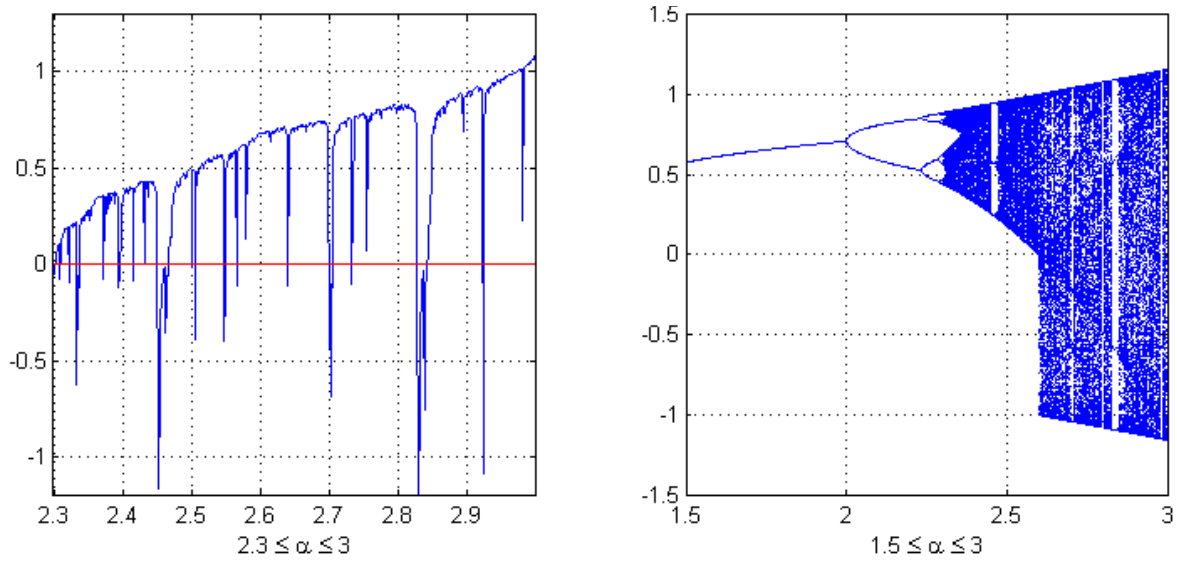

Figure.4.7- Spectre de Lyapunov et diagramme de bifurcation de la récurrence Cubique.

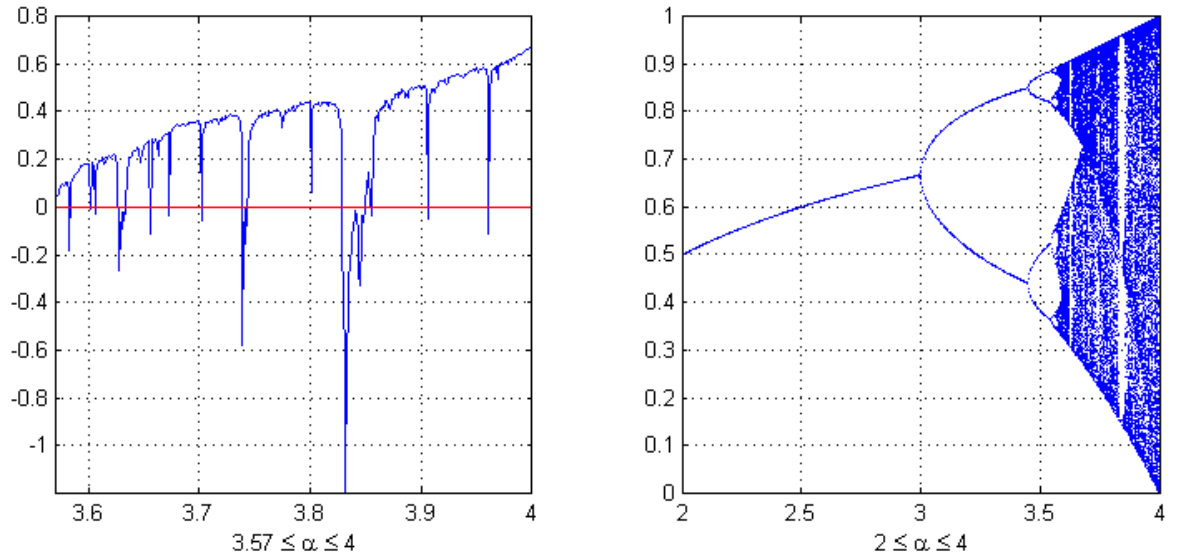

Figure.4.8- Spectre de Lyapunov et diagramme de bifurcation de la récurrence Logistique.

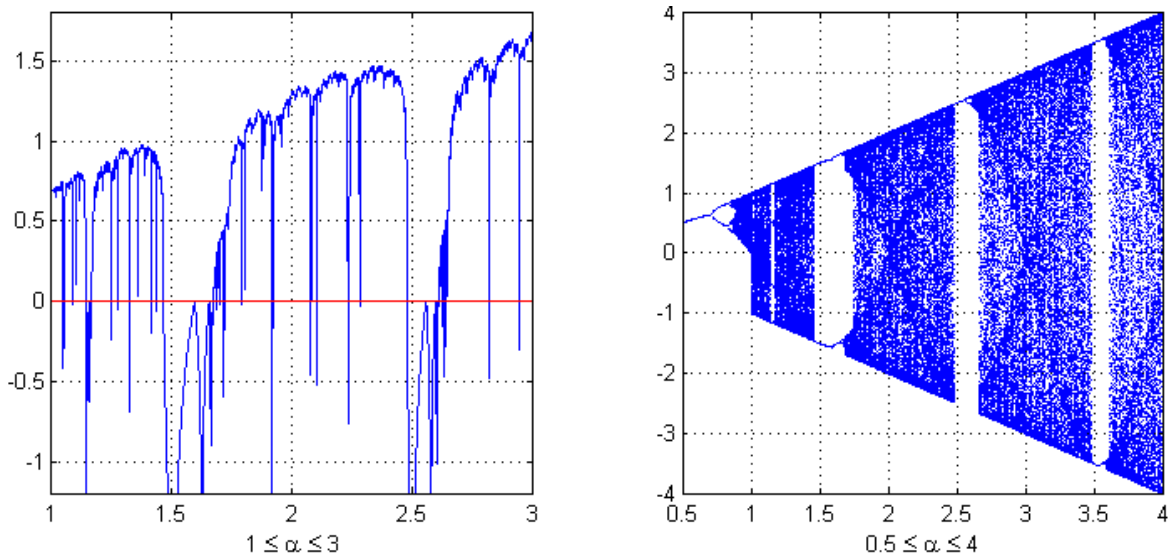

Figure.4.9- Spectre de Lyapunov et diagramme de bifurcation de la récurrence Sine.

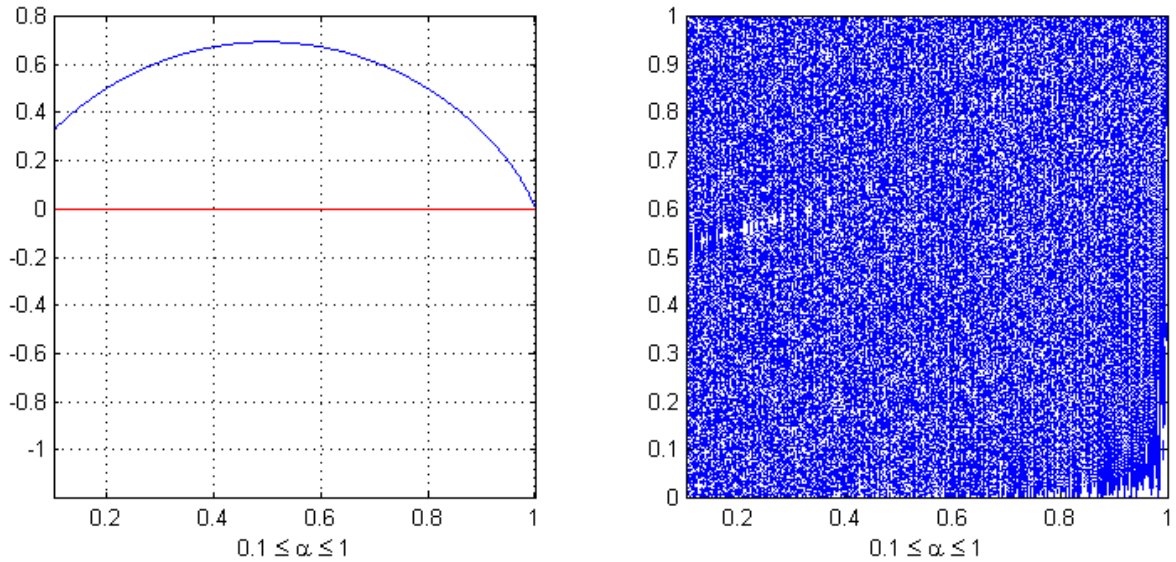

Figure.4.10- Spectre de Lyapunov et diagramme de bifurcation de la récurrence Skew-Tent.

Nous observons globalement d'après les figures ci-dessus que l'influence des variations paramétriques se traduit par le fait que les allures des courbes décrivant le spectre de Lyapunov sont dissemblables. En effet, pour la récurrence Skew-Tent et la récurrence Bernoulli, l'exposant de Lyapunov demeure positif pour toutes les valeurs de leurs paramètres critiques comprises dans les intervalles indiqués dans le tableau (4.1). Ce qui signifie que les comportements des deux systèmes sont toujours chaotiques. Ce qui n'est pas le cas pour le reste des récurrences, dont leurs courbes révèlent certaines irrégularités en incluant des valeurs nulles et négatives des exposants de Lyapunov. Par conséquent, les séquences générées par les récurrences : Cubique, Logistique et Sine ne sont pas toujours chaotiques à l'intérieur des intervalles indiqués.

L'impact du changement des valeurs des paramètres de contrôle sur la nature du comportement généré par chacune des récurrences étudiées est illustré par la visualisation graphique des diagrammes de bifurcation (détaillés dans l'annexe A). Nous remarquons d'après les figures ci-dessus qu'il existe une forte correspondance entre les spectres de Lyapunov et les digrammes de bifurcation pour toutes les récurrences. De ce fait, il est possible de fixer les valeurs optimales des paramètres de contrôle pour atteindre les régions chaotiques à travers les diagrammes de bifurcation.

2.4. Synthèse

Récurrence chaotique	Distribution uniforme	Indépendance statistique	Région chaotique
Bernoulli	✓	✓	✓
Cubique	×	✓	×
Logistique	×	✓	×
Sine	×	✓	×
Skew-Tent	✓	✓	✓

Tableau.4.2- Comparaison des performances des systèmes chaotiques unidimensionnels.

- Nous constatons à l'issu de cette étude comparative que tous les systèmes unidimensionnels étudiés sont capables à générer des comportements chaotiques ayant une très faible dépendance statistique (auto/inter-corrélation) ;

- Cependant, le comportement des trois récurrences (Cubique, Logistique et Sine) n'est pas tout à fait uniforme sur [0,1]. En outre, les intervalles des paramètres de contrôle pour lesquels les trois récurrences se comportent chaotiquement sont disjoints. Cette perte de chaoticité entraine une dégradation de la qualité des séquences générées, et une réduction de l'espace des paramètres valides, et par conséquent désencourage l'emploi de ces récurrences pour le chiffrement, car il peut causer de nombreuses failles de sécurité;
- Les récurrences : Skew-Tent et Bernoulli, qui appartiennent aux systèmes chaotiques linéaires par morceaux (PWLCM), possèdent de meilleures propriétés qualitatives et quantitatives. Les deux récurrences génèrent 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 (α>1) respectivement.

III. Algorithme proposé

L'algorithme que nous allons proposer est un algorithme de chiffrement par flux, qui exploite les séquences chaotiques produites par une récurrence Skew-Tent et deux récurrences Bernoulli, pour établir la synchronisation entre l'émetteur et le récepteur, et la génération des suites chiffrantes. La conception de l'algorithme en question se déroule ainsi en trois étapes suivant le principe du chiffrement par flux synchrone et le mécanisme général présenté dans le chapitre 3.

Posons:

f, g, et *h* les fonctions correspondantes aux récurrences Bernoulli et Skew-Tent respectivement;

Mi , Ci et *ki* dénotent le i^{ème} bit des données en clair, des données chiffrées et de la suite chiffrante respectivement ;

CIj les conditions initiales, où $i = 1, \ldots, N$, $j = 1, \ldots, 3$, et $\oplus$ désigne l'opération logique XOR.

3.1. Initialisation des systèmes chaotiques

L'algorithme proposé prend en entrée la clé secrète formée des paramètres critiques des trois récurrences chaotiques employées: $\{\alpha_1, \alpha_2, \alpha_3\}$ et une condition initiale CI, sélectionnée aléatoirement. La récurrence Skew-Tent est considérée comme un système maître, qui a pour

rôle de générer le vecteur d'initialisation à partir de CI. Ce vecteur de taille L bits ($25 < L < 50$) est envoyé directement à travers un canal publique pour établir la SDM synchronisation avec le récepteur, selon l'approche par itération en arrière expliquée au chapitre précédent.

Une fois la synchronisation établie, l'initialisation des trois récurrences chaotiques est effectuée en calculant trois nouvelles conditions initiales (une pour chaque récurrence chaotique), d'une manière circulaire comme indiqué par l'algorithme ci-dessous.

Algorithme d'initialisation
Entrée : $CI,\ \alpha_1,\ \alpha_2,\ \alpha_3$
Sortie : CI_1, CI_2, CI_3
$CI_1 \leftarrow\ f(CI,\ \alpha_1)$
$CI_2 \leftarrow\ g(CI_1, \alpha_2)$
$CI_3 \leftarrow h(CI_2, \alpha_3)$

Cette première étape sert à distribuer la sensibilité à la condition initiale partagée CI sur le comportement des trois systèmes chaotiques utilisés, en vue d'augmenter l'immunité du cryptosystème contre les attaques par resynchronisation.

3.2. Génération des suites chiffrantes

Les séquences chaotiques générées à partir de la récurrence Skew-Tent et des récurrences Bernoulli, après leur initialisation, seront combinées pour produire un bit pseudo-aléatoire à chaque cycle d'horloge suivant l'algorithme présenté ci-dessous.

Générateur de nombres pseudo-aléatoires
Entrée : $CI_1, CI_2, CI_3, \alpha_1, \alpha_2, \alpha_3$
Sortie : k_i
$x_i \leftarrow\ f^i(CI_1, \alpha_1)$
$y_i \leftarrow\ g^i(CI_2, \alpha_2)$
$z_i \leftarrow\ h^i(CI_3, \alpha_3)$
$k_i \leftarrow\ s(x_i) \oplus s(y_i)$
si $s(z_i) = 0$ **alors** permuter (x_i, z_i)
sinon permuter (y_i, z_i)

L'originalité du générateur de nombres pseudo-aléatoires proposé réside dans la perturbation des récurrences chaotiques suivant la récurrence Skew-Tent. Il s'agit de permuter l'état de la récurrence Skew-Tent avec celui de la première récurrence Bernoulli si le symbole de correspondant vaut 0. Ou bien de le permuter avec l'état de la deuxième récurrence Bernoulli dans le cas contraire (symbole=1). La nature chaotique de cette perturbation améliore significativement l'aspect aléatoire des séquences générées. Notant que toutes les séquences chaotiques utilisées dans notre générateur sont converties en séquences binaires suivant la représentation par dynamique symbolique, en considérant les états critiques $x_c = \alpha_3$ pour la récurrence Skew-Tent et $x_c =$ ½ pour les deux récurrences Bernoulli.

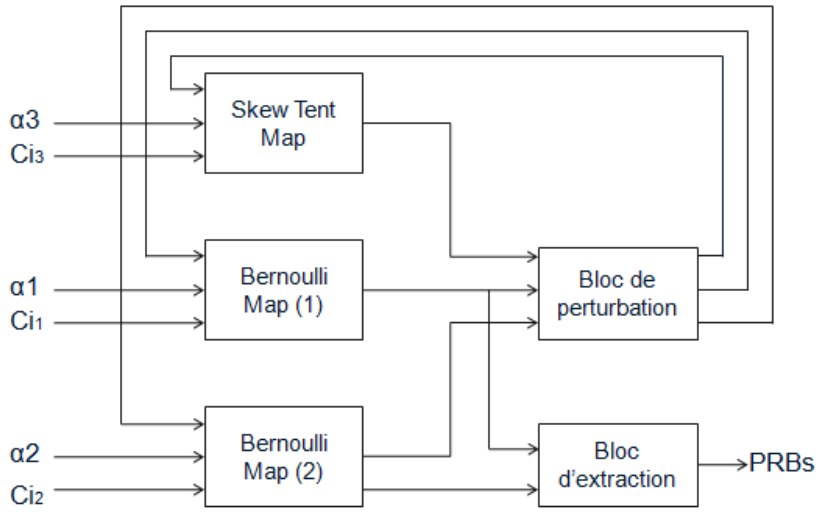

Figure.4.11- Structure interne du générateur de nombres pseudo-aléatoires proposé.

3.3. Procédure de chiffrement/déchiffrement

Le cryptosystème proposé appartient à la catégorie du chiffrement par flux additif, pour laquelle le procédé de chiffrement se fait simplement par l'opérateur "XOR" entre les données confidentielles et la suite chiffrante. Quant au procédé de déchiffrement est effectué de manière similaire.

$$Ci = Mi \oplus Ki$$

$$Mi = Ci \oplus Ki$$

En effet, le partage efficace de la condition initiale via l'approche de synchronisation par dynamique symbolique permet la régénération des séquences binaires utilisées par l'émetteur de manière synchrone et sans erreurs par le récepteur légitime. Ainsi, le déchiffrement des

données confidentielles peut être mené progressivement durant la réception des flux chiffrés en xorant en temps réel les bits chiffrés reçus avec les bits de la suite chiffrante régénérée à la réception. Ainsi, l'émetteur et le récepteur doivent utiliser des systèmes chaotiques identiques avec la même configuration paramétrique, puisque leurs paramètres constituent la clé secrète du cryptosystème. Le diagramme de la figure (4.11) décrit l'architecture interne du générateur de nombres pseudo-aléatoires considéré, tandis que la figure (4.12) illustre la structure complète du cryptosystème proposé.

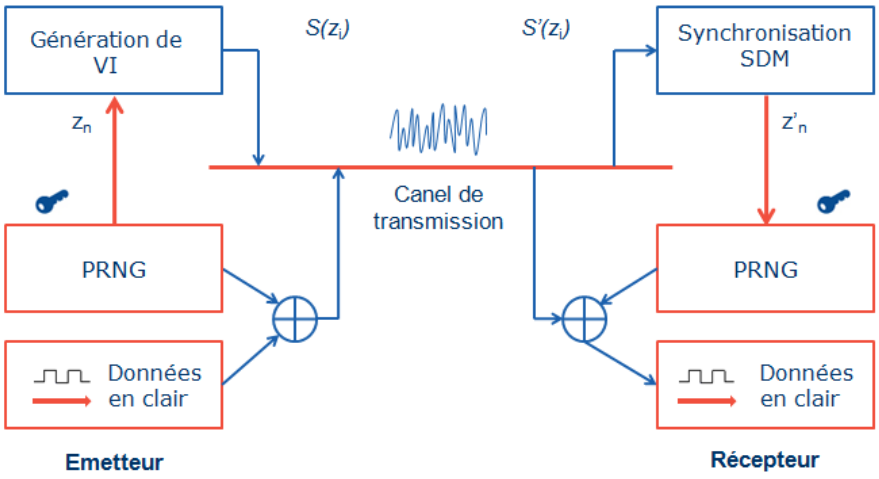

Figure.4.12- Description schématique du cryptosystème proposé.

IV. Évaluation du cryptosystème proposé

L'utilité principale des cryptosystèmes symétriques est de prévenir un récepteur non autorisé de déchiffrer un message confidentiel, sans possession de la clé secrète, étant l'élément sur lequel repose toute la sécurité du cryptosystème d'après Kerckhoffs [93]. Néanmoins, pour évaluer la sécurité d'un cryptosystème symétrique il est souvent nécessaire de se mettre à la place de l'adversaire, en étudiant des probabilités de succès des attaques possibles, afin de déterminer ses éventuelles faiblesses. De ce fait, on dit qu'un cryptosystème est résistant à une certaine attaque si celle-ci a une complexité qui dépasse 2^k en temps ou en mémoire, où k est la taille de la clé secrète. Toutefois, la réussite pratique d'une attaque dépend d'un certain nombre d'éléments, comme les connaissances nécessaires à priori, l'effort demandé (complexité, temps de calcul), la quantité et la qualité des informations pouvant être déduites de l'attaque.

En ce qui concerne les algorithmes de chiffrement par flux synchrones, la sécurité du chiffrement est entièrement déterminée par les propriétés statistiques et la complexité des générateurs de nombres pseudo-aléatoires, du fait de la simplicité de leur mode de fonctionnement surtout le mode asynchrone, et leur mécanisme déterministe. Dans ce qui suit nous allons tester la résistance de notre cryptosystème aux attaques les plus fréquentes qui peuvent avoir lieu contre les algorithmes de chiffrement par flux.

