République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Amar Thelidji- Laghouat

FACULTE DE TECHNOLOGIE

DEPARTEMENT D'ELECTRONIQUE

MEMOIRE DE MASTER

Réalisé par : Reggab Oumlkheir et Bendjaballah Aya

DOMAINE : Science et Technologie

FILIERE : Technologie

OPTION : Electronique des systèmes embarqués

Thème

Conception d'un système de chiffrement des signaux audio à base du chaos

Jury de soutenance :

Nom et Prénom	Grade	Qualité
Merah Lahcene	Pr	Encadrant
Seghier Abdelkrim	MAA	Examinateur
Ilyas Rougab	MCB	Président

Promotion : 2024/2025

ملخص

تعرض هذه الأطروحة نظامًا مبتكرًا لتشفير الصوت يعتمد على خرائط هينون الفوضوية المترابطة. ولمعالجة تأثيرات التكميم العددي، تم اقتراح آلية ما بعد المعالجة مبتكرة تشمل تقطيع البتات، وإعادة ترتيب المقاطع، وعمليات منطقية، مما حسّن بشكل كبير الخصائص العشوائية وحقق معدل نجاح بنسبة 100% في اختبارات NIST SP800-22 بدقة 32 بت . يضمن النظام درجة عالية من الإرباك والانتشار مع حساسية قصوى للظروف الابتدائية. وعلى الرغم من أن التنفيذ الحالي يتم بالمحاكاة، فإن تنفيذ النظام لاحقًا على FPGA يمثل اتجاهًا بالغ الأهمية لتطبيقات الأنظمة المدمجة الآمنة. وتُظهر النتائج الإمكانيات الكبيرة لهذا النهج في تشفير تدفقات الصوت بشكل قوي، من خلال دمج ديناميكيات الفوضى مع القوة التشفيرية ضمن بنية فعّالة مناسبة للمعالجة في الزمن الآني.

الكلمات المفتاحية: تشفير الصوت، الأنظمة الفوضوية ، خريطة هينون، السلاسل فوضوية، التكميم العددي، المعالجة غير الخطية اللاحقة • اختباراتNIST SP800-22 ، الإرباك والانتشار، الحساسية للظروف الابتدائية ، أمن المعلومات، أشباه المولدات العشوائية.

Résumé

Ce mémoire présente un nouveau système de chiffrement audio basé sur deux systèmes chaotiques de Hénon couplés. Pour contrer les effets de la quantification numérique, un mécanisme original de post-traitement (tranchage, réorganisation et opérations logiques) est proposé, améliorant significativement les propriétés aléatoires (100% de réussite aux tests NIST SP800-22 à 32 bits). Le système assure une forte confusion et diffusion, avec une sensibilité extrême aux conditions initiales. Bien que simulé dans cette étude, une implémentation matérielle sur FPGA constituera une perspective importante pour des applications embarquées sécurisées. Les résultats démontrent le potentiel de cette approche pour le chiffrement robuste de flux audio**.**

Mots-clés : carte de Hénon, cascade chaotique, quantification numérique, tests NIST SP800-22, confusion et diffusion, sensibilité aux conditions initiales, sécurité cryptographique, PRNG, chiffrement d’audio.

Abstract

This thesis presents a novel audio encryption system based on coupled chaotic Hénon maps. To address numerical quantization effects, an innovative post-processing mechanism (involving bit-slicing, segment reordering, and logical operations) is proposed, significantly enhancing random properties (achieving 100% success rate in NIST SP800-22 tests at 32-bit precision). The system ensures strong confusion and diffusion with extreme sensitivity to initial conditions. While currently implemented in simulation, future FPGA hardware implementation represents a crucial direction for secure embedded applications. The results demonstrate this approach's strong potential for robust audio stream encryption, combining chaotic dynamics with cryptographic strength in an efficient architecture suitable for real-time processing.