4.1. Analyse statistique

Tests statistiques	P-valeur	Taux de succès (%)
Frequency	0.455937	100
Block frequency (m = 128)	0.657933	100
Cumulative sums Forward	0.075719	100
Cumulative sums Reverse	0.334538	99
Runs	0.062821	99
Long runs of one's	0.437274	100
Binary Matrix Rank	0.455937	99
Spectral DFT	0.816537	100
No overlapping templates (m = 9)	0.983453	100
Overlapping templates (m = 9)	0.474986	98
Universal (L = 7,Q = 1280,K = 41577)	0.637119	99
Approximate entropy (m = 10)	0.816537	100
Random excursions	0.867692	100
Random excursions variant	0.897763	100
Serial (m=16) P-value1	0.699313	99
Serial (m=16) P-value2	0.851383	100
Linear complexity (M = 500)	0.574903	99

Tableau.4.3- Résultats des tests statistiques de NIST SP800-22.

La majorité des attaques menées contre les algorithmes de chiffrement par flux vise à détecter et exploiter les faiblesses liées aux générateurs de nombres pseudo-aléatoires employés, à travers l'analyse statistique des suites chiffrantes. 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 100 séquences pseudo-aléatoires de taille 10^6 bits, générées à partir des conditions initiales et des paramètres aléatoires. Les résultats présentés dans le tableau (4.3) 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= 96 %). Ce qui signifie que le générateur de nombres pseudo-aléatoires proposé produit des séquences indistinguables de vraies séquences aléatoires.

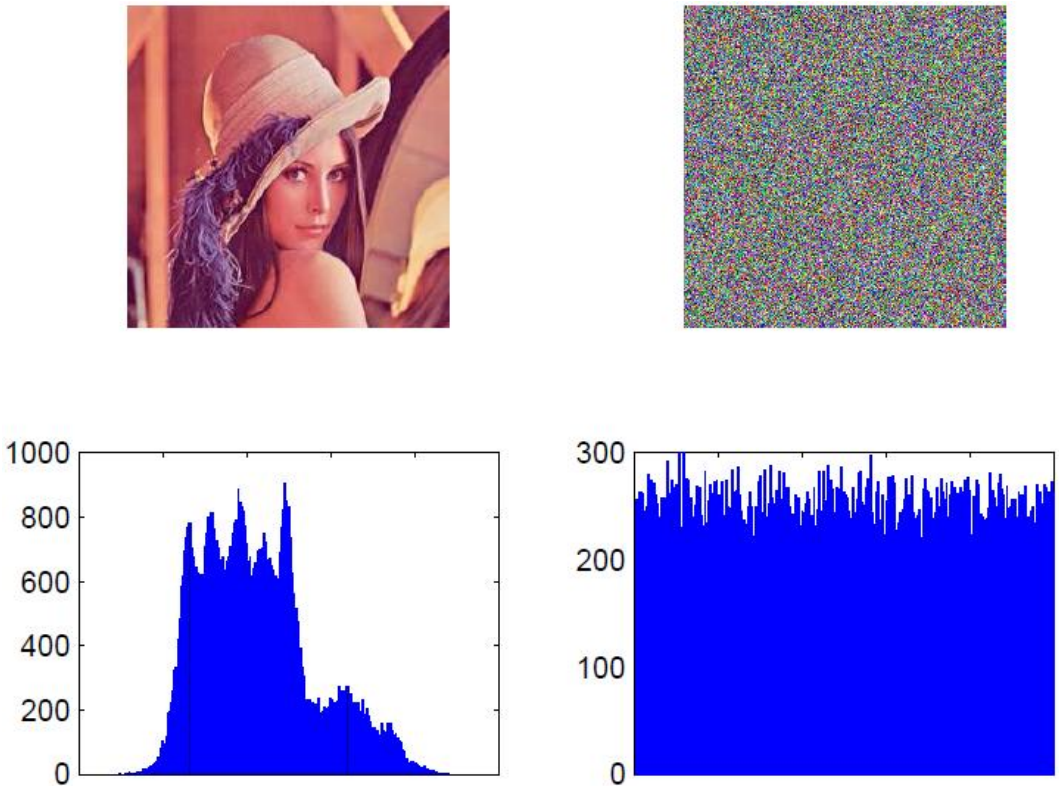

Figure.4.13- Visualisation des histogrammes de l'image originale et chiffrée.

De plus, l'application de la suite chiffrante générée à partir la clé secrète : $\{\alpha_1 = 2.98145364517528;\ \alpha_2 = 3.73092518472690;\ \alpha_3 = 0.67928153074916\}$ et la condition initiale $CI = 0.3725$; dans le chiffrement de l'image : "lena.jpg" donnée dans la figure (4.13), produit une image chiffrée avec un haut niveau de confusion, comme indiqué

par la visualisation des histogrammes de la figure (4.13), et les mesures d'entropie et de corrélation données dans le tableau (4.4).

	Image originale	**Image chiffrée**
Entropie	7.5376	7.9992
Corrélation verticale	0.9799	-0.0014
Corrélation horizontale	0.9453	9.38e-04
Corrélation diagonale	0.9211	1.93e-05

Tableau.4.4- Mesures d'entropie et de corrélation entre l'image originale et chiffrée.

D'après ces résultats, nous pouvons conclure que le générateur de nombres pseudo-aléatoires proposé est cryptographiquement sûr, de sorte qu'aucune prédiction statistique ne peut avoir lieu. Ce qui rend les attaques à texte chiffré seul, pour lesquelles on ne connaît aucune information sur le clair, inefficaces contre notre cryptosystème.

4.2. Estimation de l'espace de la clé secrète

La taille de la clé secrète d'un algorithme de chiffrement est le total des clés différentes qui peuvent paramétrer la procédure de chiffrement et/ou déchiffrement. Vu que la taille de la clé secrète est directement liée au niveau de sécurité d'un cryptosystème symétrique, il est recommandé d'utiliser des clés de taille typiquement supérieure à 128 bits pour prévenir les attaques à force brute. En effet, l'intégration de trois récurrences chaotiques avec différents paramètres critiques dans le cryptosystème proposé est dans le but d'améliorer la qualité des séquences générées d'une part, et d'augmenter la taille de la clé secrète, qui correspond à leurs paramètres critiques, d'autre part.

L'arithmétique et la précision de calcul adoptées pour l'implémentation des systèmes chaotiques utilisés dans notre algorithme constituent dans ce cas des facteurs déterminants dans l'estimation de la taille de la clé secrète. En considérant une approximation des orbites chaotiques générées en nombres réels à virgule fixe, avec 64 bits alloués à chaque paramètre (deux bits pour la partie entière et 60 bits pour la partie décimale), la taille de la clé secrète obtenue (180 bits) sera largement suffisante pour garantir une sécurité calculatoire.

De plus, l'emploi de l'approche de synchronisation par dynamique symbolique pour le partage de la condition initiale permet la définition des clés secrètes dynamiques, c'est-à-dire rendre une clé secrète réutilisable de nombreuses fois.

4.3. Attaque à texte clair connu

Pour évaluer la sécurité d'un algorithme de chiffrement par flux, on se place usuellement dans le contexte d'une attaque à texte clair connu, en raison du fort potentiel d'extraction d'informations secrètes et critiques à partir des suites chiffrantes divulguées. Cette attaque est très robuste contre les cryptosystèmes chaotiques, car elle permet, à travers la seule observation des échantillons des séquences chaotiques, de discerner quelques informations sur les systèmes chaotiques employés, et les utiliser par la suite pour identifier leurs paramètres secrets et leurs conditions initiales [94] [95], spécialement quand la suite chiffrante correspond à la sortie directe du générateur chaotique.

La structure de notre générateur de nombres pseudo-aléatoires a été conçue de manière à ne pas fournir aucune information à propos les systèmes chaotiques employés :

- La sortie du générateur de nombres pseudo-aléatoires proposé dépend de plusieurs récurrences chaotiques;
- Toutes les séquences chaotiques intervenant à la génération des suites chiffrantes sont converties en séquences dynamiques symboliques, qui fournissent une description partielle des orbites chaotiques correspondantes;
- Les séquences dynamiques symboliques des trois systèmes chaotiques sont décorrélées entre elles et uniformément distribuées, ce qui rend très difficile de repérer leurs valeurs à partir de la seule observation des suites chiffrantes;
- La technique de perturbation adoptée affecte les comportements des trois récurrences chaotiques utilisées, ce qui permet non seulement de résoudre le problème de dégradation des dynamiques chaotiques suite à leur binarisation, mais aussi d'assurer de meilleures propriétés statistiques.

D'où, la considération des attaques à texte clair connu ne présente aucune menace pour le cryptosystème proposé, car l'observation des suites chiffrantes utilisées ne fournit aucune information utile concernant les états réels ou les paramètres critiques des systèmes chaotiques employés.

4.4. Attaque différentielle

La notion d'attaque différentielle émerge de la cryptanalyse des algorithmes de chiffrement par bloc, d'où elle est considérée souvent dans le cadre d'attaque à texte clair choisi. Son principe consiste à étudier le comportement différentiel de l'algorithme de chiffrement, en

vue d'analyser les changements remarquables dans le texte chiffré résultant. C'est-à-dire comment pour des couples de clairs de différence donnée et bien choisie, cette différence initiale se propage au cours du calcul de la fonction de chiffrement, et laisse déduire des informations critiques.

Dans le contexte du chiffrement par flux additif, dans lequel le processus de chiffrement est indépendant du texte clair, l'analyse différentielle est centrée autour du générateur de nombres pseudo-aléatoires utilisé, et sa sensibilité au vecteur d'initialisation qui peut être manipulé par des attaquants dans certaines situations. De ce fait, le générateur de nombres pseudo-aléatoires doit exhiber un haut niveau de diffusion pour pouvoir résister à ce genre d'attaques.

Afin de quantifier le niveau de diffusion du générateur de nombres pseudo-aléatoires proposé nous avons fait changer légèrement la valeur de la condition initiale, et l'un des paramètres de la clé secrète séparément, puis calculer le taux de différence des suites chiffrantes résultantes selon la formule suivante [96]:

$$Taux = \frac{Diff(K, K1) + Diff(K, K2)}{2 \times N} \times 100\ \% \qquad (4.5)$$

Où $Diff(K, K_1)$ et $Diff(K, K_2)$ dénotent le nombre de bits différents entre le flux binaire référence K, généré à partir de la condition initiale $Ci = 0.2915683749$ et la clé secrète : $\{\alpha_1 = 2.9987938562;\ \alpha_2 = 3.0057031642;\ \alpha_3 = 0.6573629815\}$, et ceux modifiés légèrement K_1 et K_2 de taille $N = 10^6$. Les modifications appliquées à K_1 et K_2 résident dans des conditions initiales différentes (paramètres secrets différents): $Ci + \Delta Ci$ et $Ci - \Delta Ci$ (respectivement $\alpha_1 + \Delta\alpha_1$ et $\alpha_1 - \Delta\alpha_1$), avec $\Delta Ci = \Delta\alpha_1 = 10^{-15}$.

Pour le générateur de nombres pseudo-aléatoires proposé une légère variation des conditions initiales ou de n'importe quel paramètre secret affecte les orbites des trois récurrences chaotiques utilisées, en introduisant une modification importante dans les flux binaires obtenus avec un taux de changement $\approx 50\ \%$, satisfaisant le critère d'avalanche stricte qui s'énonce comme suit [97] :

Une fonction qui satisfait le critère d'avalanche stricte est telle que tout inversement d'un bit en entrée doit avoir une chance sur deux de modifier chaque bit de sortie, ce qui permet d'uniformiser les sorties.

En outre, l'application des suites chiffrantes : K, K_1 et K_2 dans le chiffrement de l'image de lena.jpg (figure. 4.13), produit des images chiffrées différentes avec un taux de différence

qui vaut 99.6231 % pour le changement de la condition initiale et 99.6276 % pour le changement du paramètre secret. En effet, la forte sensibilité des systèmes chaotiques aux conditions initiales et aux paramètres de contrôle assure l'immunité du cryptosystème proposé contre l'attaques différentielle, qui possède dans ce cas une efficacité équivalente à une attaque à texte clair connu.

4.5. Attaque par resynchronisation

Les algorithmes de chiffrement par flux basés sur des vecteurs d'initialisation sont très adaptés à l'échange fréquent des trames de petite taille, comme c'est le cas pour les communications téléphoniques. Toutefois, le caractère public des vecteurs d'initialisation rend possible de monter des attaques, dites par resynchronisation, qui agissent principalement sur les protocoles d'initialisation.

L'utilisation de l'approche de synchronisation par dynamique symbolique dans le cryptosystème proposé permet d'exploiter efficacement les deux principales caractéristiques des systèmes chaotiques, à savoir la sensibilité aux conditions initiales et le déterminisme, contre de telles attaques:

- D'un côté, le vecteur de synchronisation généré à partir de la récurrence Skew-Tent sert à partager la condition initiale CI, qui sera utilisée par la suite dans l'initialisation des trois récurrences chaotiques indirectement suivant la procédure décrite auparavant. De cette façon, même si un attaquant intercepte ce vecteur il ne sera pas en mesure d'établir la synchronisation sans une connaissance exacte des paramètres des trois systèmes chaotiques;
- Cependant, la condition initiale CI doit être changée régulièrement, typiquement lors de chaque nouvelle session, pour éviter les exploitations malicieuses du vecteur de synchronisation et éliminer les éventuelles collisions. La forte sensibilité des systèmes chaotiques est très utile à cet effet, puisque toute perturbation de la condition initiale se traduit par une trajectoire tout à fait divergente, et par conséquent empêche la prédiction des bits de la suite chiffrante, avec une probabilité raisonnable, via les outils statistiques conventionnels. Notant que pour estimer la condition initiale, sans connaissance préalable des paramètres critiques, le nombre de bits nécessaire et la complexité de l'attaque deviennent extrêmement grands, ce qui rend l'attaque inopérante;

- D'un autre côté la synchronisation très rapide entre l'émetteur et le récepteur (seulement quelques bits suffisent à la synchronisation) constitue un des avantages permettant d'envisager des transmissions sécurisées haut débit. Quant à la nature déterministe des systèmes chaotiques permet au récepteur légitime de générer la suite pseudo-aléatoire nécessaire au déchiffrement de manière exacte, ce qui simplifie significativement la resynchronisation en cas de perte de synchronisation.

4.6. Analyse de la sensibilité au bruit

À la différence des algorithmes de chiffrement par bloc, les algorithmes de chiffrement par flux synchrone ne propagent pas les erreurs de transmission, et offrent généralement de bonnes performances même dans des faibles SNR, du fait qu'ils chiffrent chaque octet (ou bit) individuellement.

Par ailleurs, il a été montré dans [84] que l'utilisation de la synchronisation par dynamique symbolique dans les transmissions numériques par chaos permet de limiter la quantité de bruit ajoutée lors de la transmission, et de conserver pratiquement une qualité de décodage avec un taux d'erreurs binaires (TEB) similaire à celui d'une modulation BPSK. De ce fait, même lorsque le signal reçu est corrompu par un bruit blanc gaussien additif tel que S(X) = S(X + W), les séquences dynamiques symboliques restent détectables, de sorte que le vecteur d'initialisation reçu peut être estimé correctement à l'aide d'un simple filtre adapté. L'évaluation de la performance de notre cryptosystème en termes de TEB et de la corrélation mesurée entre l'image en clair (figure .4.13) et les images déchiffrées obtenues dans différents SNR est donnée dans le tableau (4.5).

Une fois la synchronisation établie, le récepteur légitime sera en mesure de générer la même suite chiffrante utilisée dans le chiffrement d'une manière déterministe, dont le timing du processus de déchiffrement est contrôlé par le signal d'horloge. Ce qui assure une haute qualité de synchronisation avec une faible complexité. Néanmoins, le processus de déchiffrement échouera complètement lorsque la condition initiale ou la clé secrète ne soit pas correcte. Par exemple, si nous essayons de déchiffrer l'image de la figure (4.13) avec la même condition initiale $CI = 0.3725$ et la même clé secrète utilisée dans le chiffrement: $\{\alpha_1 = 2.98145364517528;\ \alpha_2 = 3.73092518472690;\ \alpha_3 = 0.67928153074916\}$, en introduisant seulement une variation de l'ordre de 10^{-15} à l'un des paramètres de la clé secrète ($\alpha_2 = 3.730925184726901$), nous obtenons une image erronée tout à fait décorrélée

avec l'image originale (corrélation entre l'image originale et l'image déchiffrée = -0.0025), comme montré dans la figure (4.14).

SNR	TEB	Corrélation
5	0.0376	0.8888
7	0.0125	0.9610
10	$7.6625e-004$	0.9975
12	$3.1275e-005$	0.9998
15	0	1

Tableau.4.5- Le taux d'erreurs binaires et la corrélation mesurée entre l'image originale et les images déchiffrées obtenues pour différents SNR.

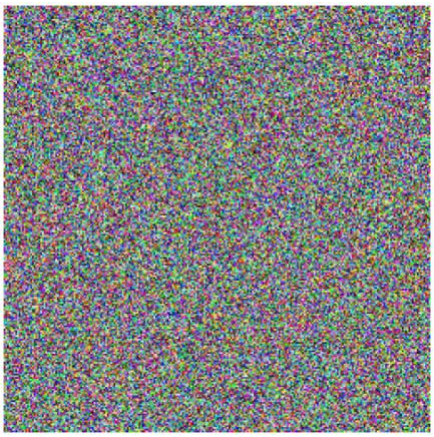

Figure.4.14- Sensibilité au changement à la clé secrète : Image déchiffrée par une clé secrète légèrement différente.

V. Analyse comparative

Les algorithmes de chiffrement par flux sont destinés essentiellement aux transmissions temps réel. À cet effet, l'exploitation des systèmes chaotiques dans le cryptosystème proposé a été fortement optimisée dans ce contexte, en tenant compte de l'efficacité d'initialisation et de génération des bits pseudo-aléatoires d'une part, et du niveau de sécurité d'autre part.

5.1. Clé secrète et initialisation

La taille de la clé secrète du cryptosystème proposé varie de 90 bits en simple précision jusqu'à 180 bits en double précision, et dépasse donc la taille des clés secrètes supportées par

la plupart des algorithmes de chiffrement par flux conventionnel comme indiqué dans le tableau (4.6).

En outre, l'initialisation des systèmes chaotiques dans l'algorithme proposé se fait par une seule condition initiale CI choisie au hasard et partagée via un vecteur d'initialisation selon l'approche de synchronisation par dynamique symbolique. L'impact de cette étape sur la performance de l'algorithme est négligeable, et elle est nettement plus efficace par rapport aux standards de chiffrement par flux conventionnel, dont leurs procédures d'initialisation sont plus rigoureuses et requièrent des mises à jour sur plusieurs cycles avant de commencer la génération des suites chiffrantes [98] [99]. Ces traitements semblent trop pénalisant pour permettre un chiffrement/ déchiffrement suffisamment rapide pour des transmissions en temps réel.

5.2. Niveau de sécurité

Malgré que les algorithmes de chiffrement par flux présentent de meilleurs performances par rapport aux algorithmes de chiffrement par bloc, mais l'efficacité de leur conception affecte souvent leur niveau de sécurité. Ainsi, la plupart des algorithmes communément utilisés se sont avérés vulnérables à certains types d'attaques, principalement à cause de la faible complexité des générateurs de nombres pseudo-aléatoires utilisés. Parmi les attaques les plus répondues nous citons : l'attaque par distingueur [100], linéaire [101] et par corrélation [102].

Toutefois, l'efficacité de ces attaques contre le cryptosystème à base du chaos proposé n'est pas du tout évidente, en raison de la structure du générateur de nombres pseudo-aléatoires adoptée, qui intègre trois systèmes chaotique avec un procédé de perturbation. De plus, la forte sensibilité des systèmes chaotiques aux variations empêche toute prédiction statistique des séquences symboliques intervenant à la génération des suites chiffrantes, à travers l'étude probabiliste des flots de sortie.

5.3. Efficacité d'exécution

Compte tenu que le fonctionnement des algorithmes de chiffrement par flux synchrones consiste à xorer les données confidentielles avec la suite chiffrante, leur performance en terme de temps d'exécution dépend du chemin critique du générateur de nombres pseudo-aléatoires adopté, que ce soit pour le chiffrement ou le déchiffrement.

En effet, le choix judicieux des systèmes chaotiques, qui ne nécessitent pas une grande puissance de calcul, et la combinaison de leurs séquences chaotiques via l'opérateur xor pour

produire un seul bit à chaque cycle d'horloge, permettent une exécution relativement efficace de l'algorithme proposé, tant au niveau logiciel que matériel. Nous envisagerons une étude plus détaillée de la performance de notre cryptosystème dans le chapitre suivant.

Algorithme	**Clé secrète (bits)**	**Vecteur d'initialisation**	**Structure du générateur de bits pseudo-aléatoires**	**Initialisation**
Algorithme proposé	90- 180	25- 50	Combinaison de trois systèmes chaotiques unidimensionnels	1 cycle
A5/1	64	22	Combinaison par addition de trois registres à décalage à rétroaction linéaire	188 cycles
E0	128	64	Combinaison de quatre registres à décalage à rétroaction linéaire	239 cycles
Grain	80- 128	64- 80	Combinaison de deux registres à décalage à rétroaction linéaire et non-linéaire	256 cycles
RC4	40- 256	-	Combinaison de deux tables d'états à 256 octets	768 cycles
Trivium	80	80	Combinaison de trois registres à décalage à rétroaction non-linéaire	1152 cycles

Tableau.4.6- Comparaison entre le cryptosystème proposé et les standards de chiffrement par flux.

V. Conclusion

Nous avons tenté à travers ce chapitre de montrer comment la description des systèmes chaotiques en dynamique symbolique peut conduire à des contributions primordiales dans le contexte du chiffrement par flux, à travers la proposition d'un nouvel algorithme qui s'appuie sur l'intégration de trois systèmes chaotiques unidimensionnels. Rappelons que nous avons choisi les deux récurrences chaotiques Bernoulli et Skew-Tent en raison de leurs bonnes performances démontrées par l'étude comparative menée dans la deuxième section de ce chapitre. Ainsi, des mécanismes originaux ont été considérés lors de la conception de notre

algorithme, afin d'exploiter parfaitement les propriétés des récurrences chaotiques utilisées et leur description symbolique.

Par ailleurs, l'analyse de sécurité présentée dans la troisième section de ce chapitre démontre que le générateur de nombres pseudo-aléatoires proposé est cryptographiquement sûr, de manière à rendre les attaques classiques ciblant les algorithmes de chiffrement par flux inopérantes. Nous avons prouvé également que l'algorithme en question assure de meilleures propriétés en comparant ses performances avec les standards de chiffrement par flux. Ces résultats nous ont incités à implémenter notre algorithme sur un composant FPGA afin d'estimer sa performance au niveau hardware. Cette étude fera l'objet du chapitre suivant.

Chapitre5 : Implémentation de l'algorithme proposé sur FPGA

I. Introduction

Malgré le grand nombre des algorithmes de chiffrement par chaos proposés dans littérature, leur mise en pratique reste un domaine peu exploré. En effet, les études de performance des algorithmes proposés dans ce contexte se limitent la plupart du temps à la simulation, sans aborder leurs implantions matérielles sur des composants numériques. Certes la simulation est une étape importante pour déboguer les codes et estimer leurs performances, mais reste néanmoins limitée, et souffre de plusieurs inconvénients tels que les hypothèses et les approximations qui nuisent parfois à la précision. Pour cette raison, nous nous sommes orientés dans ce dernier chapitre vers une implémentation matérielle de l'algorithme de chiffrement par flux décrit dans le chapitre précédent sur un circuit reconfigurable FPGA de type Spartan-XC6LX16 de Xilinx.

En outre, étant donné que la conception des algorithmes de chiffrement sur les circuits FPGA soulève un vrai challenge, concernant l'optimisation de l'implémentation en termes de sécurité, de flexibilité et de performance, il arrive parfois aux concepteurs de proposer plusieurs variantes d'un même algorithme de chiffrement ayant des propriétés d'efficacité et de sécurité différentes, pour satisfaire aux exigences des différentes applications, et atteindre le bon compromis entre un algorithme très sûr, mais très lent et un algorithme extrêmement efficace, mais pour lequel la prise de risque en matière de sécurité est plus grande. De notre côté nous proposons dans ce chapitre une variante de l'algorithme de chiffrement proposé appropriée pour une implémentation matérielle, en lui apportant de légères modifications en vue d'optimiser sa performance. Il s'agit du nombre de bits pseudo-aléatoires générés par chaque cycle d'horloge et l'arithmétique adoptée.

Les résultats de notre implémentation nous ont servi à une étude comparative entre l'algorithme proposé et les principaux standards de chiffrement par flux, afin de mettre en

évidence les avantages apportés par l'application des systèmes chaotiques au chiffrement par flux.

II. Environnement du travail

Les FPGAs (Field-Programmable Gate Arrays) ou réseaux logiques programmables sont une famille de composants programmables depuis un programme appelé "bitstream". Ce dernier n'est pas destiné à être exécuté par un microprocesseur, mais plutôt à configurer des portes logiques et les relier entre elles selon une logique d'interconnexion, pour répondre à un objectif bien déterminé.

De part, la possibilité d'être reconfigurés dans leur totalité et leur haut degré de parallélisme et de flexibilité, les FPGAs sont devenus les plus populaires en matière d'implantation et de prototypage des circuits numériques, pour un bon nombre d'applications, y compris les applications cryptographiques [103]. 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 algorithme de chiffrement par flux 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. Les caractéristiques du Spartan-XC6LX16 sont les suivantes:

- **12278** slices (éléments logiques) contenant chacun quatre LUT 6-entrée et huit bascules (Filp Flops);
- **576** Kbits bloc de RAM rapide;
- **2** tuiles d'horloge (quatre RDR et deux PLL) ;
- **32** slices DSP;
- **500** MHz vitesses d'horloge.

2.1. Méthodologie de conception

Le processus de conception d'un circuit numérique sur d'un composant FPGA s'appuie sur l'utilisation d'un outil CAO (Conception Assistée par Ordinateur) qui, à partir d'une description sous forme graphique (approche schématique) ou par langage HDL (approche textuelle), génère le schéma logique capable de reproduire le fonctionnement logique décrit.

Ainsi, la réalisation d'un circuit donné se fera sous le contrôle d'un ensemble de directives en utilisant les ressources disposées par la technologie cible.

En effet, la structure mathématique des systèmes chaotiques utilisés au sein du générateur de nombres pseudo-aléatoires proposé nous impose l'utilisation de l'approche textuelle basée sur le langage de description matériel VHDL, liée davantage aux processus algorithmiques.

Par ailleurs, une démarche qui passe par une description dite de haut niveau sera considérée lors de la conception de notre cryptosystème, du fait qu'elle ne nécessite pas des connaissances spécifiques de la technologie de réalisation du composant ciblé.

2.2. Définition (*Langage VHDL*)

VHDL l'abréviation anglaise de «VHSIC Hardware Description Langage » est un langage formel pour la spécification des systèmes digitaux, aussi bien au niveau comportemental que structurel.

De nos jours, le langage VHDL devient un outil de description indispensable pour le développement des systèmes électroniques intégrés, en raison des fonctionnalités qu'il offre:

- Portabilité des descriptions VHDL sur n'importe quel composant ou structure, indépendamment des compilateurs de silicium des différents fournisseurs de FPGA;
- Possibilité d'aborder les modèles à différents niveaux d'abstraction, à savoir les abstractions comportementales, structurelles et flot de données;
- Conception de haut niveau qui ne suit plus la démarche descendante habituelle (du cahier des charges jusqu'à la réalisation et le calcul des structures finales) mais qui se limite à une description comportementale issue directement des spécifications techniques du produit visé ;
- Simplification de la conception par la création des composants, des paquetages et des modèles de simulation permettant d'assurer une grande réutilisabilité du code réalisé.

Dans ce qui suit nous allons détailler l'implémentation matérielle de notre algorithme de chiffrement par flux en VHDL suivant la démarche présentée à la figure (5.1), dont la validation des codes est accomplie en deux phases:

- Une phase de simulation pré-synthèse: qui comprend l'étape de synthèse et de simulation fonctionnelle de l'algorithme en question dans le but d'estimer sa performance, et de vérifier son fonctionnement;

- Une phase d'implémentation et de configuration physique de l'algorithme synthétisé sur le composant ciblé.

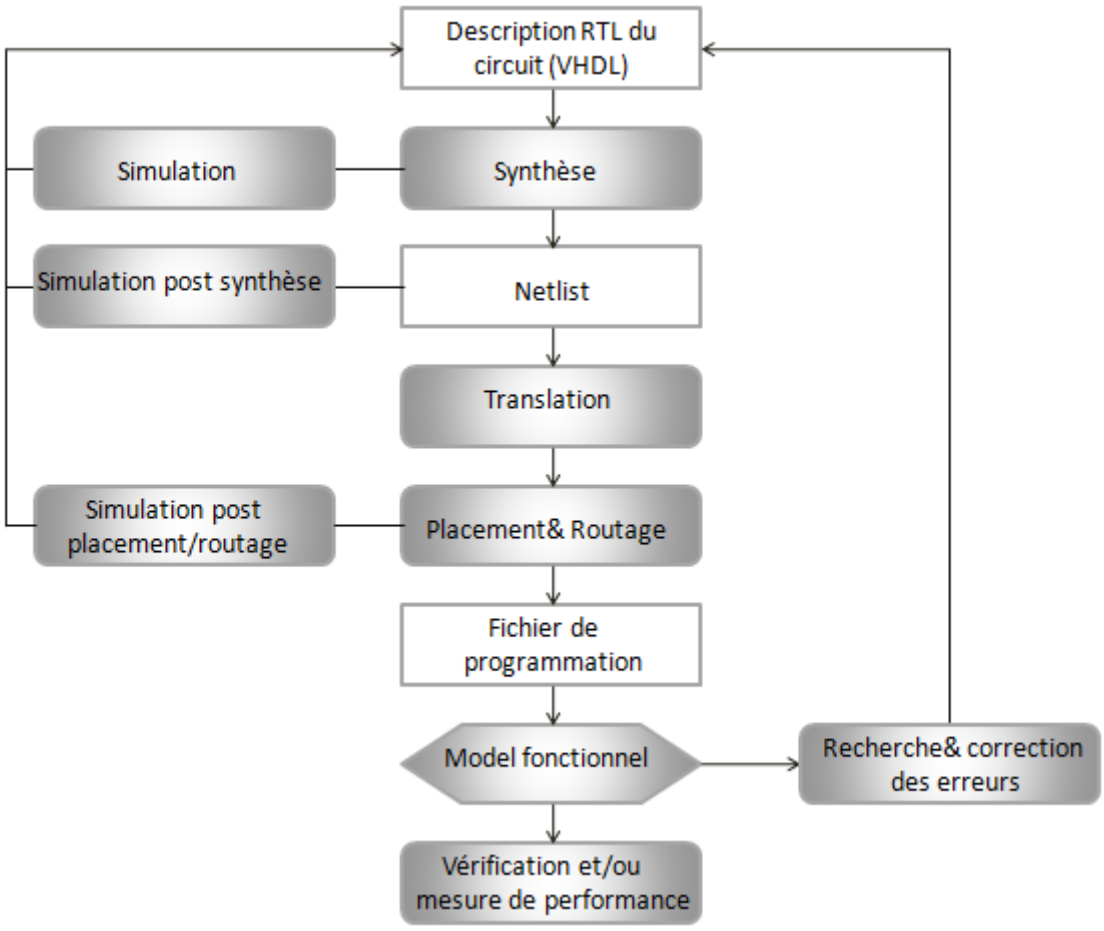

Figure.5.1- Flot générique de conception d'un circuit sur FPGA.

III. Synthèse de l'algorithme de chiffrement proposé

La synthèse logique est le processus par lequel une description VHDL de haut niveau est transformée en une description RTL (Register Transfer Level), qui correspond à une liste de signaux (Netlist) interconnectant les primitives (portes logiques, registres, blocs mémoire, multiplieurs…) de la bibliothèque du composant ciblé. À cet effet, nous avons décidé d'utiliser le navigateur de projet ISE Design Suite.14.5 pour l'implémentation de notre algorithme de chiffrement par flux. Cet outil, téléchargeable depuis le site de Xilinx[7], constitue un environnement de conception extrêmement efficace, qui regroupe tous les mécanismes nécessaires à l'implémentation d'un circuit numérique, allant de la description

[7] www.xilinx.com

comportementale en VHDL jusqu'à la génération du schéma correspondant en portes logiques.

Pour ce qui est de la synthèse et du placement/routage, nous utiliserons l'outil de développement intégré au FPGA ciblé. Nous allons décrire dans la section suivante tous les aspects liés au processus d'implémentation de l'algorithme de chiffrement proposé.

3.1. Description comportementale

Compte tenu des limites imposées par les outils de synthèse et la technologie du FPGA ciblé, nous nous somme limités dans la description VHDL de notre algorithme de chiffrement par des fonctions synthétisables, issues de la norme IEEE P1076.6-2004, en vue d'atteindre une conception exploitable au plan pratique, à base des composants élémentaires propres au FPGA ciblé.

La norme IEEE P1076.6-2004 (Standard for VHDL Register Transfer Level Syntesis), connue par VHDL RTL, définit quelles descriptions VHDL sont synthétisables et garantissent la portabilité d'une conception VHDL d'un outil de synthèse à un autre [104].

Par ailleurs, nous avons opté pour une description comportementale du générateur de nombres pseudo-aléatoires proposé sous forme d'instructions séquentielles, afin de mettre en valeur la simplicité de son chemin critique. De ce fait, la description en VHDL a été exprimée de façon à regrouper la routine d'initialisation des systèmes chaotiques et les procédures de perturbation et d'extraction des bits pseudo-aléatoires en une seule entité, comme un composant globale nommée PRNG.

3.2. Représentation binaire des systèmes chaotiques

L'arithmétique à virgule fixe est largement recommandée lors de l'implémentation des cryptosystèmes chaotiques sous des composants numériques, afin d'accélérer la vitesse du chiffrement et veiller à la simple réalisation matérielle. D'où l'intérêt d'utiliser une représentation binaire en virgule fixe à 32 bits (2Q30) pour l'implémentation des systèmes chaotiques intégrés au sein de notre générateur de nombres pseudo-aléatoires.

En outre, la structure de notre générateur de nombres pseudo-aléatoires a subi une modification concernant le nombre et le procédé d'extraction des bits pseudo-aléatoires. Il s'agit de l'extension du nombre de bits générés à huit bits au lieu d'un seul bit par cycle d'horloge, comme indiqué dans la version originale décrite au chapitre précédent. Les huit bits extraits correspondent au Xor des bits de poids faible des états chaotiques des deux

récurrences Bernoulli. Cette modification permet une amélioration significative du débit et d'efficacité de notre algorithme, sans altérer la qualité des séquences générées en matière de propriétés statistiques.

3.3. Modélisation du circuit configurable

Un schématique de l'architecture du générateur de nombres pseudo-aléatoires proposé, issu de la phase de synthèse, est visible sur la figure (5.2). Notant que toutes les opérations internes effectuées au sein de l'entité « PRNG » sont soumises aux contrôles des différents signaux d'entrée/sortie décrits au tableau (5.1).

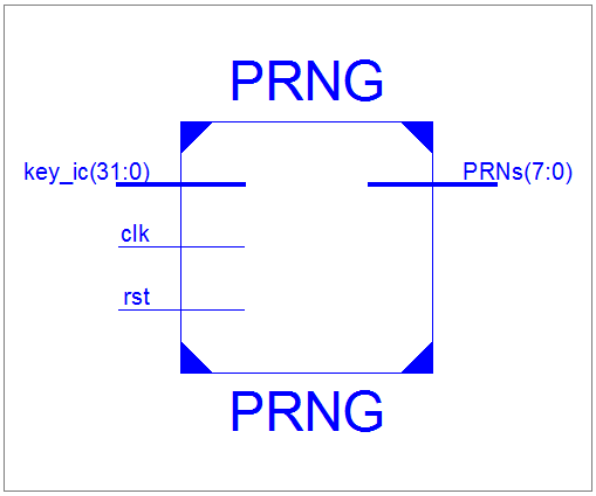

Figure.5.2- Architecture externe du générateur de nombres pseudo-aléatoires proposé.

Nom	Direction	Description
clk	Entrée	Signal d'horloge du système.
rst	Entrée	Signal de réinitialisation asynchrone du système.
Key_ic(31 :0)	Entrée	Bus de chargement du vecteur d'initialisation et de la clé secrète de taille 96 bits, formée par les paramètres des trois systèmes chaotiques. Il est à noter que cette taille est raisonnable pour un chiffrement au niveau hardware.
PRNs(7 :0)	Sortie	Flux des bits pseudo-aléatoires, dont 8 bits sont produits à chaque cycle d'horloge.

Tableau.5.1- Description des signaux intervenant à l'entité PRNG.

La description sous forme séquentielle mise en place pour notre générateur de nombres pseudo-aléatoires assure une forte connectivité entre les signaux internes et externes intervenant à l'entité « PRNG », sachant que les trois systèmes chaotiques et les procédures de perturbation et d'extraction des bits pseudo-aléatoires sont opérés 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 trois systèmes chaotiques se voient assignés un état suivant qui peut varier selon la procédure de perturbation.

De plus de la partie logique, qui décrit le générateur de nombres pseudo-aléatoires, la structure de l'algorithme de chiffrement développé intègre une porte logique Xor qui génère les octets chiffrés à partir des octets en clair et des bits pseudo-aléatoires, comme illustré dans la figure (5.3), en utilisant les signaux décrits ci-dessous.

Nom	Direction	Description
data_in(7 :0)	Entrée	Bus des données confidentielles à chiffrer
data_out(7 :0)	Sortie	Bus des données chiffrées

Tableau.5.2- Description du signal en clair et celui chiffré.

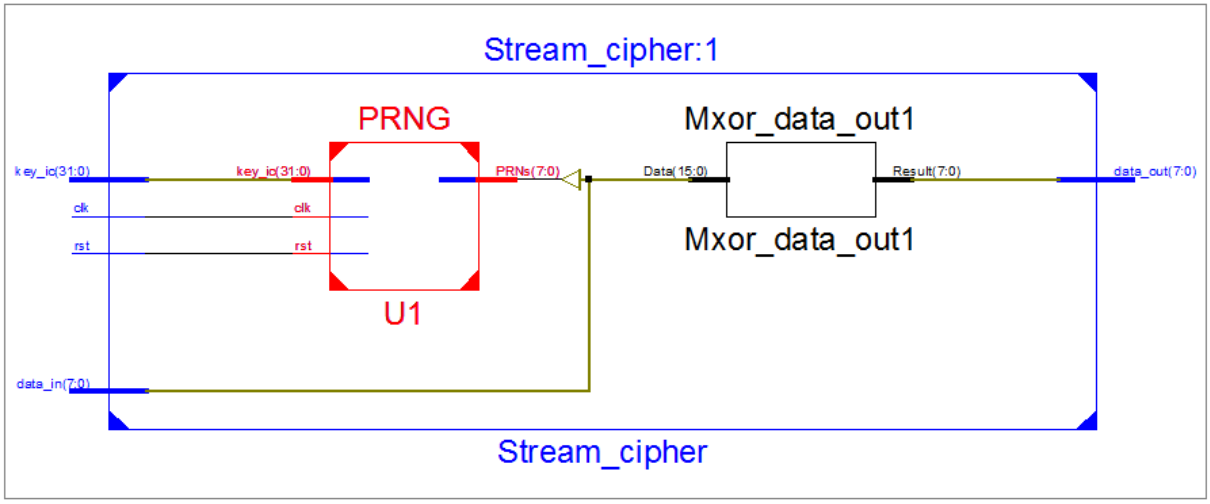

Figure.5.3- **A**rchitecture globale de l'algorithme de chiffrement par flux proposé.

Device Utilization Summary (estimated values)			[-]
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice Registers	72	18224	0%
Number of Slice LUTs	492	9112	5%
Number of fully used LUT-FF pairs	54	510	10%
Number of bonded IOBs	50	232	21%
Number of BUFG/BUFGCTRL/BUFHCEs	1	16	6%
Number of DSP48A1s	22	32	68%

Tableau.5.3- Taux d'occupation en ressources de l'algorithme de chiffrement proposé pour le FPGA ciblé (Spartan-XC6LX16).

Le circuit configurable « Stream_cipher » réalise bien la fonction souhaitée. Il reçoit en entrée le signal contenant l'information et produit en sortie sa somme avec le signal pseudo-aléatoire, c'est-à-dire le signal chiffré. Notant que les ports **data_in** et **data_out** peuvent permuter les rôles, selon que les données en entrée sont en clair ou chiffrées. Le Tableau (5.3) récapitule les ressources hardwares occupées par l'algorithme de chiffrement par flux proposé suite à la synthèse.

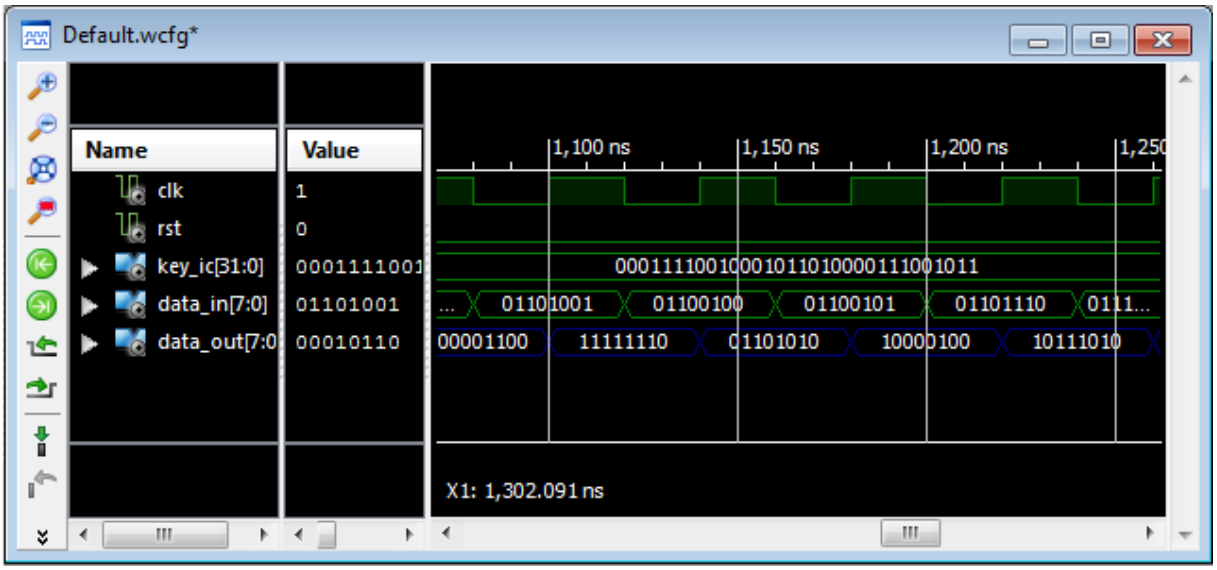

Figure.5.4- Simulation du chiffrement d'un message confidentiel.