Keywords: Audio encryption, chaotic systems, Hénon map, chaotic cascade, Numerical quantization, NIST SP800-22 tests, confusion and diffusion, initial condition sensitivity, cryptography, PRNG.

Remerciement

Avant toute chose, nous rendons grâce à Allah, Le Tout-Puissant, Le Sage, pour nous avoir accordé la santé, la patience et la force nécessaires pour mener à bien ce travail. C'est grâce à Sa volonté et à Sa miséricorde que nous avons pu franchir les différentes étapes de ce mémoire.

Nous exprimons notre profonde gratitude à nos parents, pour leur amour sincère, leur soutien indéfectible et leurs prières constantes. Leur présence à nos côtés, dans les moments de doute comme dans les instants de réussite, a été une source essentielle de motivation.

Nos remerciements les plus sincères vont à notre encadrant, Merah Lahcene, pour sa disponibilité, ses conseils éclairés, et son accompagnement bienveillant tout au long de ce travail. Ses remarques pertinentes nous ont permis d'avancer avec rigueur et confiance.

Nous remercions également l'ensemble des enseignants de Université Amar Thelidji, pour la qualité de leur enseignement, leur engagement et leur dévouement qui ont largement contribué à notre formation.

Que chacun de vous trouve ici l'expression de notre reconnaissance la plus sincère.

Dédicace

À mes plus grands soutiens et sources d'inspiration, je dédie ce travail avec tout mon amour et une reconnaissance infinie.

À **ma mère**, qui a toujours été mon port d'attache et ma boussole, merci pour ton amour inconditionnel, ton dévouement et ton soutien inébranlable. Tu as été la lumière qui a guidé mes pas dans l'obscurité et tu as toujours cru en moi, même lorsque je doutais de moi-même.

À **mon père**, qui m'a transmis les valeurs du travail acharné, de la persévérance et de l'honnêteté, je te suis profondément reconnaissante pour tes conseils avisés et ton soutien sans faille. Tu m'as inspirée à viser haut et à croire en mes rêves. Merci pour ta confiance, ton amour et ta force.

À **mes frères** Oussama, Aïssa et Mouhamed, ainsi qu'à **ma sœur adorée** Soumia, qui êtes aussi mon bras droit, merci pour votre soutien constant, votre humour contagieux et votre présence réconfortante. Vous êtes ma source de joie et de courage, et je suis fière de vous avoir dans ma vie.

À **mon binôme Aya**, devenue une amie chère et une collaboratrice talentueuse, merci pour notre belle complicité, notre entraide et ta présence bienveillante. Ton esprit de coopération et ta détermination m'ont inspirée tout au long de ce parcours.

Enfin, au-delà des noms cités, il existe un cercle précieux de personnes qui ont marqué mon chemin. À vous toutes et tous, je vous exprime ma profonde gratitude pour votre présence et votre soutien qui ont enrichi ma vie.

Oumelkheir

À mes plus grands soutiens et sources d'inspiration, je dédie ce travail avec tout mon amour et une reconnaissance infinie.

À **ma mère**, qui a toujours été mon port d'attache et ma boussole, merci pour ton amour inconditionnel, ton dévouement et ton soutien inébranlable. Tu as été la lumière qui a guidé mes pas dans l'obscurité et tu as toujours cru en moi, même lorsque je doutais de moi-même.

À **mon père**, qui m'a transmis les valeurs du travail acharné, de la persévérance et de l'honnêteté, je te suis profondément reconnaissante pour tes conseils avisés et ton soutien sans faille. Tu m'as inspirée à viser haut et à croire en mes rêves. Merci pour ta confiance, ton amour et ta force.

À **mes frères**, ainsi qu'à **mes sœurs adorées**, merci pour votre soutien constant, votre humour contagieux et votre présence réconfortante. Vous êtes ma source de joie et de courage, et je suis fière de vous avoir dans ma vie.