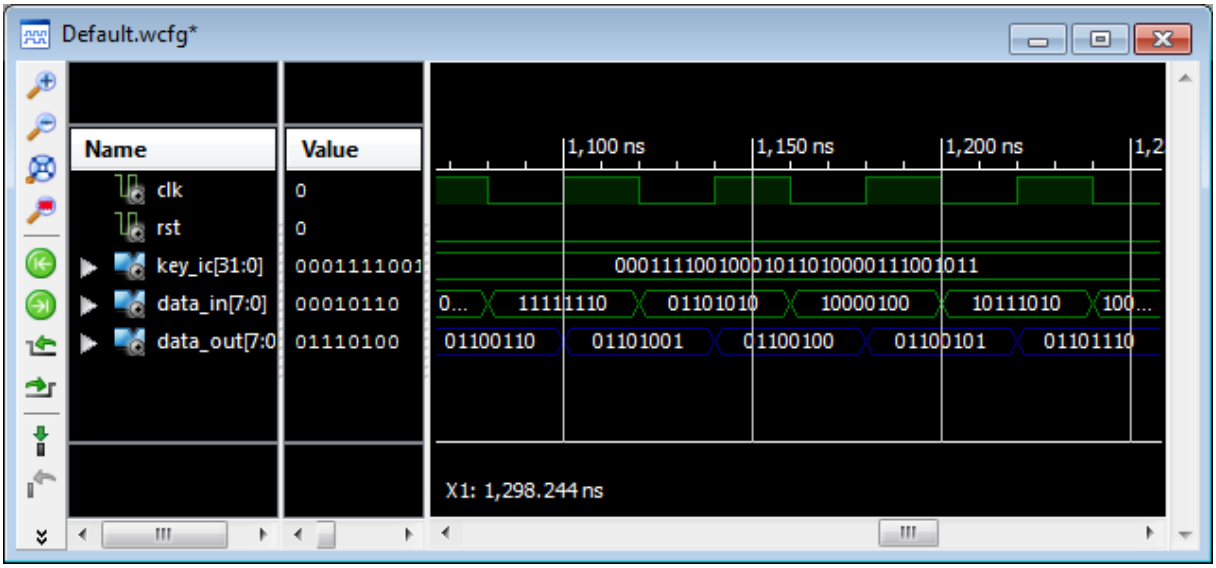

Figure.5.5- Simulation du déchiffrement avec la clé secrète valide.

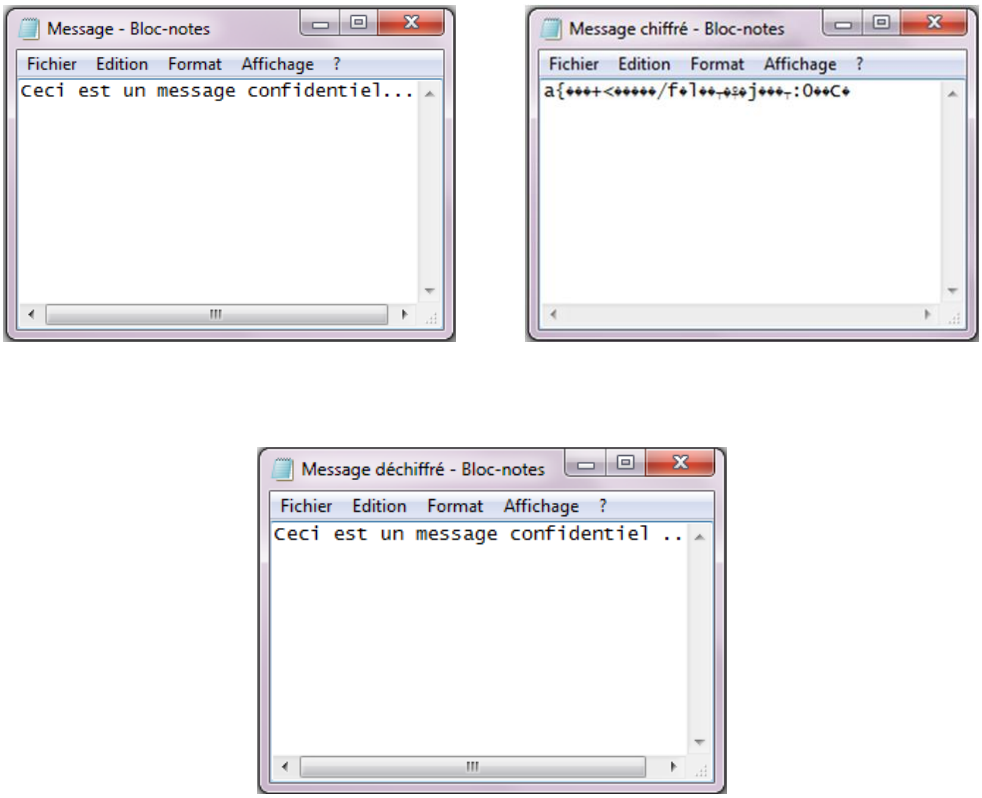

Figure.5.6- Résultats de chiffrement/déchiffrement d'un message confidentiel.

Une simulation pré-synthèse du circuit de l'algorithme de chiffrement proposé est établie pour vérifier sa validité et s'assurer que son fonctionnement est conforme aux résultats obtenus par simulation numérique, avant de passer à son implémentation sur le composant FPGA. La simulation pré-synthèse se fait usuellement par la conception des modèles de simulation numérique ou bancs de tests en VHDL, qui peuvent d'être invoqués directement par le simulateur Isim intégré à l'outil de développement ISE Design Suite. Les figures (5.4) et (5.5) permettent la visualisation des résultats de chiffrement/ déchiffrement d'un message confidentiel en utilisant la condition initiale : $ic = 0.47$ et la clé secrète : $key\{\alpha 1 = 2.998;\ \alpha 2 = 2.899,\ \alpha 3 = 0.617\}$, avec une horloge cadencée à 20 ns.

IV. Implémentation du circuit synthétisé

Après la synthèse logique, l'implémentation de notre l'algorithme de chiffrement consiste en une adaptation du circuit logique synthétisé aux ressources matérielles disponibles sur le FPGA ciblé. À cette fin, l'outil de conception procède en quatre étapes:

- **Traduction « Translate » :** opération de fusion entre les Netlists (listes des noeuds, c'est à dire d'interconnexions et des composants logiques) résultantes de la synthèse logique avec le fichier de contraintes spécifiées;
- **Cartographie « Mapping » :** planifie la conception à l'intérieur des ressources disponibles du FPGA ciblé (qui peut être partiellement occupé par d'autres fonctions déjà intégrées) ;
- **Placement et Routage « Placing and Routing » :** place les composants élémentaires et les relie physiquement, tout en respectant les contraintes spécifiées lors de la synthèse, afin d'obtenir un fichier de configuration ;
- **Génération du fichier binaire « Generate programming file » :** produit un fichier binaire pour la configuration physique du FPGA ciblé.

Il est à noter que les paramètres représentatifs auxquels dépend la performance des implantations des systèmes embarqués sur FPGA, à savoir les limites temporelles des éléments séquentiels, la valeur minimale de la période d'horloge et les broches d'entrées/sorties physiques à utiliser sur le FPGA ciblé, représentent des contraintes strictes qui agissent fortement sur les outils d'implémentation. D'où l'intérêt d'associer toutes les spécifications liées au fonctionnement de notre algorithme de chiffrement à un fichier de contraintes. Ainsi, nous avons vérifié la conformité du circuit implémenté avec les contraintes

prè-établies suite au placement et au routage. Cette étape permet d'évaluer la performance réelle de notre algorithme de chiffrement à travers l'estimation des paramètres déterminants suivants:

5.1. La surface

Une implémentation efficace cherche à diminuer au maximum le taux d'occupation de surface d'un FPGA. Elle s'exprime en "slice" qui, dans le cas d'un Spartan-XC6LX16, contient quatre LUT6-entrée (Look-Up Table ou table de correspondance) avec six entrées et huit bascules (Flip-Flops). Il est cependant intéressant de noter que pour un algorithme de chiffrement, trop peu de logique peut entrainer une très grande fragilité de l'algorithme.

Pour l'algorithme de chiffrement proposé, le taux d'occupation en surface = 154 silices, ce qui est l'équivalent de 6 % de la capacité du Spartan-XC6LX16. Cette occupation réduite de ressources s'explique par le choix judicieux des systèmes chaotiques ainsi que la simplicité des opérations effectuées par notre générateur de nombres pseudo-aléatoires.

5.2. La fréquence maximale de fonctionnement

L'estimation correcte de la fréquence de fonctionnement d'un système est conditionnée par l'étape de placement/routage, et les contraintes spécifiées par le concepteur. De ce fait, il est indispensable de contraindre le design par les limites temporelles souhaitées ainsi que la valeur minimale de la période d'horloge, afin d'en établir une optimisation en terme de vitesse de fonctionnement.

La fréquence maximale du circuit de notre algorithme de chiffrement suite au placement/routage atteint $52.208\,\text{MHz}$ pour une période minimale de $19.154\,\text{ns}$. Une augmentation de la fréquence de fonctionnement reste envisageable en adoptant une programmation parallèle (piplinée) et non pas séquentielle du code, ou bien en intégrant des noyaux IP.

5.3. Le débit en sortie

Le débit est le paramètre le plus important dans l'évaluation des cryptosystèmes, puisqu'il nous renseigne sur la capacité qu'a un algorithme à chiffrer un message, et détermine par conséquent ses domaines d'applications privilégiés. Il s'exprime en Mbps (Mega bits par seconde) et se calcule comme suit :

$$Débit = N \times fréquence\ d'horloge \quad (5.1)$$

Où N est le nombre de bits produits à chaque cycle d'horloge.

D'après (5.1), le débit de notre algorithme de chiffrement atteint 417 Mbps pour N= 8 bits, sachant que le nombre de cycles d'horloge pour le traitement d'une unité de données confidentielles est égale à un dans le cas de notre algorithme. Ce débit est largement suffisant pour répondre aux besoins des transmissions en temps réel.

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.

5.4. Le rapport débit sur slice

Algorithme	**Surface** (slice)	**Débit** (Mbps)	**Débit/Surface** (Mbps/slice)
Algorithme proposé	154	417	2,70
A5/1	57	174	3,05
E0	895	189	0,21
Grain	122	193	1,58
RC4	140	120,8	0,86
Trivium	188	201	1,07

Tableau.5.4- Comparaison des performances entre l'algorithme proposé et les standards de chiffrement par flux.

Le rapport débit-par-slice, qui s'exprime en Mbps/slice, nous donne une idée globale de l'efficacité d'une implémentation en terme de l'utilisation de ressources. Cette métrique est largement considérée lors des études comparatives des algorithmes de chiffrement. Le tableau (5.4) fournit un résumé des fréquences, débits et utilisations des ressources pour l'implémentation de l'algorithme de chiffrement proposé comparée aux résultats précédemment publiés des principaux algorithmes de chiffrement par flux implantés sur des plateformes FPGA [105] [106].

Nous constatons d'après le tableau (5.4) que l'algorithme de chiffrement par flux que nous avons proposé présente des performances compétitives par rapport aux implémentations existantes des algorithmes de chiffrement par flux, notamment en termes de surface et de débit. Néanmoins, cette comparaison reste strictement relative, puisque les implémentations matérielles considérées ne sont pas toutes faites sur la même plateforme FPGA.

En effet, l'algorithme proposé prend d'avantage de la simplicité des systèmes chaotiques utilisés ainsi que l'efficacité du générateur de nombres pseudo-aléatoires proposé et la durée du chemin critique associé, ce qui justifie les bonnes performances obtenues. En revanche, dans le cas des algorithmes : A5/1, Crain et Trivium il n'y a qu'un seul bit produit à chaque cycle d'horloge ($N = 1$), d'où le débit de chiffrement est égale à la fréquence d'horloge. D'autre part, l'algorithme RC4 produit 8 bits à la fois, mais il nécessite trois cycles d'horloge ($N = 8/3$) pour produire 8 bits de sortie. Par conséquent, nous pouvons conclure que l'implémentation matérielle de l'algorithme proposé accomplit un bon compromis entre densité, flexibilité et performances temporelles. Ce qui est très attrayant pour de nombreuses applications.

VI. Transfert de la solution vers la cible

La mise en œuvre de l'algorithme de chiffrement par flux s'achève par l'étape « generate programming 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, dont la connexion entre l'ordinateur et la carte de développement NEXYS3 de Digilent (illustrée par la figure 5.8) contenant le Spartan-XC6LX16 est établie par un câble JTAG.

La carte NEXYS3 consiste en un circuit numérique prêt à l'utilisation, avec une plateforme complète de développement dotée, entre autre, des éléments suivants [107]:

- Deux convertisseurs A/N 12-bits, 125-MHz;
- Deux convertisseurs N/A 14-bits, 165-MHz;
- Une mémoire flash de 64 Mbits;
- Deux mémoires SRAM 256 K×36 bits ;
- Un oscillateur à quartz de fréquence 80 MHz;
- Deux connecteurs d'entrées/sorties numériques de 60-pins chacun;
- Un connecteur JTAG;
- Trois boutons-poussoirs;
- Un bloc de 8 interrupteurs positionnables par l'utilisateur;
- Deux Leds.

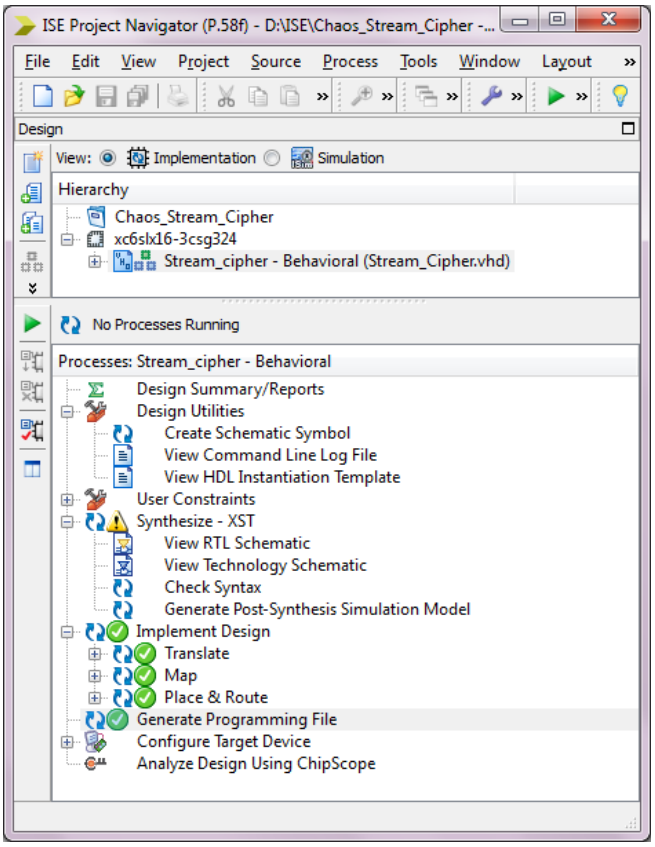

Figure.5.7- Génération du fichier binaire de configuration.

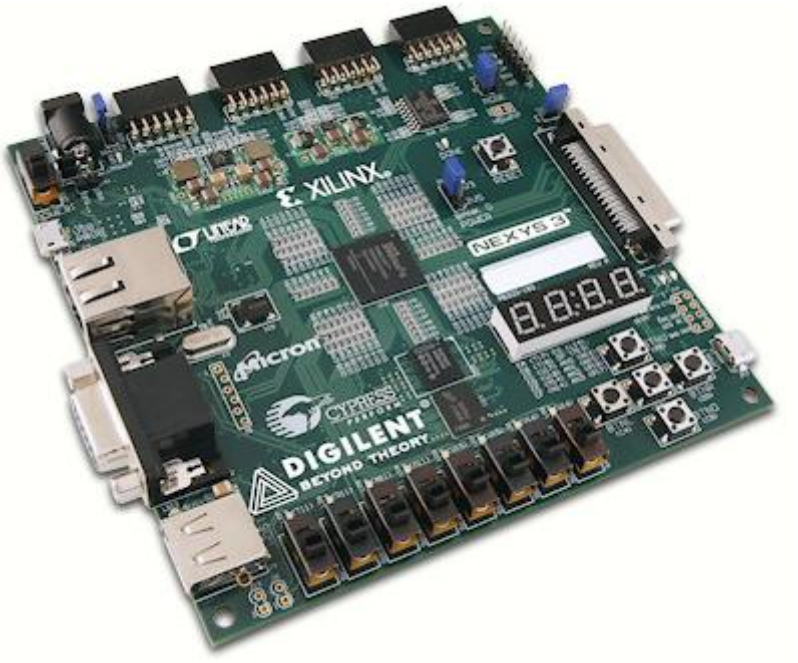

Figure.5.8- La carte de développement NEXYS3.

Une fois le fichier chargé, nous obtenons un circuit prêt à utilisation et être intégré en tant que noyau de chiffrement au sein des dispositifs embarqués dédiés aux transmissions confidentielles.

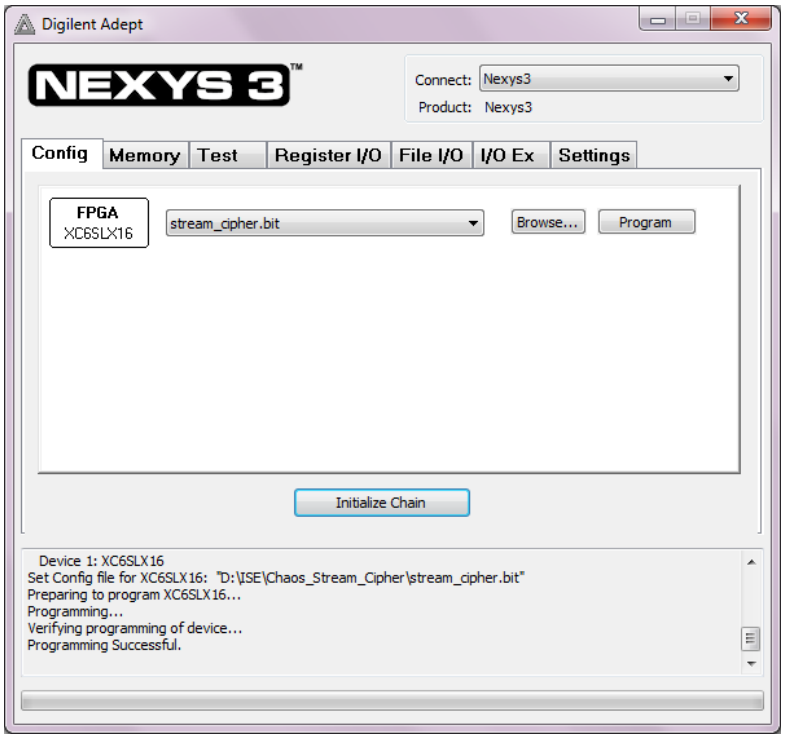

Figure.5.9- Configuration de la carte de développement NEXYS3.

VII. Conclusion

Nous avons abordé au cours de ce dernier chapitre les différents aspects liés à l'implémentation matérielle de l'algorithme de chiffrement par flux à base du chaos que nous avons proposé sur un FPGA Spartan-6 XC6SLX45 de Xilinx, à savoir la description comportementale en VHDL, la synthèse, l'implémentation et la vérification fonctionnelle.

Cette implémentation nous a permis d'une part, une validation expérimentale de l'architecture mise en place via la détermination du taux des ressources occupées ainsi que la fréquence maximale de fonctionnement et le débit binaire atteint par notre algorithme, et d'autre part, de tester le bon fonctionnement du cryptosystème proposé.

Par ailleurs, nous avons pu constater que notre algorithme présente de bonnes performances vis-à-vis des algorithmes de chiffrements par flux largement utilisés tels que A5/1 et RC4, avec un débit de 417 Mbits/s dans une condition de fonctionnement de 52.208 MHz de la fréquence d'horloge, contre un taux d'occupation de 6 % des ressources disponibles sur le FPGA ciblé. Les performances obtenues se justifient par la simplicité de l'algorithme proposé et le choix judicieux des systèmes chaotiques employés.

Conclusion générale et perspectives

Dans cette thèse nous avons abordé l'application des systèmes chaotiques aux transmissions chiffrées, qui malgré les nombreuses études et les avancées marquées dans ce domaine soulèvent encore de nombreux défis.

Nous avons tenté à travers les recherches effectuées d'apporter certaines solutions aux problématiques détaillées tout au long des chapitres de ce document, à savoir celles dues à la représentation binaire des signaux chaotiques et leur implémentation matérielle, et l'établissement de la synchronisation entre l'émetteur et le récepteur en dépit de la forte sensibilité des systèmes chaotiques aux conditions initiales. Les contributions ainsi développées s'articulent autour de trois points principaux, qui peuvent se résumer comme suit:

Le premier concerne l'étude des caractéristiques des systèmes chaotiques du point de vue de la cryptographie, ainsi que les principales approches proposées pour leur exploitation dans cette optique, tout en mettant l'accent sur les problèmes relatifs à la représentation binaire des signaux chaotiques en pratique. Le deuxième et le troisième chapitre de cette thèse ont été consacrés à cet effet. Après avoir exposé un état de l'art des travaux portant sur les transmissions chiffrées par chaos, que ce soit en mode analogique ou numérique, une synthèse résumant les points forts et faibles de chacun des modes a été présentée. En plus, nous avons souligné l'intérêt de la description en dynamique symbolique des systèmes chaotique au chiffrement par flux, notamment pour résoudre le problème de synchronisation entre l'émetteur et le récepteur dans les transmissions par chaos. Nous avons montré également la faisabilité de cette approche dans la génération de nombres pseudo-aléatoires à travers l'étude présentée au troisième chapitre.