À **mon binôme Omelkheir** , devenue une amie chère et une collaboratrice talentueuse, merci pour notre belle complicité, notre entraide et ta présence bienveillante. Ton esprit de coopération et ta détermination m'ont inspirée tout au long de ce parcours.

Enfin, au-delà des noms cités, il existe un cercle précieux de personnes qui ont marqué mon chemin. À vous toutes et tous, je vous exprime ma profonde gratitude pour votre présence et votre soutien qui ont enrichi ma vie.

Aya

SOMMAIRE

Liste des Figures

Chapitre 01 : Introduction Sur La Cryptographie

Chapitre 02 : Signaux chaotiques et cryptographie

Chapitre 3 : Conception et implémentation d'un système fiable de chiffrement audio

Liste des tableaux

Chapitre 3 : Conception et implémentation d'un système fiable de chiffrement audio

Introduction générale

Introduction Générale

À l'ère du numérique, la sécurité des communications est devenue un enjeu majeur, que ce soit pour protéger les données personnelles, les transactions financières ou les échanges gouvernementaux. La cryptographie, science ancestrale devenue incontournable, joue un rôle central dans cette protection en garantissant la confidentialité, l'intégrité, l'authenticité et la non-répudiation des informations échangées. Traditionnellement, les algorithmes cryptographiques reposent sur des fondements mathématiques rigoureux, comme le chiffrement symétrique (AES, DES) ou asymétrique (RSA, ECC). Cependant, face à l'évolution des technologies et des menaces, notamment avec l'avènement de l'informatique quantique, la recherche de nouvelles méthodes de chiffrement plus robustes et innovantes s'impose.

Parmi les approches prometteuses, la cryptographie chaotique émerge comme une alternative puissante, exploitant les propriétés uniques des systèmes dynamiques non linéaires. Ces systèmes, caractérisés par leur sensibilité extrême aux conditions initiales et leur comportement imprévisible, offrent des caractéristiques idéales pour la génération de séquences pseudo-aléatoires complexes, essentielles dans les algorithmes de chiffrement. Les signaux chaotiques, bien que déterministes, présentent une apparence aléatoire et une grande complexité, ce qui les rend difficiles à prédire ou à reproduire sans connaissance exacte des paramètres initiaux. Ces propriétés en font des candidats de choix pour concevoir des systèmes de chiffrement sécurisés et résistants aux attaques.

Ce mémoire s'inscrit dans cette dynamique en proposant une étude approfondie sur la conception et la simulation d'un système de chiffrement par flot innovant, basé sur les propriétés uniques des systèmes dynamiques chaotiques. Notre travail se concentre spécifiquement sur la sécurisation des signaux audio, dont l'importance croît avec le développement des communications vocales numériques, de la musique en streaming et des assistants vocaux intelligents.

L'originalité de notre approche réside dans l'exploitation d'une architecture cascade de deux systèmes de Hénon modifiés, combinée à un mécanisme novateur de post-traitement visant à compenser les limitations induites par la précision numérique finie. Cette conception permet de générer des séquences pseudo-aléatoires présentant des caractéristiques cryptographiques optimales, tout en maintenant une complexité algorithmique maîtrisée.

Notre étude s'articule autour de trois axes principaux développés dans les chapitres suivants :

- Fondements théoriques : Nous établissons le cadre conceptuel en présentant les principes de la cryptographie moderne et des systèmes chaotiques, avec un accent particulier sur leurs points de convergence. Ce chapitre met en lumière comment les propriétés intrinsèques du chaos (sensibilité aux conditions initiales, comportement ergodique, mélange topologique) peuvent être exploitées pour répondre aux exigences cryptographiques.

- Conception et simulation du système : Nous détaillons notre approche basée sur une double carte de Hénon interconnectée, enrichie d'un module de traitement numérique innovant. Une analyse rigoureuse évalue les performances du système à travers :

  - Des mesures de complexité (longueur de cycle, propriétés statistiques, etc.).
  - Des tests statistiques (suite NIST SP800-22).
  - Des analyses qualitatives (diagrammes de bifurcation, portraits de phase).
  - Des simulations de chiffrement/déchiffrement de signaux audio.

- Validation et perspectives : Nous démontrons l'efficacité de notre solution à travers des tests approfondis de sensibilité aux clés et d'analyse différentielle. Les résultats obtenus ouvrent des perspectives prometteuses pour une implémentation matérielle future sur FPGA, tout en soulignant l'adaptabilité potentielle du système à d'autres types de données multimédias.

L'importance pratique de cette recherche réside dans sa capacité à proposer une alternative viable aux générateurs pseudo-aléatoires conventionnels, particulièrement adaptée aux environnements contraints en ressources. Les simulations exhaustives menées sous MATLAB/Simulink valident non seulement les propriétés cryptographiques du système, mais aussi sa faisabilité technique pour des applications temps réel.

Cette étude contribue ainsi à l'effort continu d'innovation en sécurité informatique, en démontrant comment les systèmes dynamiques complexes peuvent enrichir l'arsenal cryptographique moderne. Les résultats obtenus posent les bases pour de futurs développements, notamment l'optimisation des performances en vue d'une implémentation matérielle, tout en ouvrant de nouvelles voies d'exploration pour la protection des flux multimédias sensibles.

CHAPITRE 01 : INTRODUCTION SUR LA CRYPTOGRAPHIE

1. Introduction

À l'ère du numérique, où les échanges d'informations sont omniprésents et souvent sensibles, la cryptographie s'impose comme une discipline incontournable pour assurer la confidentialité, l'intégrité, l'authenticité et la non-répudiation des données. Initialement utilisée pour protéger les communications militaires ou diplomatiques, la cryptographie a aujourd'hui envahi tous les aspects de la société moderne : transactions bancaires, communications électroniques, stockage en nuage, objets connectés, ou encore systèmes de vote électronique.

Ce chapitre vise à introduire les principes fondamentaux de la cryptographie, en fournissant une base théorique nécessaire à la compréhension des mécanismes de sécurité utilisés dans les systèmes d'information. Nous commencerons par définir les objectifs de la cryptographie et ses fonctions principales, avant de présenter les deux grandes familles d'algorithmes cryptographiques : la cryptographie symétrique et la cryptographie asymétrique. Seront également abordées des notions essentielles telles que les fonctions de hachage, les signatures numériques, et les certificats.

2. Définition et objectifs de la cryptographie

La cryptographie, du grec kryptos (caché) et graphein (écrire), est la science qui étudie les techniques permettant de protéger l'information en la rendant incompréhensible aux personnes non autorisées. Dans le contexte moderne de la sécurité informatique, elle repose sur des méthodes mathématiques rigoureuses pour garantir la confidentialité, l'intégrité, l'authenticité et la non-répudiation des données. On distingue principalement deux grandes familles de techniques : la cryptographie symétrique et la cryptographie asymétrique. Aujourd'hui, la cryptographie joue un rôle essentiel dans la protection des systèmes numériques, des communications électroniques et des infrastructures critiques.

La cryptographie poursuit quatre objectifs fondamentaux, communément appelés les piliers de la sécurité de l'information :

- **La confidentialité** garantit que l'information n'est accessible qu'aux personnes autorisées. Elle protège contre l'écoute passive et assure que même si des données sont interceptées, elles restent incompréhensibles sans la clé appropriée [1].

- **L'intégrité** assure que l'information n'a pas été modifiée de manière non autorisée. Elle permet de détecter toute altération, qu'elle soit accidentelle ou malveillante, garantissant ainsi la fiabilité des données transmises ou stockées [2].
- **L'authenticité** confirme l'identité de l'expéditeur d'un message ou de l'origine d'une donnée. Elle répond à la question "qui a créé cette information ?" et constitue un élément crucial dans les communications sécurisées [3].
- **La non-répudiation** empêche qu'une partie puisse nier avoir effectué une action ou envoyé un message. Elle fournit une preuve irréfutable de l'origine et de l'intégrité d'une transaction ou d'une communication [4].