Le deuxième point concerne la proposition d'un nouvel algorithme de chiffrement par flux, intégrant un générateur de nombres pseudo-aléatoires à base de systèmes chaotiques discrets. Cette contribution porte sur plusieurs aspects, à savoir le choix des systèmes chaotiques convenables au chiffrement, la représentation binaire adéquate et le procédé d'extraction des

bits pseudo-aléatoires. Tout d'abord, une étude comparative entre plusieurs systèmes chaotiques unidimensionnels a été présentée dans la deuxième section du quatrième chapitre, en vue d'en sélectionner les plus adaptés à notre algorithme. Ensuite, nous avons détaillé la structure du générateur de nombres pseudo-aléatoires basée chaos mise en place, et son utilisation dans le chiffrement par flux. Enfin, nous avons montré par une analyse de sécurité que notre cryptosystème est apte à résister aux différentes techniques de cryptanalyse ciblant les algorithmes de chiffrement par flux. Ainsi, nous avons pu confirmer les bonnes performances de notre algorithme qui sont bien adaptées au chiffrement en temps réel.

Le dernier point abordé correspond à la validation de l'algorithme de chiffrement par flux proposé par une implémentation matérielle sur un composant FPGA. À cet effet, une variation de l'algorithme proposé a été considérée, dans le cinquième chapitre, en raison d'optimisation. Toutefois, les propriétés statistiques des séquences pseudo-aléatoires ont été conservées.

Comparé aux principaux standards de chiffrement par flux, notre algorithme dévoile des performances compétitives, avec un bon compromis entre la sécurité et l'efficacité de fonctionnement.

Les travaux de recherche développés dans le cadre de cette thèse apportent des contributions prometteuses en matière d'exploitation des systèmes chaotiques dans le chiffrement par flux, et laissent entrevoir, par ailleurs, quelques perspectives et élargissements aussi bien sur le plan théorique que pratique :

- D'un point de vue théorique, les systèmes sur lesquels nous avons porté notre attention sont des systèmes discrets unidimensionnels. Cependant des études plus approfondies doivent être établies sur des modèles mathématiques pouvant générer des comportements chaotiques convenables aux applications de chiffrement, y compris les systèmes multidiemsionnels;
- L'algorithme de chiffrement par flux que nous avons proposé présente une solution originale pour préserver la confidentialité dans les transmissions sécurisées. néanmoins, il sera très utile de le combiner avec d'autres mécanismes de cryptographie au sein des protocoles de sécurité, pourquoi pas purement chaotiques, afin d'assurer d'autre fonctionnalités telles que l'intégrité et l'authentification;

- D’un point de vue pratique, l’expérimentation de l’algorithme de chiffrement proposé sur FPGA constitue une version basique qui peut subir différentes optimisations, par l’augmentation du débit de génération de nombres pseudo-aléatoires d’une part, et la réduction des ressources occupées d’autre part, notamment pour répondre aux exigences des systèmes de chiffrement à bas coût;
- Par ailleurs, le choix de la méthode d’implémentation d’un algorithme de chiffrement sur FPGA n’impacte pas uniquement ses performances mais également ses vulnérabilités face aux attaques physiques. De ce fait, une évaluation de sécurité de l’implémentation effectuée est nécessaire, en tenant compte des techniques d’attaques ciblant les composants embarqués, telles que les attaques par canaux cachés, qui nécessitent la mise en œuvre d’un certain nombre de contremesures matérielles. Ces attaques consistent à exploiter toute sorte d’informations physiques émanant du circuit ou à perturber son fonctionnement pour en déduire les données secrètes.

Annexe A : Systèmes dynamiques non-linéaires et chaos

Cette annexe est destinée à introduire quelques notions fondamentales relatives aux systèmes dynamiques non-linéaires, avec un accent particulier porté sur les systèmes exhibant un comportement chaotique, à savoir leurs modèles généraux en temps continu et en temps discret. Par ailleurs, nous évoquerons les principaux outils mathématiques servant à caractériser un comportement chaotique, que se soit qualitativement (l'attracteurs étrange, l'étude de bifurcation), ou quantitativement (les exposants de lyapunov, le spectre de fréquence).

I. Les systèmes dynamiques

1.1. Définition (*Système dynamique*)

Un système dynamique est un ensemble de variables qui évoluent au cours du temps, en décrivant, à partir d'un vecteur de conditions initiales X_0, l'état instantané d'un phénomène donné (mécanique, chimique, électronique, biologique, économique,…).

De point de vue mathématique, un système dynamique est modélisé par un triplet (X, f, T), où:

- $X = \{x_i \in \mathbb{R}^n\}, n = 1..n,$ constitue le vecteur d'état du système à n dimensions;
- f est la loi d'évolution qui détermine la variation temporelle de l'état du système. Elle peut être linéaire ou non-linéaire selon la nature du système modélisé;
- T représente le domaine temporel.

Suivant que la fonction f est indépendante ou dépendante explicitement de la variable temporelle t, le système est dit autonome ou non autonome. Seuls les systèmes dynamiques autonomes à caractère non-linéaire ont été considérés dans cette thèse. Ils sont généralement classés en deux catégories:

Système dynamique à temps continu: dans le cas où la variable temporelle est continue ($t \in \mathbb{R}^+$) le système dynamique est exprimé par un système d'équations différentielles de la forme (A.1).

$$\frac{dx}{dt} = f(x, t, \alpha) \quad (A.1)$$

Avec f est un champ de vecteur autonome, $x \in \mathbb{R}^n$ est le vecteur d'état et $\alpha \in \mathbb{R}^p$ est celui des paramètres.

Système dynamique à temps discret: dans le cas où le temps est discret, le système dynamique est exprimé par une équation récurrente de la forme (A.2).

$$x_{i+1} = f(x_i, \alpha) \quad (A.2)$$

Où f est une fonction continue ou au continue par morceaux, $x_i \in \mathbb{R}^n$ est le vecteur d'état à l'instant $i \in \mathbb{N}$ et $\alpha \in \mathbb{R}^p$ 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 [108].

1.2. Définition (*Système dynamique réversible*)

Un système dynamique discret de la forme (A.2) est dit réversible si f est un homéomorphisme (topologique), i.e. si f est une bijection bi-continue.

En associant à chaque composante du vecteur d'état X une coordonnée dans un espace de dimension n, l'évolution temporelle des états successifs d'un système dynamique défini par des équations différentielles de la forme (A.1) (respectivement par des fonctions récurrentes de la forme (A.2)), à partir d'un vecteur d'états initiaux X_0, admet une solution unique qui se traduit par une trajectoire (respectivement une orbite) dans un espace abstrait, appelé espace des phases.

1.3. Définition (*Espace des phases*)

L'espace des phases, encore appelé espace des états, est un espace euclidien à n dimensions, dont chaque dimension correspond à l'une des composantes du vecteur d'état X d'un système dynamique.

En effet, l'espace des phases couvre l'ensemble de tous les états accessibles par un système dynamique, de sorte qu'à chaque instant donné le système est caractérisé par un point de cet espace. Ainsi, l'espace des phases constitue un outil indispensable pour étudier qualitativement les solutions engendrées par un système dynamique.

II. Classifications des solutions des systèmes dynamiques

Contrairement aux systèmes linéaires qui génèrent des solutions asymptotiques indépendamment de leurs conditions initiales, les systèmes dynamiques munis des non linéarités peuvent exhiber différents types de régimes asymptotiques, en fonction de leurs

états initiaux, ou encore des paramètres qui régissent leurs équations. Cependant, l'évolution de leurs solutions, après un régime transitoire plus ou moins long, restent confinées dans une région bien définie de l'espace des phases appelée «attracteur». Nous allons présenter dans cette section les différentes solutions asymptotiques pouvant être engendrées par un système dynamique non-linéaire, ainsi que les attracteurs qui leurs sont associés [109].

2.1. Point d'équilibre

Cette solution correspond à un état stationnaire pour lequel le système dynamique n'évolue pas avec le temps. Cet équilibre physique est présenté par un point (puits) de l'espace des phases, dont sa valeur est déterminée en fonction de la condition initiale choisie. De ce fait, pour des conditions initiales différentes on peut retrouver plusieurs points d'équilibre.

2.2. Solution périodique

L'évolution d'un régime périodique correspond à une trajectoire formée d'un ensemble fini de valeurs, qui se reproduisent continûment au cours du temps à des intervalles $n \times \mathrm{T}$, où $n \epsilon N^+$ et T désigne la période. Cette solution prend la forme d'un cycle limite fermé dans l'espace des phases. Or, pour une période $\mathrm{T} = 1$ on obtient un point d'équilibre.

2.3. Solution quasi-périodique

Le régime quasi-périodique correspond à une somme de solutions périodiques (au moins deux périodes simultanées) linéairement indépendantes. Les trajectoires associées aux solutions quasi-périodiques sont souvent complexes, et elles ont tendance à être attirées par un attracteur de type tore.

2.4. Solution chaotique

Contrairement aux attracteurs réguliers présentés antérieurement (point fixe, cycle limite et tore), dont les trajectoires qui partent de deux points proches l'un de l'autre dans l'espace des phases restent indéfiniment voisines, et par conséquent leur évolution à long terme reste prévisible à partir d'une situation connue. La solution chaotique se caractérise par un comportement extrêmement sensible aux conditions initiales, de telle sorte que deux trajectoires générées à partir de deux conditions initiales très proches, vont diverger très vite l'une par rapport à l'autre. Cette sensibilité aux conditions initiales traduit aussi le comportement en apparence stochastique des régimes chaotiques, qui implique un attracteur plus complexe dénommé « étrange ». Ce type d'attracteur sera défini ultérieurement.

III. La théorie du chaos

La théorie du chaos a pris son essor au cours des années soixante, suite aux découvertes impressionnantes constatées par plusieurs scientifiques, autour du phénomène fondamental d'instabilité des systèmes dynamiques non-linéaires, communément appelé «sensibilité aux conditions initiales» [110].

En effet, au début du vingtième siècle, le mathématicien français Henri Poincaré fut l'un des premiers à entrevoir la théorie du chaos, en découvrant l'imprévisibilité de l'évolution temporelle de certains systèmes dynamiques complexes, lors de l'étude de stabilité du système solaire. Poincaré avait exprimé cet effet par : « *Une cause très petite, et qui nous échappe, détermine un effet considérable que nous ne pouvons pas ne pas voir, et alors nous disons que cet effet est dû au hasard.* »

Par ailleurs, des recherches sur la stabilité du mouvement des systèmes dynamiques ont conduit le mathématicien russe Alexandre Lyapunov à introduire l'idée de mesurer l'écart entre deux trajectoires ayant des conditions initiales voisines. C'est ainsi qu'il a découvert que l'évolution exponentiellement de cet écart implique une sensibilité du système dynamique aux conditions initiales. Cette contribution sera plus tard très utile pour étudier certains aspects de la théorie du chaos, notamment pour quantifier la sensibilité aux conditions initiales des systèmes chaotiques.

Plus tard en 1963, le problème de la sensibilité aux conditions initiales a été mis en évidence par le météorologue américain Edwards Lorenz, qui expérimentait une méthode lui permettant de prévoir les phénomènes météorologiques. C'est par pur hasard qu'il observa qu'une modification minime des données initiales pouvait changer de manière considérable ses résultats, et par conséquent aucune prévision à long terme n'est possible. Ce phénomène a été popularisé par Edwards Lorenz sous « l'effet papillon »: *le battement d'aile d'un papillon à Tokyo peut entraîner une tempête à New-York (sic)*.

Suite à la révélation de ce nouveau comportement dynamique, ce qui était dû à la complexité du système étudié est maintenant perçu comme une manifestation de processus déterministes souvent simples amenant un comportement chaotique imprévisibles. Quant au terme « chaos », il a été introduit pour la première fois par le mathématicien Jim Yorke, en 1975.

Ces résultats ont été assimilés et exploités par des scientifiques de différents domaines de recherche : mathématiques, physique, électronique, biologie, médecine,

télécommunications...etc. D'où de nombreuses définitions des systèmes chaotiques ont été proposées dans la littérature. Ci-dessous, nous retiendrons la définition qui confine les trois caractères fondamentaux du chaos, énoncée par Strogatz [111].

3.1. Définition *(Comportement chaotique)*

Le chaos est un comportement apériodique à long terme dans un système déterministe, qui présente une dépendance sensible aux conditions initiales.
Les trois propriétés du chaos tirées de la définition peuvent être expliquées comme suit:

- **Comportement apériodique**: l'évolution temporelle d'un système chaotique dans l'espace des phases, lorsque le temps tend vers l'infini, ne converge vers aucun régime régulier (point fixe ou orbite périodique). Ce comportement irrégulier provient des non-linéarités attachées aux systèmes chaotiques ;
- **Déterminisme:** un système chaotique obéit à des lois mathématiques qui décrivent son comportement dynamique, à partir de son état initial et ses paramètres critiques. 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 ;
- **Sensibilité aux conditions initiales**: quelle que soit la proximité de deux états initiaux, les trajectoires qui en sont issues divergent rapidement l'une de l'autre. Par conséquent, bien que le système soit déterministe, aucune prévision à long terme n'est possible. Cette sensibilité découle aussi des variations des paramètres critiques qui régissent les systèmes chaotiques.

Exemple

$$\begin{cases} \frac{dx(t)}{dt} = a(y(t) - x(t)) \\ \frac{dy(t)}{dt} = bx(t) - y(t) - x(t)z(t) \\ \frac{dz(t)}{dt} = x(t)y(t) - cz(t) \end{cases} \qquad \text{(A.3)}$$

La définition évoquée ci-dessus peut être illustrée à travers l'étude du système dynamique de Lorenz, donné par les équations (A.3). L'évolution temporelle de ce système dynamique fait apparaître un comportement chaotique pour les valeurs des paramètres : $\{a = 10,\ b = 8/3,\ c = 28\}$. La figure (A.1) présente l'évolution temporelle de l'une de ses variables

d'état, tandis que la figure (A.2) correspond à la simulation des trajectoires issues de deux conditions initiales légèrement différentes.

En effet, l'évolution temporelle en apparence aléatoire des trajectoires du système de Lorenz et son hypersensibilité aux conditions initiales confirment bien son aspect chaotique. Par ailleurs, il existe plusieurs outils pour détecter et évaluer les comportements chaotiques des systèmes dynamiques non-linéaires. Nous allons présenter dans la section suivante les outils les plus répandus servant à identifier qualitativement et quantitativement le chaos.

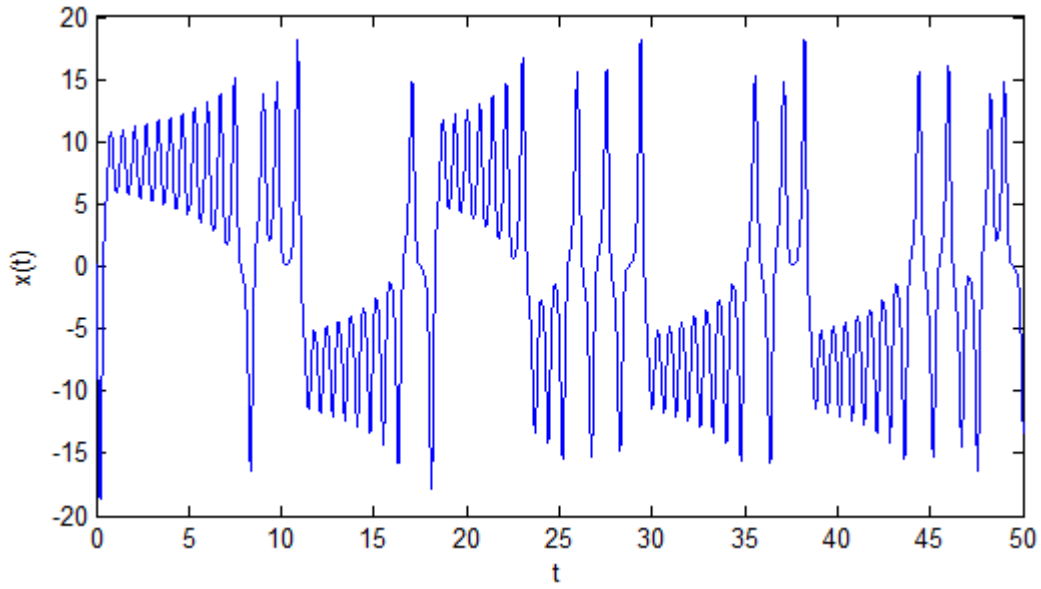

Figure.A.1-Série temporelle x(t) générée par le système de Lorenz, à partir des paramètres: a= 10, b= 8/3, c= 28 et des conditions initiales : x=0.1, y=-10 et z=5.

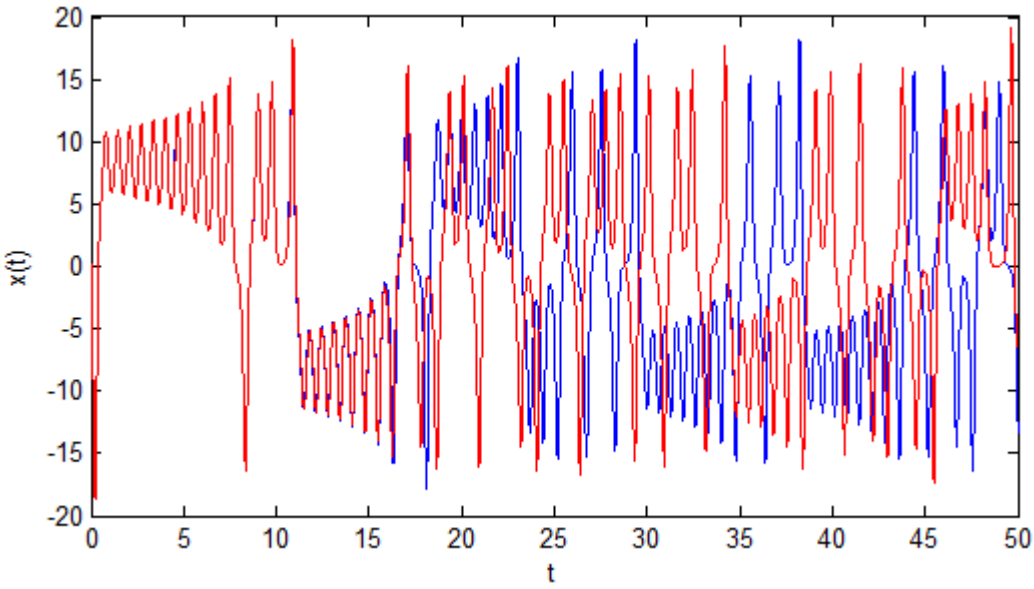

Figure.A.2- Séries temporelles x(t) et x'(t) générées par le système de Lorenz, à partir des conditions initiales : x_0=0.1 et x'_0=0.1001.

IV. Caractérisation des comportements chaotiques

La visualisation du comportement asymptotique d'un système dynamique non-linéaire dans l'espace des phases permet d'entrevoir son allure, et d'interpréter la nature de son évolution. Cependant, lorsqu'il s'agit d'un comportement chaotique, des outils mathématiques adéquats sont requis pour pouvoir détecter son existence. Certains de ces outils sont déjà bien connus en traitement du signal comme l'analyse fréquentielle, et d'autres sont plus spécifiques au domaine des dynamiques non-linéaires comme les diagrammes de bifurcation et les exposants de Lyapunov.

4.1. Attracteur étrange

Le terme « attracteur étrange » a été introduit pour la première fois par Ruelle et Takens en 1971, pour désigner l'objet mathématique issu de l'évolution chaotique d'un système dynamique non-linéaire dans l'espace des phases. La forme de cet attracteur se caractérise par une géométrie particulière qui n'est pas une courbe ni une surface et n'est même pas continue, et dispose notamment des propriétés remarquables suivantes:

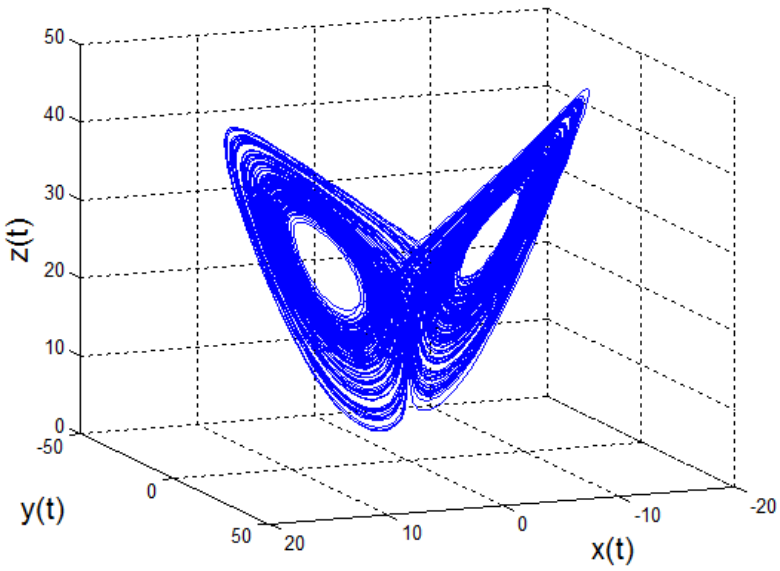

Figure.A.3- Vue en trois dimensions de l'attracteur étrange de Lorenz.

- Une dimension fractale formée d'une infinité de cycles périodiques, contenus dans un ensemble borné non variant;
- Les trajectoires de phases sont attirées vers le même attracteur, mais sans repasser deux fois par le même point ;
- Les paires de trajectoires voisines divergent sur l'attracteur sans jamais le quitter;

En général, la visualisation d'un attracteur étrange qui remplit les propriétés précitées affirme l'existence du chaos. L'attracteur étrange constitue donc la façon la plus simple pour la détection des régimes chaotiques. La figure (A.3) illustre le célèbre attracteur étrange du modèle de Lorenz, qui constitua le premier système différentiel permettant d'observer un attracteur étrange.

4.2. Etude de bifurcation

Les systèmes dynamiques non-linéaires évoluent souvent vers des régimes stationnaires qui varient en fonction de certains paramètres de contrôle. Une faible perturbation de l'un de ceux-ci, lorsque les points d'équilibre du système sont stables, ne change pas son comportement. Cependant, il y a des valeurs particulières des paramètres pour lesquelles on observe un changement qualitatif des caractéristiques du système. Par exemple, nombre de points d'équilibre, perte ou changement de stabilité d'un point fixe, ou encore l'apparition de nouvelles solutions éventuellement plus complexes comme le chaos. Un changement de nature dans le comportement d'un système dynamique est appelé « bifurcation ». Elle surgit lorsqu'un paramètre de contrôle franchit une valeur critique. Ainsi, un système dynamique non-linéaire est confronté à bifurquer vers le chaos, lorsqu'on fait varier progressivement l'un de ses paramètres de contrôle, selon trois scénarios de transition possible [112]:

L'intermittence : il s'agit d'un régime qui demeure pratiquement périodique durant de longs laps de temps, et qui se déstabilise brutalement, pour laisser place à une courte bouffée de bruit, puis le régime redevient périodique et ainsi de suite... Lorsqu'on augmente la valeur du paramètre de contrôle, les bouffées deviennent de plus en plus fréquentes, et finalement, le chaos domine;

Le doublement de période (cascade sous-harmonique) : la variation d'un paramètre de contrôle fait passer le système par une suite de bifurcations, chacune correspondant à l'apparition d'une orbite de période double de la précédente, qui devient alors instable. La succession de ces bifurcations converge de manière géométrique vers un point d'accumulation, au-delà de lequel peuvent être observés des régimes chaotiques, qui n'apparaissent donc que lorsqu'un nombre infini d'orbites périodiques ont été créées ;

La quasi-périodicité : ce phénomène intervient lorsque le régime périodique devient quasi-périodique, c'est-à-dire son spectre contient deux fréquences d'oscillation indépendantes. L'influence des oscillations l'une sur l'autre conduit à un dérèglement de leur mouvement,

qui peut à son tour perdre sa stabilité et devenir chaotique, soit directement, soit par la survenance d'une troisième fréquence.

Ces scénarios transitoires permettent de comprendre les mécanismes qui conduisent à l'apparition du chaos. Notant que les valeurs des paramètres critiques qui régissent ces changement sont appelées points de bifurcation. Elles peuvent être repérées graphiquement à l'aide d'un diagramme de bifurcations.

Exemple

Prenons l'exemple de la récurrence logistique (A.4) qui est l'un des plus simples systèmes dynamiques pouvant exhiber un comportement chaotique. La figure (A.4) représente le diagramme de bifurcation associé à la récurrence logistique, obtenu en faisant varier la valeur de son paramètre de contrôle α dans l'intervalle [2, 4], à partir de l'état initial x_0=0.5.

$$x_{n+1} = \alpha x_n(1 - x_n) \quad (A.4)$$

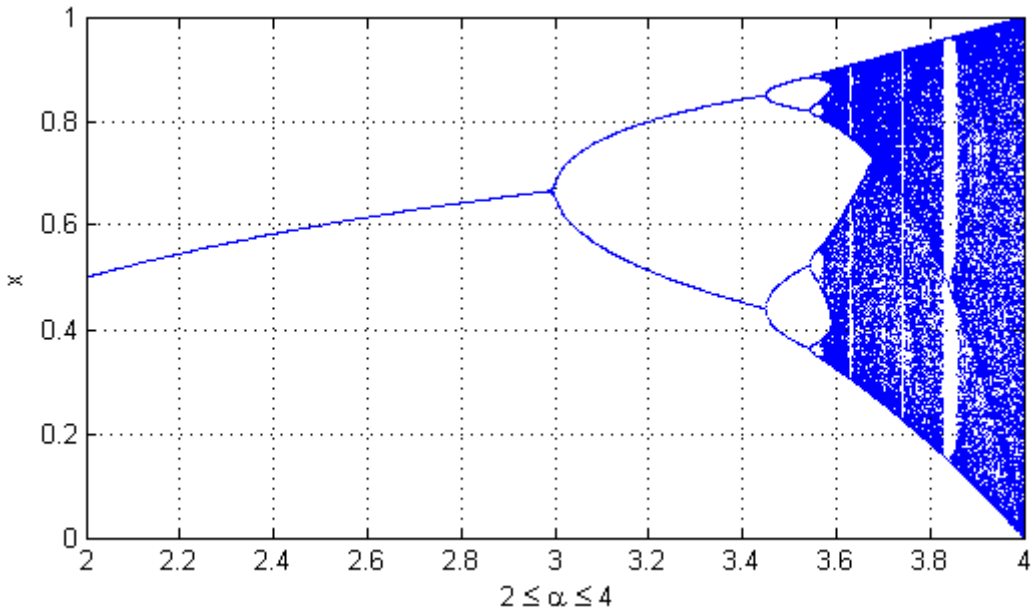

Figure.A.4- Diagramme de bifurcation de la récurrence Logistique**.**

Il s'agit dans ce cas d'une bifurcation par doublement de période, dans laquelle nous pouvons constater les caractéristiques suivantes [113]:

- Le diagramme est composé d'intervalles sur lesquels les solutions asymptotiques évoluent continûment avec le paramètre α;

- Les intervalles qui correspondent aux différents régimes périodiques sont séparés par les points de bifurcation;
- Aux points de bifurcations plusieurs branches de solutions semblables ou différentes peuvent apparaître ou disparaître;
- Par augmentation progressive du paramètre α, le régime périodique voit tout d'abord sa période doubler, puis être multipliée par 4, par 8, par 16, et ainsi de suit;
- Après un régime transitoire et le passage par une multiplication de la période de base jusqu'à l'infini, la trajectoire de la récurrence logistique atteint le seuil du chaos à partir de α =3.57.

4.3. Exposant de Lyapunov

L'extrême sensibilité des trajectoires chaotiques aux conditions initiales est la caractéristique fondamentale permettant de reconnaître les régimes chaotiques. En effet, à partir de conditions initiales qui diffèrent de façon infinitésimale, le système chaotique évolue sur des trajectoires totalement divergentes bien que liées au même attracteur étrange. Ce qui empêche la prévisibilité de leurs comportements à long terme. Le mathématicien russe Alexander Lyapunov s'est focalisé sur ce phénomène en proposant de mesurer la vitesse moyenne de divergence entre deux trajectoires issues de deux conditions initiales différentes. Cette grandeur λ, appelée exposant de Lyapunov, se définit par rapport à deux trajectoires voisines $x(t)$ et $x'(t)$ issues d'un système dynamique de dimension n, à partir de deux conditions initiales différentes : $x(0)$ et $x'(0)$, en fonction de la déformation subie sur la i-ème direction par la limite (A.5).

$$\lambda_i = \lim_{t\to+\infty} \frac{1}{t} ln \frac{\| \delta x_i(t) \|}{\| \delta x_i(0) \|} , i = 1 \dots n \quad (A.5)$$

Avec $\delta x_i(t) = x_i(t) - x'_i(t)$.

Il suffit alors de calculer la limite quand t tend vers l'infinie pour déterminer la façon dont s'amplifie l'erreur initiale. L'obtention d'un exposant positif signifie que les trajectoires ont tendance à diverger l'une de l'autre, tendis que pour un exposant négatif celles-ci convergeront. Or, pour un exposant nul, les trajectoires sont confondues.

En conclusion, pour dire qu'un système est chaotique au sens de Lyapunov, il doit posséder un exposant positif selon au moins un axe de l'espace des phases, tout en rendant compte que la somme des exposants est négative ou nulle.

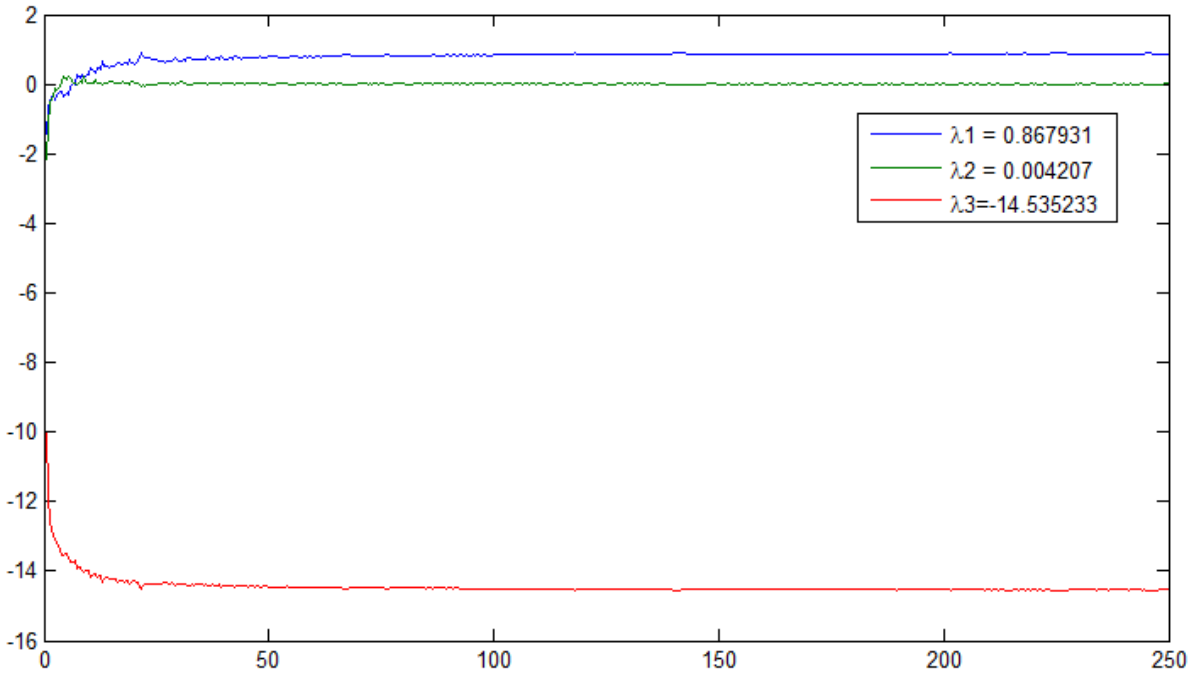

Figure.A.5- Exposants de Lyapunov du système de Lorenz pour les paramètres : a= 10, b= 8/3 et c= 28.

Les résultats de calcul des exposants de Lyaponov du système de Lorenz (A.3) confirment l'existence du comportement chaotique pour les valeurs de paramètres considérées dans la simulation donnée à la figure (A.5). Cependant, cette condition n'est pas suffisante pour conclure qu'un système est chaotique. Il demeure indispensable de confronter les résultats de calcul des exposants de Lyapunov avec ceux fournis par d'autres outils d'analyse non-linéaire.

4.4. Spectre de puissance

L'analyse spectrale est un outil de caractérisation très classique en traitement du signal, qui permet d'identifier le type d'un signal, qu'il soit périodique, chaotique ou encore aléatoire, à partir de l'observation de la manière dont se comporte sa série temporelle. En général, le spectre d'un signal périodique ou quasi-périodique fait apparaître un ensemble de raies discrètes correspondant aux fréquences fondamentales et harmoniques du signal. En revanche, le spectre d'un signal chaotique a une allure continue qui ressemble à celle d'un signal bruité, dans laquelle n'émerge aucune fréquence dominante, mais plutôt une large gamme de fréquences comme montré dans la figure (A.6) qui représente le spectre de fréquence du système de Lorenz.

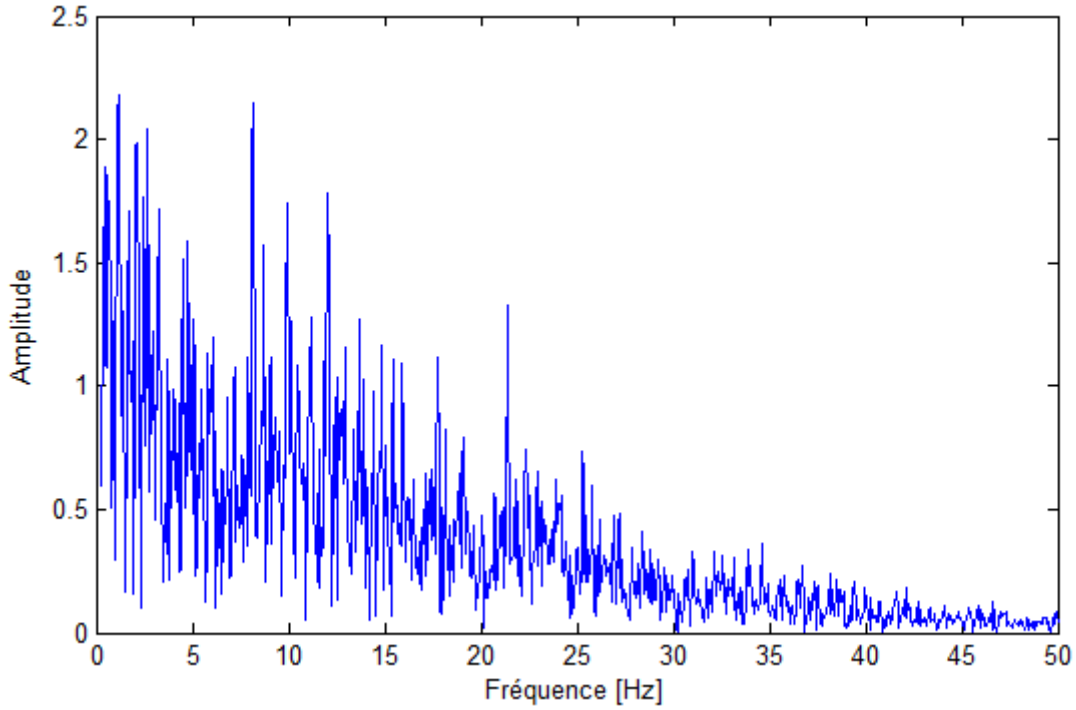

Figure.A.6- Spectre de fréquence du système de Lorenz.

L'existence d'un spectre continu est une caractéristique essentielle des mouvements chaotiques d'un système dynamique. Cette propriété est très bénéfique pour certains domaines d'applications tels que les télécommunications, en particulier pour la transmission des signaux à caractère confidentiel qui nécessitent une forte robustesse face aux interférences et une faible probabilité de détection.

Annexe B : Description des tests statistiques de NIST SP800-22

Les tests du NIST publiés sous NIST SP800-22, forment un paquetage de tests statistiques conçus pour vérifier l'aspect aléatoire des séquences binaires à la sortie des générateurs de nombres aléatoires ou pseudo-aléatoires utilisés dans des primitives cryptographiques. Nous avons utilisé dans notre étude la dernière version de NIST SP800-22, qui comporte une implémentation des 15 tests statistiques d'aléa les plus évolués qui existent.

L'exécution des tests s'appuie sur le concept d'hypothèses, qui permet d'accepter (ou rejeter) l'hypothèse sur l'aléarité de la suite binaire testée. Le résultat fourni par chaque test consiste en une P-value qui représente la probabilité qu'un générateur de nombre aléatoire parfait produise une séquence moins aléatoire que la séquence testée. Les P-values calculées par rapport à une constante α appelée "niveau de signification", sont interprétées comme suit:

- P-value égale à 0 signifie que la séquence est non aléatoire;
- P-value $\geq \alpha$, l'hypothèse nulle est acceptée, c'est à dire la séquence apparaît aléatoire;
- P-value $< \alpha$, l'hypothèse nulle est rejetée, c'est-à-dire la séquence apparaît non aléatoire;

Le niveau de signification α est choisi typiquement dans l'intervalle [0.001, 0.01]. Par exemple α égale à 0.001 indique qu'une séquence sur 1000 est rejetée par le test si la séquence n'est pas aléatoire. Or, pour α égale à 0.01 une séquence sur 100 est rejetée. Donc, une P-value ≥0.01 signifie que la séquence est aléatoire.

Dans ce qui suit nous allons énumérer la batterie NIST SP800-22 avec une brève description de chaque test [114]. L'ensemble des tests que nous avons utilisé dans notre étude sont disponibles dans le package STS version 1.8[8] fourni par le NIST.

1. Test de fréquence (Frequency)

Le but de ce test est de déterminer si le nombre de uns et de zéros dans une séquence est approximativement identique à celui prévu pour une séquence réellement aléatoire. Le test vérifie notamment si la fraction des uns est proche de 1/2.

[8] http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html

L'exécution de ce test consiste tout d'abord à remplacer les uns par (+1) et les zéros par (-1) dans la séquence étudiée, puis faire la somme bit à bit de la séquence. Si la somme obtenue est très grand (trop de 1) ou très petit (trop de 0) alors la séquence est considérée comme non aléatoire. Il est recommandé que la séquence testée soit d'une longueur minimale de 100 bits.

2. Test de fréquence par bloc (Block frequency)

Ce test reprend le même principe du test de fréquence, en étudiant la proportion de « uns » et de « zéros » des sous-séquences de M bits issues da la suite binaire à tester. A ce propos, la suite binaire sera divisée en blocs de M bits, puis on vérifie si la fréquence des uns est approximativement 1/2 dans chaque bloc. Il est recommandé que chaque sous-séquence ait une longueur minimale égale à 100 bits. D'où nous avons considéré des blocs de 128 bits pour le test du générateur de nombres pseudo-aléatoires proposé.

3. Test de la somme cumulée (Cumulative sums)

Le but de ce test est de déterminer si la somme cumulée des bits consécutifs de la séquence analysée ajustée à (−1, +1) est très grande ou très petite, afin de détecter la présence de nombre important de zéros ou de uns. En effet, la plus grande somme partielle (en valeur absolue) ne doit pas être trop grande, car elle indiquerait une mauvaise répartition des zéros et des uns. Mais elle ne doit pas non plus être trop faible, car au contraire cela indiquerait que les zéros et les uns sont trop bien mélangés.

Deux approches sont possibles pour appliquer ce test. La première notée mode 0 consiste à parcourir la séquence à partir du premier bit. Tandis que la seconde notée mode 1 consiste à parcourir la séquence en sens inverse en partant du dernier bit.

4. Test des suites homogènes (Runs)

Le but de ce test est de déterminer si les oscillations entre les zéros et les uns sont trop rapides ou trop lentes dans une séquence binaire. La détection des oscillations se fait par le calcul du nombre de suites homogènes sur la totalité de la séquence binaire testée. Il est à noter qu'une suite homogène de longueur L est une séquence invariante de bits identiques encadrée par des bits de valeur opposée. Si le nombre de suites homogènes est petit (oscillation très lente) alors la séquence est considérée comme non aléatoire.

5. Test de la plus longue série de uns (Long runs of one's)

Ce test consiste à déterminer la plus longue suite homogène de « uns » pour chacun des blocs de taille M bits formant la séquence entière étudiée, puis vérifier si la distribution des suites recensées est conforme avec les probabilités théoriques des séquences aléatoires. C'est-à-dire la longueur de la plus grande suite homogène de uns correspond à celle de la plus grande suite homogène de uns rencontrée dans une suite véritablement aléatoire.

6. Test de rang de la matrice binaire (Binary Matrix Rank)

L'objectif de ce test est d'observer s'il y une dépendance linéaire entre les différents blocs de la suite à tester. À cet effet, des matrices binaires de taille 32 × 32 sont construites à partir de la suite entière, puis le rang des matrices disjointes est calculé et distribué par rapport au rang plein. Il suffit alors de comparer les valeurs obtenues avec celles d'une vraie séquence aléatoire pour savoir si la suite est bien aléatoire.

7. Test spectral (Spectral DFT)

Ce test utilise la transformée de Fourier discrète de la suite, pour détecter la périodicité de certains motifs dans la séquence testée. Plus particulièrement, le test vise à détecter si le nombre de pics dont la hauteur dépasse le seuil de 95% est largement différent de 5 %, comme prévu pour une séquence aléatoire.

8. Recherche d'un motif apériodique (Non overlapping template Matching)

Le but de ce test est de calculer le nombre d'occurrence d'un motif apériodique (template) de taille m bits à l'intérieur de la séquence étudiée après l'avoir décomposée en blocs.

La recherche des motifs apériodiques se fait en trois étapes. La première étape consiste à diviser la séquence étudiée en N blocs de taille T bits. Ensuite, la deuxième étape consiste à choisir le motif de taille m à rechercher. Enfin, la dernière étape consiste à parcourir les N blocs avec la fenêtre contenant le motif recherché et compter le nombre d'occurrence correspondant. Le nombre d'occurrences dans chaque bloc est enregistré en incrémentant un vecteur V_i. V_0 est incrémenté quand il n'y a pas d'égalité, et V_1 est incrémenté dans le cas contraire.

Une fois trouvé le motif recherché, la fenêtre de recherche sera décalée jusqu'au premier bit qui suit le motif en question. Au final, le test rejettera les séquences qui ont un très grand nombre d'occurrence d'un motif apériodique.

9. Recherche d'un motif périodique (Overlapping template Matching)

Le principe de ce test est identique au test de recherche d'un motif apériodique, qui s'agit de compter le nombre d'occurrence d'un motif particulier dans la séquence étudiée. Cependant, lorsque ce motif est trouvé dans la suite, la fenêtre de recherche ne sera pas déplacée à la fin de celui-ci, mais continue à traverser la suite normalement bit par bit. Ainsi, Le test rejettera les séquences qui ont un très grand nombre d'occurrence d'un motif.