3. Histoire brève de la cryptographie

L'histoire de la cryptographie s'étend sur plus de deux millénaires, évoluant des techniques manuelles simples aux algorithmes complexes de l'ère numérique.

L'Antiquité marque les premiers pas avec le chiffre de César (vers 50 av. J.-C.), où chaque lettre est remplacée par une lettre située à une position fixe dans l'alphabet. Bien que rudimentaire, ce système illustre déjà le principe de substitution qui reste fondamental en cryptographie moderne.

Le Moyen Âge voit l'émergence de techniques plus sophistiquées, notamment avec les travaux d'Al-Kindi au IXe siècle, qui développe la première méthode d'analyse de fréquence pour casser les chiffres de substitution. Cette période marque le début de la cryptanalyse scientifique (Kahn, 1996).

La Renaissance apporte des innovations majeures avec le chiffre de Vigenère au XVIe siècle, utilisant une clé répétée pour chiffrer le message. Ce système polyalphabétique résiste pendant des siècles à la cryptanalyse, étant surnommé "le chiffre indéchiffrable".

L'ère industrielle révolutionne la cryptographie avec l'invention de machines comme Enigma pendant la Seconde Guerre mondiale. Ces dispositifs mécaniques permettent des chiffrements complexes mais restent vulnérables aux attaques systématiques, comme l'a démontré le décryptage d'Enigma à Bletchley Park [5].

L'ère numérique débute véritablement dans les années 1970 avec deux révolutions majeures : l'adoption du DES (Data Encryption Standard) en 1977 comme premier standard de chiffrement civil, et surtout la publication en 1976 de l'article révolutionnaire de Diffie et Hellman introduisant la cryptographie à clé publique.

4. Principe de base de chiffrement/déchiffrement

La figure.1 décrie le principe de base de processus de chiffrement (cryptage) et de déchiffrement (décryptage). Comme illustré à la figure 1, un message initial, appelé **texte en clair** (*plaintext*), est transformé par un processus de chiffrement en un message illisible sans autorisation, appelé **texte chiffré** (*ciphertext* ou parfois *cryptogramme*). Le **chiffrement** est l'opération qui applique un algorithme, à l'aide d'une clé, pour coder le message. À l'inverse, le **déchiffrement** permet de reconstituer le texte original à partir du message chiffré à l'aide d'une clé appropriée.

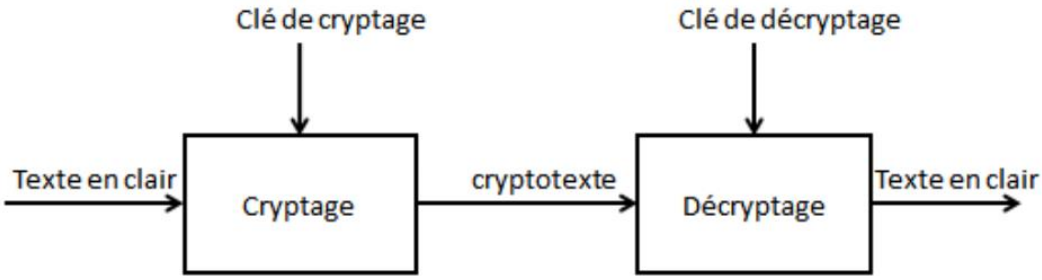

Figure.1. Un schéma de base d'un crypto-système.

Les deux processus, chiffrement et déchiffrement, sont conditionnés par une **clé cryptographique**, un paramètre fondamental qui garantit la sécurité et la confidentialité des échanges. En effet, sans connaissance de la clé, il est censé être extrêmement difficile, voire impossible, de retrouver le message original.