10. Test universel de Maurer (Universal)

Le but de ce test est de mesurer l'écart entre deux mots identiques dans la suite, en vue de détecter si la séquence étudiée peut être compressée ou non sans perte d'information. En effet, une séquence significativement compressible est considérée comme non aléatoire.

Le test prend deux paramètres : la longueur L et le nombre des mots utilisés. Le programme parcourt la suite et commence par créer un dictionnaire avec les Q premiers mots. Celui-ci contient la position de la dernière occurrence de chaque mot. Le parcours du reste de la suite permet de mettre à jour les positions des dernières occurrences et de calculer la somme des logarithmes en base deux des écarts entre deux occurrences consécutives d'un même mot. Cette valeur servira pour déterminer si la suite est aléatoire ou pas grâce à une comparaison avec des valeurs théoriques.

Si ce test est passé avec succès alors tous les tests statistiques classiques le seront également. Cependant, ce test nécessite des suites relativement longues pour que le résultat soit pertinent.

11. Test de l'entropie approximative (Approximate entropy)

Le principe général de ce test est similaire au test série. Il s'agit de comparer les fréquences d'occurrence de toutes les sous-séquences possibles dans deux blocs superposés, de longueur consécutive M et $M + 1$, avec celles rencontrées dans une suite aléatoire.

12. Test d'excursions aléatoires (Random excursion)

Ce test consiste à séparer la suite selon ces cycles (excursion aléatoire), dont chacun est une succession de valeurs pour lesquelles la séquence partielle commence à 0 et termine par 0 (avec des valeurs non nulles entre les deux zéros). Ainsi, pour chaque cycle, le programme compte le nombre de fois où les valeurs -4 à -1 et 1 à 4 sont atteintes par la somme partielle. En fonction des résultats obtenus, la séquence est considérée aléatoire ou non aléatoire.

13. Variante du test d'excursions aléatoires (Random excursion variant)

Comme pour le test d'excursions aléatoires, le principe de ce test consiste à calculer le nombre de fois où un état particulier est visité dans la marche aléatoire de la séquence étudiée, afin de détecter les écarts par rapport au nombre d'occurrence normal des différents états : -9, -8,...,-1. Et +1, +2,..., +9, pour une séquence aléatoire.

14. Test série (Serial)

Ce test concerne la fréquence d'occurrence de chaque sous-séquence de M bits tout au long de la séquence entière. L'objectif de ce test est de déterminer si toutes les sous-séquences de M bits formant la suite à tester ont la même chance d'apparence, comme c'est le cas pour une vraie séquence aléatoire.

En résumé, la séquence qui passe le test avec succès doit être uniforme, de sorte que les nombres d'occurrence de tous les modèles de M bits soient identiques. De ce fait, pour $M = 1$, le test de série est équivalent au test de fréquence.

15. Test de la complexité linéaire (Linear complexity)

Ce test permet de déterminer si la séquence analysée est suffisamment complexe pour être considérée comme aléatoire à partir de la longueur minimale du registre à décalage à rétroaction linéaire produisant la séquence en question.

L'exécution du test consiste à partager la séquence entière en N blocs indépendants de M bits, puis la longueur minimale du registre à décalage permettant de générer les bits de chaque bloc est calculée à l'aide de l'algorithme de Berlekamp-Massey. La longueur minimale obtenue désigne la complexité linéaire de chaque bloc de la suite. De ce fait, un LFSR trop court implique que la suite testée n'est pas aléatoire.

Il est à noter que les 15 tests cités ne permettent en aucune façon de garantir ou de prouver qu'une suite est vraiment aléatoire, le mieux que l'on puisse déduire c'est que la suite en question parait aléatoire, c'est à dire qu'elle est de bonne qualité.

Par ailleurs, bien que l'ordre d'application des tests soit arbitraire, le test de fréquence doit être appliqué en premier lieu, puisqu'il fournit la preuve la plus évidente de l'aspect non aléatoire, qui est la non-uniformité. Si le test de fréquence ne réussit pas, la probabilité d'échec des autres tests est très élevée.

Annexe C : Algorithmes de chiffrement par flux conventionnels

Dans cette annexe nous rappelons la structure et le principe de fonctionnement des algorithmes de chiffrement par flux synchrones, considérés dans les études comparatives menées dans cette thèse.

1. Algorithme A5/1

L'algorithme A5/1 développé à la fin des années 1980, constitue actuellement le standard de chiffrement des transmissions GSM. Il fait partie des algorithmes de chiffrement dépendants de vecteurs d'initialisation IV, qui ont pour effet de générer plusieurs suites chiffrantes différentes à partir d'une même clé secrète, ainsi que la simplification de la gestion de la resynchronisation.

Le principe de fonctionnement de l'algorithme A5/1 s'appuie sur la combinaison de trois registres à décalage à rétroaction linéaire de taille 18, 20 et 22 bits, initialisés à partir d'une clé secrète de 64 bits et un vecteur d'initialisation de 22 bits. Chacun des registres comporte un bit de décision servant à la mise à jour des états internes des registres suivant le diagramme présenté dans la figure (C.1).

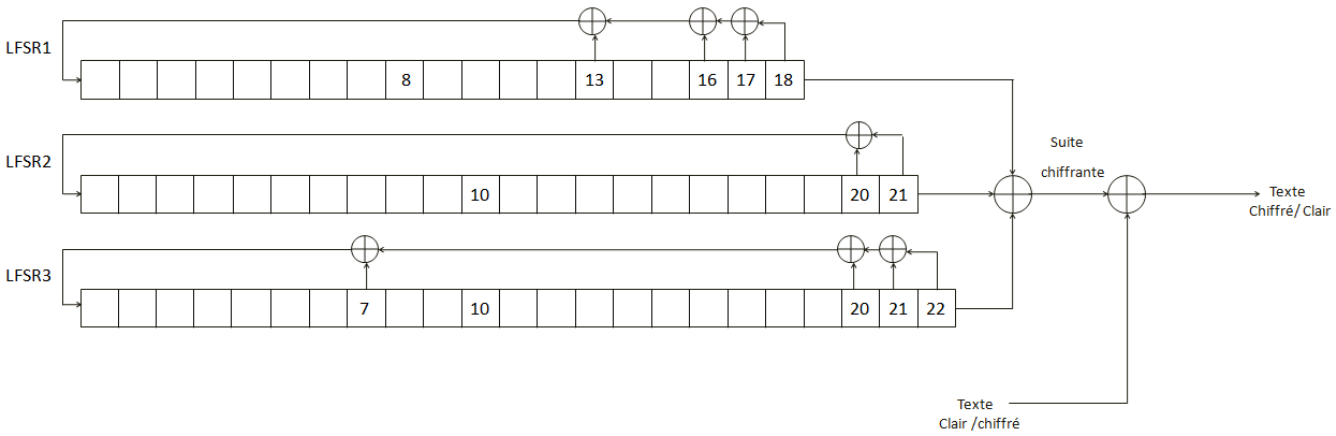

Figure.C.1- Schéma descriptif de l'algorithme A5/1.

À chaque coup d'horloge, le bit majoritaire des trois registres est déterminé et seuls les registres dont le bit de décision est conforme à la majorité seront mis à jour. De ce fait, au moins deux registres sont mis à jour à chaque coup d'horloge. Les bits de la suite chiffrante sont générés via le XOR des derniers bits des trois registres [115].

2. Algorithme E0

E0 est l'algorithme de chiffrement par flot utilisé pour préserver la confidentialité dans le protocole de transmission sans fil « Bluetooth ». Le générateur de nombres pseudo-aléatoires associé à l'algorithme E0 est composé de quatre registres à décalage à rétroaction linéaire de longueurs 25, 31, 33 et 39 bits, combinés selon une fonction non-linéaire comportant 4 bits de mémoire interne. L'initialisation des registres se fait par une clé secrète de taille 128 bits, et un vecteur d'initialisation de 64 bits.

À chaque coup d'horloge, tous les registres sont décalés et leurs états internes sont mis à jour en utilisant l'état courant, l'état précédent et les valeurs déjà contenues dans les registres. Quatre bits sont extraits des quatre registres puis additionnés. L'algorithme effectue ensuite un XOR entre la somme obtenue et la valeur du registre de 2 bits, le premier bit obtenu est la sortie pour le chiffrement.

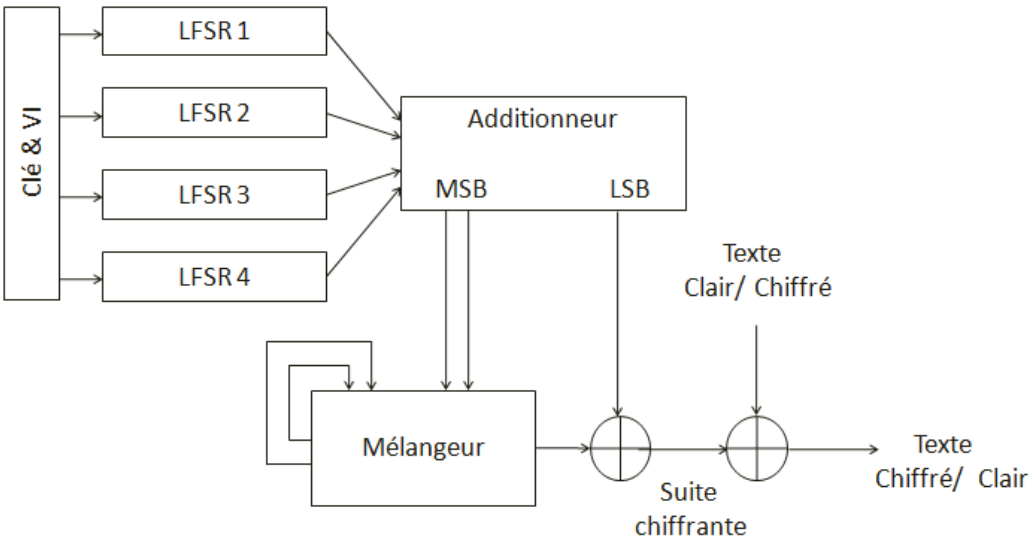

Figure.C.2- Schéma descriptif de l'algorithme E0.

3. Algorithme Grain

L'algorithme Grain et l'un des finalistes du projet eSTREAM[9], destiné à être implémenté en matériel. La structure de son générateur de nombres pseudo-aléatoires est composée de deux registres à décalage de longueur 80 bits avec un état interne de 160 bits. Le premier est un registre à décalage avec rétroaction linéaire (LFSR) permettant de garantir une période minimale pour la suite chiffrante. Tandis que le second registre à décalage est avec rétroaction non-linéaire (NFSR).

Une fois son état interne chargé à partir d'une clé secrète et un vecteur d'initialisation de taille souvent 80 et 64 bits respectivement, la suite chiffrante est générée en filtrant simultanément deux bits du NFSR et sept bits du LFSR, via une fonction de filtrage non-linéaire utilisant l'opérateur "ET" logique, comme indiqué sur la figure (C.3) [116].

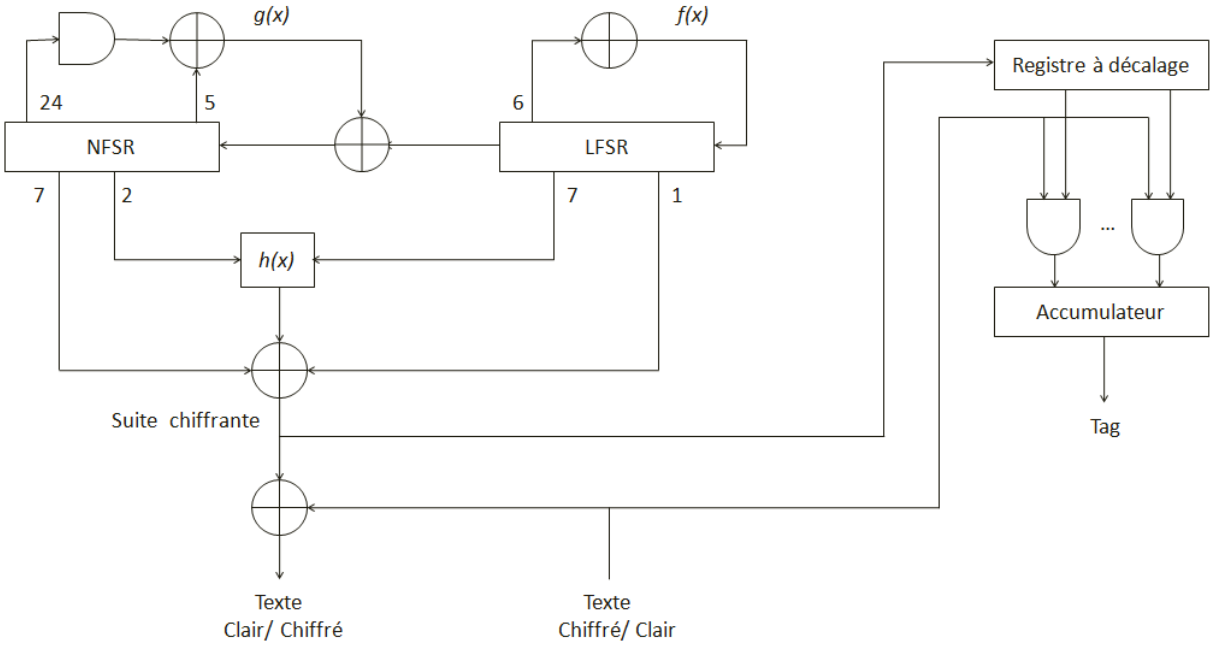

Figure.C.3- Schéma descriptif de l'algorithme Grain.

1. RC4 (Rivest Cipher 4)

L'algorithme RC4 est l'un des plus répandus algorithmes du chiffrement par flux dédiés aux applications logicielles. Il a été inventé en 1987 par Ron Rivest l'un des concepteurs du

[9] http://www.ecrypt.eu.org/stream/index.html

RSA. Depuis, il est largement déployé notamment dans les protocoles SSL et TLS et la norme de chiffrement WEP (Wired Equivalent Privacy) pour les réseaux sans fil.

La génération des suites chiffrantes au sein de l'algorithme RC4 est basée sur une manipulation spécifique des tables de mots en deux étapes. La première étape consiste à initialiser une table d'états S de 256 octets à partir d'une clé secrète de longueur variable, souvent fixée à 128 bits. Quand à la deuxième étape produit les octets de la suite chiffrante, à partir de la table S et de deux compteurs i et j mis à zéro, comme illustré dans la figure (C.4). La génération d'un nouvel octet aléatoire s'effectue selon l'algorithme ci-dessous :

Générateur de nombres pseudo-aléatoires
Entrée : $i,\ j$
Sortie : $s[t]$
$i \leftarrow (i+1)\ mod\ 256$
$j \leftarrow j + s[i]\ mod\ 256$
Permuter (s[i], s[j])
$s[t] \leftarrow s[i] + s[j]\ mod\ 256$

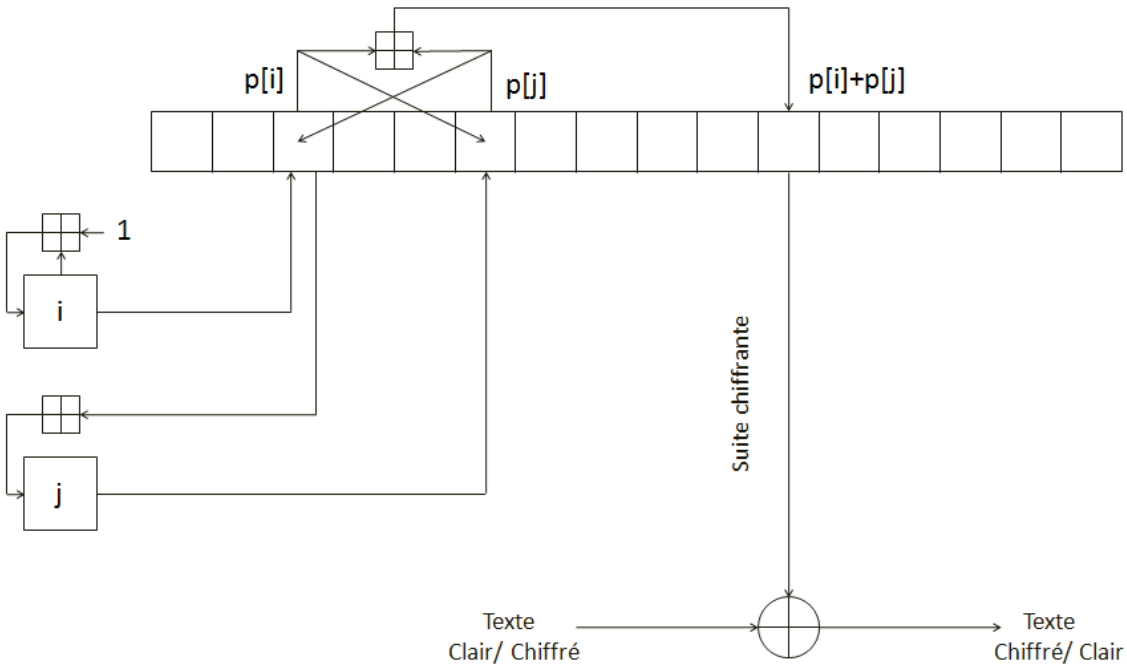

Figure.C.4- Schéma descriptif de l'algorithme RC4.

1. Algorithme Trivium

Trivium est l'un des candidats du projet E-Stream orienté au niveau matériel. Il pend en entrée une clé secrète de taille 80 bits et un vecteur d'initialisation de la même taille, avec un état interne de 288 bits. La structure de son générateur de nombres pseudo-aléatoires est composée de trois registres à décalage de longueur 93, 84 et 111 bits, interconnectés selon des fonctions de rétroaction non-linéaires, de façon à former un réseau de substitution-permutation. La génération des bits pseudo-aléatoire se fait ainsi par le biais d'une fonction d'extraction linéaire comme indiqué sur la figure (C.5) [117].

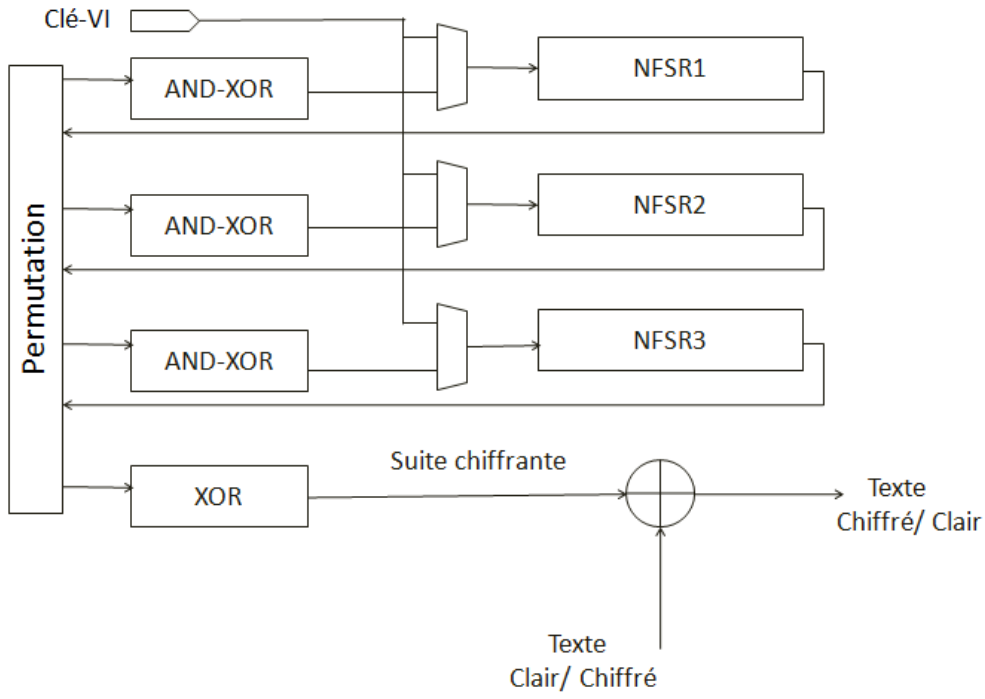

Figure.C.5- Schéma descriptif de l'algorithme Trivium.

Références bibliographiques

[1] C. E. Shannon, "*Communication theory of secrecy systems**". Bell system technical journal, vol. 28, no 4, p. 656-715 (1949).

[2] G. Millérioux, J. M. Amigó, and J. Daafouz, "*A connection between chaotic and conventional cryptography*". IEEE Transactions on Circuits and Systems I : Regular Papers, 55(6) (2008).

[3] G. Alvarez & S. Li. "*Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems*". International Journal of Bifurcation and Chaos", vol. 16, no. 8, pages 2129–2151 (2006).

[4] R. SCHMITZ, "*Use of chaotic dynamical systems in cryptography*". Journal of the Franklin Institute, vol. 338, no 4, p. 429-441(2001).

[5] P. Stavroulakis & M. Stamp (Eds.), "*Hand book of Information and Communication Security*", Springer (2010).

[6] L. Pecora & T. Caroll, "*Synchronization in chaotic systems*". Physical Review Letters, 64(8) :821-824 (1990).

[7] S. H. Strogatz, "*Nonlinear dynamics and chaos: with applications to physics, biology, chemistry, and engineering*". Westview press (2014).

[8] L. M. Pecora, et al. "*Fundamentals of synchronization in chaotic systems, concepts, and applications.*" Chaos: An Interdisciplinary Journal of Nonlinear Science 7.4, p. 520-543 (1997).

[9] H. Nijmeijer & I. M. Mareels, "*An observer Looks at Synchronization*". IEEE transaction on circuits and Systems: Fundamantal Theory and Applications, vol.44, p. 882-890 (1997).