Sur le plan formel, la cryptographie peut être définie comme l'ensemble des règles, souvent mathématiques, destinées à assurer la confidentialité, l'intégrité et parfois l'authenticité des données. Le processus de chiffrement peut être représenté par une fonction :

$$E_k(M) = C \qquad (1)$$

Où:

- E_k : est la fonction de chiffrement paramétrée par la clé k.
- M : désigne le message en clair.
- C : est le message chiffré.

Le déchiffrement est l'opération inverse :

$$D_{k'}(C) = M \qquad (2)$$

Où:

- $D_{k'}$ est la fonction de déchiffrement paramétrée par une clé k',
- k et k' peuvent être identiques ou différents, selon le système utilisé.

Il est requis que pour tout message M, on ait :

$$D_{k'}\big(E_k(M)\big) = M \qquad (3)$$

Cela implique que la fonction de chiffrement E_k doit être injective, afin que chaque message chiffré provienne d'un seul message clair, et que la fonction de déchiffrement $D_{k'}$ soit surjective, de manière à pouvoir reconstruire tout message clair depuis un message chiffré valide.

Un **algorithme cryptographique** désigne l'ensemble des fonctions, mathématiques ou logicielles, utilisées pour assurer le chiffrement et le déchiffrement. Les clés k et k' appartiennent à un **espace des clés**, un ensemble contenant toutes les valeurs possibles que les clés peuvent prendre.

Ainsi, on distingue deux grandes catégories de systèmes cryptographiques, selon la relation entre k et k' :

- Cryptographie symétrique (ou à clé secrète), où la même clé est utilisée pour le chiffrement et le déchiffrement. Exemples : DES, AES, IDEA, Blowfish [6].
- Cryptographie asymétrique (ou à clé publique), où deux clés différentes mais mathématiquement liées sont utilisées : une pour le chiffrement (clé publique) et l'autre pour le déchiffrement (clé privée). Exemples : RSA, ElGamal, cryptosystèmes basés sur les courbes elliptiques (ECC) [7].

5. Typologies de cryptographie

Il existe deux grandes typologies de cryptographie : la cryptographie symétrique et la cryptographie asymétrique. Le type que j'ai choisi est la cryptographie symétrique, car elle utilise une seule clé pour chiffrer et déchiffrer les messages.

5.1. Cryptographie symétrique

La cryptographie symétrique, également appelée cryptographie à clé secrète, utilise la

même clé pour les opérations de chiffrement et de déchiffrement. Cette clé doit être partagée préalablement entre l'expéditeur et le destinataire et maintenue secrète pour garantir la sécurité du système [8].

Le processus se déroule en trois étapes (figure.2) : l'expéditeur chiffre le message en clair avec la clé secrète, le message chiffré est transmis par un canal potentiellement non sécurisé, et le destinataire déchiffre le message avec la même clé secrète pour retrouver le texte original.

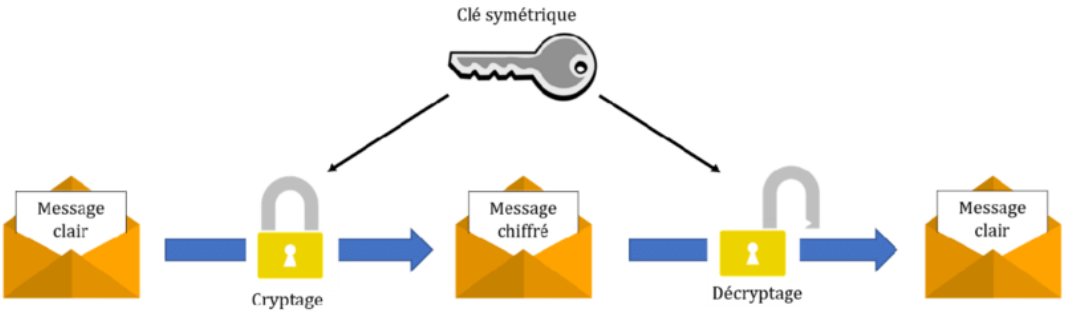

Figure.2. Principe de Base de la Cryptographie Symétrique.

La cryptographie à clé symétrique comprend deux types principaux : les chiffrements par blocs et les chiffrements par flot, chacun utilisant des méthodes distinctes pour sécuriser les données. Les deux reposent sur une clé secrète partagée pour le chiffrement et le déchiffrement, mais ils diffèrent dans la manière dont ils traitent le texte en clair et génèrent le texte chiffré :

- Les chiffrements par blocs **:** divisent le texte en clair en blocs de taille fixe (généralement 64 ou 128 bits) et chiffrent chaque bloc séparément. Si le texte en clair n'est pas un multiple parfait de la taille du bloc, un bourrage (*padding*) est ajouté pour combler l'espace restant.
- Les chiffrements par flot : Contrairement aux chiffrements par blocs, les chiffrements par flot chiffrent les données bit par bit ou octet par octet, ce qui les rend particulièrement adaptés aux communications en temps réel. Ils génèrent un flot de clés pseudo-aléatoire à partir d'une clé secrète, qui est ensuite combiné avec le texte en clair par une opération XOR pour produire le texte chiffré. Étant donné que les chiffrements par flot traitent les données de manière continue, ils ne nécessitent pas de bourrage.

5.1.1. AES (Advanced Encryption Standard)

Le Advanced Encryption Standard (AES) est un algorithme de chiffrement symétrique par

blocs qui constitue aujourd'hui le standard mondial pour la sécurisation des données sensibles. Il a été conçu par les cryptographes belges Joan Daemen et Vincent Rijmen sous le nom de Rijndael, et a été sélectionné en 2001 par le National Institute of Standards and Technology (NIST) pour succéder au Data Encryption Standard (DES), jugé vulnérable face aux progrès du calcul informatique [9].

L'AES chiffre les données en blocs fixes de **128 bits** organisés sous forme d'une matrice carrée de 4 lignes sur 4 colonnes, appelée État (*State*). L'algorithme supporte trois tailles de clés : 128, 192 et 256 bits, correspondant respectivement à 10, 12 et 14 tours de transformations cryptographiques successives. Chaque tour applique une combinaison d'opérations visant à assurer la confidentialité et la résistance aux attaques analytiques.

5.1.1.1. Les transformations fondamentales de l'AES

À chaque tour, quatre opérations principales sont effectuées sur la matrice (Figure.3) :

- SubBytes : chaque octet de l'État est remplacé par un autre selon une substitution non linéaire déterminée par une boîte S (*S-box*) calculée sur des inverses multiplicatifs dans le corps fini GF(2^8), suivie d'une transformation affine. Cette étape introduit de la confusion, notion introduite par Claude Shannon [Shannon, 1949].
- ShiftRows : les lignes de la matrice sont décalées circulairement d'un certain nombre de positions, augmentant la diffusion horizontale des données.
- MixColumns : les colonnes de l'État sont transformées par une multiplication matricielle dans GF(2^8), assurant une diffusion verticale efficace. Cette étape est cruciale pour propager les modifications d'un octet sur tout le bloc.
- AddRoundKey : une opération XOR est appliquée entre l'État courant et une sous-clé dérivée de la clé principale via un algorithme de dérivation clé. Cette étape lie directement la sécurité du chiffrement à la confidentialité de la clé.

5.1.1.2. Fondements théoriques et sécurité

La robustesse d'AES repose sur une application rigoureuse des principes de confusion et de diffusion définis par Shannon. L'utilisation d'algèbre linéaire dans GF(2^8) permet une bonne analyse mathématique et une complexité maîtrisée. AES est conçu pour résister à des attaques classiques telles que les attaques linéaires et différentielles [10]. À ce jour, aucune attaque pratique n'a compromis la version AES-256 lorsque celui-ci est correctement implémenté, bien

que certaines attaques par canaux auxiliaires (side-channel attacks) aient mis en évidence l'importance de l'environnement d'exécution [11].