[10] O. Morgul, E. Solak and M. Akgul, "*Observer based chaotic message transmission*", International Journal of Bifurcation and Chaos, vol 13, No 4, p. 1003-1007, (2003).

[11] G. Besançon, "*Nonlinear Observers and Applications*". Lecture Notes in Control and Information Sciences (2007).

[12] A. ZEMOUCHE, "*Sur l'observation de l'état des systèmes dynamiques non-linéaires*". Thèse de doctorat. Université Louis Pasteur-Strasbourg I (2007).

[13] L. Kovarev, K. S. Eckert, L. O. Chua and U. Parlitz, "*Experimental demonstration of secure communications via chaotic synchrionization*", International Journal of Bifurcation and Chaos, vol. 2, 709-713 (1992).

[14] T. Yang, "*A Survey of Chaotic Secure Communication Systems*". International Journal of Computational Cognition, vol. 2, no 2, pp. 81-130 (2004).

[15] G. Alvarez, S. Li, F. Montoya, G. Pastor & M. Romera, "*Breaking projective chaos synchronization secure communication using filtering and generalized synchronization*". Chaos, Solitons & Fractals, vol. 24, no 3, p. 775-783 (2005).

[16] U. Parlitz, L. O. Chua, L. Kocarev, K. S. Halle & A. Shang, "*Transmission of digital signals by chaotic synchronization*". International Journal of Bifurcation and Chaos, vol. 2, no 04, p. 973-977 (1992).

[17] G. Kolumban, M. P. Kenedy & L. O. chua. "*The role of synchronization in digital communications using chaos-part II : Chaotic modulation and chaotic synchronization*". IEEE Trans. Circuits and Systems, vol. 45, p. 1129-1140, (1998).

[18] T. YANG, L. B. YANG & C. M. YANG, "*Cryptanalysing chaotic secure communications using return maps*". Physics Letters A, vol. 245, no 6, p. 495-510 (1998).

[19] T. Yang, L. B. Yang & C. M. Yang. "*Breaking chaotic switching using generalized synchronization: examples*". Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on, vol. 45, p. 1062-1067 (1998).

[20] T. Yang & L. O. Chua, "*Secure communication via chaotic parameter modulation*", IEEE transactions on circuits and systems. 1, Fundamental theory and applications, vol. 43, p. 817-819 (1996).

[21] M. Feki. "*An adaptive chaos synchronization scheme applied to secure communication*". Chaos, Solitons and Fractals, vol. 18, p. 141–148 (2003).

[22] U. Feldmann, M. Hasler & W. Schwarz, "*Communication by chaotic signals :the inverse system approach*". International Journal of Circuit Theory and Applications, vol. 24, p. 551-579 (1996).

[23] M. Chen, D. Zhou, & Y. Shang. "*A sliding mode observer based secure communication scheme*". Chaos, Solitons and Fractals, vol. 25, p. 573–578 (2005).

[24] L. Larger, V. S. Udaltsov, S. Poinsot et al. "*Electro-optic nonlinear oscillator for ultra-fast secure chaos communication*". In: European Symposium on Optics and Photonics for Defence and Security. International Society for Optics and Photonics, p. 83-89 (2004).

[25] V. Annovazzi-Lodi, M. Benedetti, S. Merlo, T. Perez, P. Colet & C. R. Mirasso, "*Message encryption by phase modulation of a chaotic optical carrier*". IEEE Photonics Technology Letters, vol. 19, p. 76-78 (2007).

[26] A. A. Koronovskii, O. I. Moskalenko & A. E. HRAMOV, "*On the use of chaotic synchronization for secure communication*". Physics-Uspekhi, vol. 52, no 12, p. 1213 (2009).

[27] A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, ... & K. A. Shore, "*Chaos-based communications at high bit rates using commercial fibre-optic links*". Nature, vol. 438, no 7066, p. 343-346 (2005).

[28] R. Lavrov, M. Peil & M. Jacquot, "*Nonlocal nonlinear electro-optic phase dynamics demonstrating 10 Gb/s chaos communications*", IEEE Journal on Quantum Electronics, vol. 46, p. 1430–1435 (2010).

[29] G. Alvarez, F. Montoya, M. Romera & G. Pastor. "*Breaking two secure communication systems based on chaotic masking*". IEEE transactions on circuits and systems. I : Regular Papers, vol. 51, p. 505-506 (2004).

[30] G. Alvarez, L. Hernandez, J. Munoz, F. Montoya & S. Li. "*Security analysis of communication system based on the synchronization of different order chaotic systems*". Physics Letters A, vol. 345, no 4, p. 245-250 (2005).

[31] T. Yang, L. B. Yang & C. M. Yang. "*Cryptanalyzing chaotic secure communications using return maps*". Physics Letters A, vol. 245, n° 6, p. 495-510 (1998).

[32] S. Ercan , "*Cryptanalysis of observer based discrete-time chaotic encryption schemes*", International Journal of Bifurcation and Chaos, vol. 15, no 2, p. 653-658 (2005).

[33] R. Kharel, K. Busawon & Z. Ghassemlooy, "*Modified Chaotic Shift Keying using Indirect Coupled Chaotic Synchronization for Secure Digital Communication*". CHAOS 2010, 3rd Chaotic Modeling and Simulation International Conference, Chania, Crete, Greece (2010).

[34] A. Khadra, X. Liu & X. Shen, "*Application of impulsive synchronization to communication*". Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on, vol. 50, no 3, p. 341-351 (2003).

[35] K. Li, Y. C. Soh, & Z. G. Li, "*Chaotic cryptosystem with high sensitivity to parameter mismatch*". Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on, vol. 50, no 4, p. 579-583 (2003).

[36] Z. P. JIANG, "*A note on chaotic secure communication systems*". Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on, vol. 49, no 1, p. 92-96 (2002).

[37] G. Zheng, D. Boutat, T. Floquet & J. P. Barbot, "*Secure data transmission based on multi-input multi-output delayed chaotic system*". International Journal of Bifurcation and Chaos, vol. 18, no 7, p. 2063-2072 (2008).

[38] H. HAMICHE, "*Inversion à Gauche des Systèmes Dynamiques Hybrides Chaotiques. Application à la Transmission Sécurisée de Données*". Thèse de doctorat, Universite Mouloud Mammeri de Tizi-Ouzou (2011).

[39] C. Robilliard, E. H. Huntington, & M. R. Frater, "*Digital transmission for improved synchronization of analog chaos generators in communications systems*". Chaos: An Interdisciplinary Journal of Nonlinear Science, vol. 17, no 2, p. 023130 (2007).

[40] L. Kocarev, & L. Shiguo , "*Chaos-based cryptography: theory, algorithms and applications*". Springer, Vol. 354 (2011).

[41] B. Furht & D. Kirovski, "*Multimedia security handbook*". CRC press, (2004).

[42] J. H. Huang & Y. Liu, "*A block encryption algorithm combined with the Logistic mapping and SPN structure. In : Industrial and Information Systems (IIS)* ", 2nd International Conference on. IEEE, p. 156-159 (2010).

[43] A. Benjeddou, A.K. Taha, D. Fournier-Prunaret & R. Bouallegue, "*A New Cryptographic Hash Function Based on Chaotic S-box*", CSNDSP, Austria, p. 23-25 July, 2008.

[44] E. Elbadawy, A. Mokhtar, W. El-masry, A. Waleed, et al. "*A new chaos advanced encryption standard (AES) algorithm for data security*". In : Signals and Electronic Systems (ICSES), International Conference on. IEEE, p. 405-408 (2010).

[45] G. Zaibi, A. Kachouri, F. Peyrard et al. "*On dynamic chaotic S-Box*". In : Information Infrastructure Symposium, GIIS'09. Global. IEEE, p. 1-5 (2009).

[46] M. Khan, T. Shah, H. Mahmood & M. A. Gondal, "*An efficient method for the construction of block cipher with multi-chaotic systems*", Nonlinear Dyn, vol. 71, p. 489-492 (2013).

[47] G. Chen, Y. Chen & X. Liao, "*An extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps*". Chaos, Solitons & Fractals, vol. 31, no 3, p. 571-579 (2007).

[48] P. L. Carmen & L. R. Ricardo, "*Notions of Chaotic Cryptography: Sketch of a Chaos Based Cryptosystem*". In : Applied Cryptography and Network Security. p. 267-294 (2012).

[49] T. Habutsu, Y. Nishio, I. Sasase et al. "*A secret key cryptosystem by iterating a chaotic map*". In : Advances in Cryptology-EUROCRYPT'91. Springer Berlin Heidelberg, p. 127-140 (1991).

[50] X. Wang, L. Teng & X. Qin, "*A novel color image encryption algorithm based on chaos*". Signal Processing, vol. 92, no 4, p. 1101-1108 (2012).

[51] C. Fu, B. B. Lin, Y. S. Miao & J. J. Chen, "*A novel chaos-based bit-level permutation scheme for digital image encryption*". Optics Communications, vol. 284, no 23, p. 5415-5423 (2011).

[52] M. S. Baptista, "*Cryptography with chaos*". Physics Letters A, vol. 240, no 1, p. 50-54 (1998).

[53] E. Alvarez, A. Fernandez, P. Garcia, J. Jiménez & A. Marcano, "*New approach to chaotic encryption*". Physics Letters A, vol. 263, no 4, p. 373-375 (1999).

[54] LI, Shujun, X. Zheng, X. Mou & Y. Cai, "*Chaotic encryption scheme for real-time digital video*". In : Electronic Imaging. International Society for Optics and Photonics, p. 149-160 (2002).

[55] V. Guglielmi, H. Poonith, D. fournier-prunaret et al. "*Security performances of a chaotic cryptosystem*". In : Industrial Electronics, IEEE International Symposium on. IEEE, p. 681-685 (2004).

[56] L. Wang, Q. Ye, Y. Xiao et al. "*An image encryption scheme based on cross chaotic map*". In : Image and Signal Processing. CISP'08. Congress on. IEEE, vol. 3, p. 22-26 (2008).

[57] S. Lian, J.Sun & Z.Wang, "*A block cipher based on a suitable use of the chaotic standard map*". Chaos Soliton Fract, Vol. 26, p.117–29 (2005).

[58] M. Andrecut, "*Logistic map as a random number generator*". International Journal of Modern Physics B, vol. 12, no 09, p. 921-930 (1998).

[59] M. Alioto, S. Bernardi, A. Fort et al. "*Analysis and design of digital PRNGS based on the discretized sawtooth map*". In : Electronics, Circuits and Systems, ICECS. Proceedings of the 10th IEEE International Conference on. IEEE, p. 427-430 (2003).

[60] M. E. Yalcin, J. AK. Suykens & J. Vandewalle, "*True random bit generation from a double-scroll attractor*". Circuits and Systems I: Regular Papers, IEEE Transactions on, vol. 51, no 7, p. 1395-1404 (2004).

[61] M. A. Zidan, A. G. Radwan & K. N. Salama, "*Random number generation based on digital differential chaos*". In : Circuits and Systems (MWSCAS), IEEE 54th International Midwest Symposium on. IEEE, p. 1-4 (2011).

[62] Y. Kun, Z. Han, & L. Zhaohui, "*An improved AES algorithm based on chaos*". In: Multimedia Information Networking and Security. MINES'09. International Conference on. IEEE, p. 326-329 (2009).

[63] H. S. Kwok & W. KS. Tang, "*A fast image encryption system based on chaotic maps with finite precision representation*". Chaos, Solitons & Fractals, vol. 32, no 4, p. 1518-1529 (2007).

[64] R. U. Ginting & R. Y. Dillak, " *Digital color image encryption using RC4 stream cipher and chaotic logistic map*". In : Information Technology and Electrical Engineering (ICITEE), International Conference on. IEEE. p. 101-105 (2013).

[65] Y. Mao & G. Chen, "*Chaos-based image encryption*". In : Handbook of Geometric Computing. Springer Berlin Heidelberg, p. 231-265 (2005).

[66] D. Arroyo, G. Alvarez, S. Li, C. Li, & J. Nunez, "*Cryptanalysis of a discrete-time synchronous chaotic encryption system*". Physics Letters A, vol. 372, no 7, p.1034-1039 (2008).

[67] M. Maqableh *et al.* "*Analysis and design security primitives based on chaotic systems for ecommerce*". Thèse de doctorat. Durham University (2012).

[68] S. Li, "*Analyses and New Designs of Digital Chaotic Ciphers*". PhD thesis, School of Electronic and Information Engineering, Xi'an Jiaotong University (2003).

[69] G. D. ARROYO, "*Framework for the analysis and design of encryption strategies based on discrete-time chaotic dynamical systems*". Thèse de doctorat. Agronomos (2009).

[70] ANSI/IEEE Std 754-1985, "*IEEE Standard for Binary Floating-Point Arithmetic*",Standards Committee of the IEEE Computer Society, (1985).

[71] S. Wang, W. Liu, H. Lu et al. "*Periodicity of chaotic trajectories in realizations of finite computer precisions and its implication in chaos communications*". International journal of modern physics B, vol. 18, no 17n19, p. 2617-2622 (2004).

[72] J. Keller & H. Wiese. "*Period lengths of chaotic pseudo-random number generators*". Proceedings of the Fourth IASTED International Conference on Communication, Network and Information Security. ACTA Press, p. 7-11 (2007).

[73] S. Li, X. Mou & Y. Cai, "*Chaotic Crypography in Digital World: State-of-the-art, Problems and Solutions*". transformation, vol. 57, p. 58 (2006).

[74] B. L. Hao, "*Elementary symbolic dynamics and chaos in dissipative systems*". Singapore : World Scientific (1989).

[75] E. M. Bollt, "*Review of chaos communication by feedback control of symbolic dynamics*". International Journal of Bifurcation and Chaos, vol. 13, no 02, p. 269-285 (2003).

[76] T. Stojanovski, L. Kocarev & R. Harris, "*Applications of symbolic dynamics in chaos synchronization*". IEEE transactions on circuits and systems part 1 fundamental theory and applications, vol. 44, p. 1014-1017 (1997).

[77] H. Dimassi, "*Synchronisation des systèmes chaotiques par observateurs et applications à la transmission d'informations*". Thèse de doctorat. Paris 11 (2012).

[78] S. Atwal, "*Un système de communication à faible probabilité d'interception basé sur la modulation chaotique*". Thèse de doctorat. École de technologie supérieure (2010).

[79] Y. Lau, "*Techniques in Secure Chaos Communication*", Ph.D. Thesis, School of Electrical and Computer Engineering Science, RMIT University, Victoria, Australia (2006).

[80] A. Rukhin, J. Soto, J. Nechvatal et al. "*A statistical test suite for random and pseudorandom number generators for cryptographic applications*". Booz-allen and hamilton inc mclean va, 2001.

[81] C. Ling et X. Wu, "*A back-iteration method for reconstructing chaotic sequences in finite-precision machines*". Circuits, Systems & Signal Processing, vol. 27, no 6, p. 883-891 (2008).

[82] B. L. Hao & W. M. Zheng, "*Applied symbolic dynamics and chaos*". World scientific (1998).

[83] R. L. Devaney, "*An introduction to chaotic dynamical systems*" (2003).

[84] A. P. Kurian, & S. Puthusserypady, "*Secure digital communication using chaotic symbolic dynamics*". Turkish Journal of Electrical Engineering & Computer Sciences, vol. 14, no 1, p. 195-207 (2006).

[85] E. Alvarez, A. Fernandez, P. Garcıa, J. Jiménez & A. Marcano, "*New approach to chaotic encryption*". Physics Letters A, 263(4), 373-375 (1999).

[86] G. Alvarez et al. "*Cryptanalysis of a chaotic encryption system*". Physics Letters A 276.1, p.191-196 (2000).

[87] X. Wu, H. Hu & B. Zhang, "*Parameter estimation only from the symbolic sequences generated by chaos system*". Chaos, Solitons & Fractals, vol. 22, no 2, p. 359-366 (2004).

[88] D. Arroyo, G. Alvarez, S. Li et al. "*Cryptanalysis of a new chaotic cryptosystem based on ergodicity*". International Journal of Modern Physics B, vol. 23, no 05, p. 651-659 (2009).

[89] S. Li, X. Mou, Y. Cai et al. "*On the security of a chaotic encryption scheme: problems with computerized chaos in finite computing precision*". Computer physics communications, vol. 153, no 1, p. 52-58 (2003).

[90] G. Alvarez, J. M. Amigó, D. Arroyo et al. "*Lessons Learnt from the Cryptanalysis of Chaos-Based Ciphers*". Chaos-Based Cryptography. Springer Berlin Heidelberg, p. 257-295 (2011).

[91] A. Pallavisini, "*Système d'interférences radiofréquences pour la cryptographie par chaos appliquée aux transmissions hertziennes*". Thèse de doctorat. Université de Franche-Comté (2007).

[92] M. Halimi, "*Observation et détection de modes pour la synchronisation des systemes chaotiques: une approche unifiée*". Thèse de doctorat. Université de Lorraine (2013).

[93] A. J. Menezes, P. C. Van Oorschot & S. A. Vanstone, "*Handbook of applied cryptography*". CRC press (1996).

[94] X. Wu, H. Hu & B. Zhang, "*Parameter estimation only from the symbolic sequences generated by chaos system*". Chaos, Solitons & Fractals, vol. 22, no 2, p. 359-366 (2004).

[95] K. Wang, W. Pei, X. Hou et al. "*Symbolic dynamics approach to parameter estimation without initial value*". Physics Letters A, vol. 374, no 1, p. 44-49 (2009).

[96] S. Lian, J. Sun & Z. Wang, "*A block cipher based on a suitable use of the chaotic standard map*". Chaos, Solitons & Fractals, vol. 26, no 1, p. 117-129 (2005).

[97] A. F. Webster & S. E. Tavares, "*On the design of S-boxes*". Advances in Cryptology—CRYPTO'85 Proceedings. Springer Berlin Heidelberg, p. 523-534 (1986).

[98] S. Babbage, C. Canniere, A. Canteaut et al. " *The eSTREAM portfolio*". eSTREAM, ECRYPT Stream Cipher Project (2008).

[99] M. Rogawski, "*Hardware evaluation of estream candidates: Grain, lex, mickey128, salsa20 and trivium*". State of the art of stream ciphers (2007).

[100] I. Mantin & A. Shamir, "*A practical attack on broadcast RC4*". Fast Software Encryption. Springer Berlin Heidelberg, p. 152-164 (2002).

[101] J. Dj. Golić, V. Bagini & G. Morgari, "*Linear cryptanalysis of Bluetooth stream cipher*". Advances in Cryptology—EUROCRYPT 2002. Springer Berlin Heidelberg, p. 238-255 (2002).

[102] A. Maximov, T. Johansson & S. Babbage, "*An improved correlation attack on A5/1*". Selected areas in cryptography. Springer Berlin Heidelberg, p. 1-18 (2005).

[103] T. Wollinger, J. Guajardo & C. Paar, "*Security on FPGAs: State-of-the-art implementations and attacks*". ACM Transactions on Embedded Computing Systems (TECS), vol. 3, no 3, p. 534-574 (2004).

[104] Design Automation Standards Committee, "*IEEE standard for VHDL Register Transfer Level (RTL) synthesis*", IEEE std1076.6-1999, New York: IEEE press (1999).

[105] M. D. Galanis, P. Kitsos, G. Kostopoulos et al. "*Comparison of the Performance of Stream Ciphers for Wireless Communications*". In : International Conference on Computing, Communications and Control Technologies. p. 14-17 (2004).

[106] K. Gaj, G. Southern & R. Bachimanchi, "*Comparison of hardware performance of selected Phase II eSTREAM candidates*". State of the Art of Stream Ciphers Workshop (SASC 2007), eSTREAM, ECRYPT Stream Cipher Project, Report (2007).

[107] Digilent. "*Nexys3™ Board Reference Manual*", (2013).

http://www.digilentinc.com/Data/Products/NEXYS3/Nexys3_rm.pdf

[108] C. Guyeux, "*Le désordre des itérations chaotiques et leur utilité en sécurité informatique*". Thèse de doctorat. Université de Franche-Comté (2010).

[109] M. B. Luca, "*Apports du chaos et des estimateurs d'états pour la transmission sécurisée de l'information*". Thèse de doctorat. Université de Bretagne occidentale-Brest (2006).

[110] F. Anstett, "*Les systèmes dynamiques chaotiques pour le chiffrement: synthèse et cryptanalyse*", Thèse de doctorat, Université de Henri Poincaré, Nancy1 (2006).

[111] S. H. Strogatz, "*Non linear dynamics and chaos: Preseus Books Publishing*", LLC, 1994.

[112] O. Zehrour, "*Contribution à l'étude et à la classification du chaos dans les systèmes dynamiques*". Thèse de doctorat. Université Mentouri Constantine (2013).

[113] F. Alin, "*Contribution à la prédiction et au contrôle des comportements apériodiques dans les convertisseurs électromécaniques: Application de la théorie du chaos*". Thèse de doctorat, Reims (2005).

[114] M. Doulcier, "*Test intégré de circuits cryptographiques*". Thèse de doctorat. Université Montpellier II-Sciences et Techniques du Languedoc (2008).

[115] C. Berbain, "*Analyse et conception d'algorithmes de chiffrement à flot*". Thèse de doctorat. Université Paris Diderot (2007).

[116] M. Hell, T. Johansson & W. G. Meier, "*A stream cipher for constrained environments*". International Journal of Wireless and Mobile Computing, 2007, vol. 2, no 1, p. 86-93.

[117] T. Good, W. Chelton & M. Benaissa, "*Review of stream cipher candidates from a low resource hardware perspective*". SASC 2006 Stream Ciphers Revisited, p. 125 (2006).