En raison de sa sécurité éprouvée, le NIST recommande toujours AES pour la protection des informations classifiées, tout en préparant la transition vers des solutions post-quantiques, capables de résister à l'algorithme de Shor et aux autres menaces associées à l'informatique quantique [12].

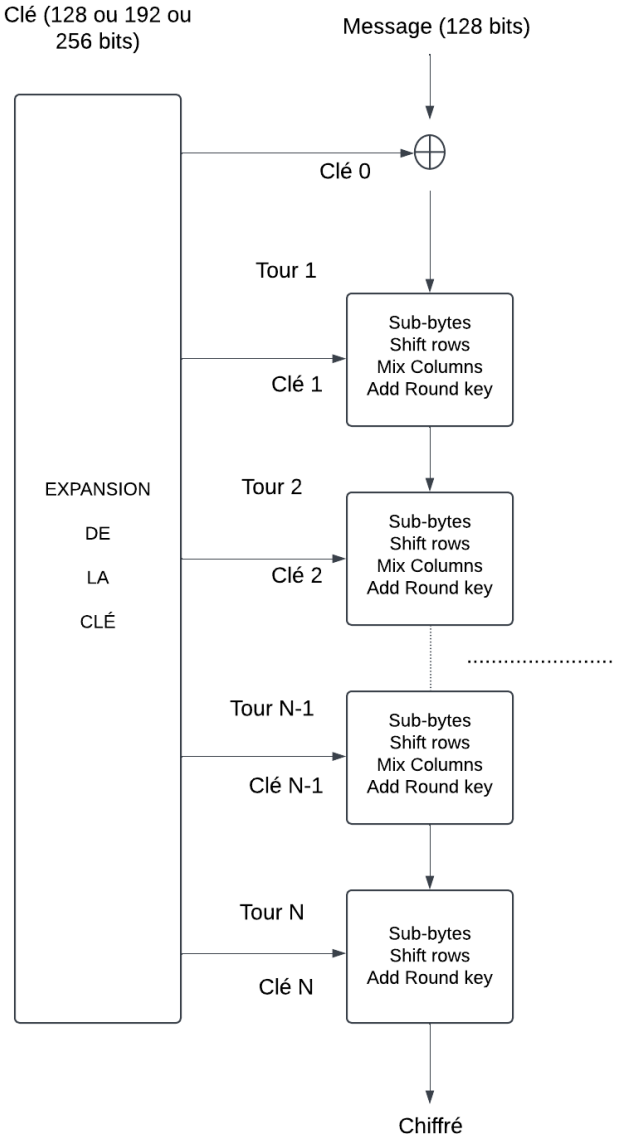

Figure.3. Mécanisme du chiffrement AES.

5.1.1.3. Applications et importance contemporaine

AES est aujourd'hui omniprésent dans la cybersécurité moderne : il sécurise les

communications HTTPS, les transactions bancaires, le chiffrement de disque (comme BitLocker ou FileVault), les réseaux sans fil (WPA2/WPA3), et bien d'autres systèmes critiques. Son architecture permet des implémentations rapides en matériel (ASIC, FPGA) comme en logiciel, et il est compatible avec des environnements embarqués aux ressources limitées [13].

Face à l'émergence de l'informatique quantique, des travaux explorent son renforcement ou sa combinaison avec des systèmes post-quantiques, bien que l'attaque de Grover ne réduise que de moitié l'espace de recherche de clés, maintenant AES-256 encore sécurisé dans ce nouveau paradigme [14].

En résumé, AES représente un équilibre remarquable entre rigueur théorique, performance pratique et résilience cryptographique, justifiant sa position dominante dans l'écosystème de la sécurité numérique.

6. Conclusion

Ce premier chapitre a permis d'établir les fondements théoriques essentiels de la cryptographie moderne. Nous avons vu que cette discipline repose sur quatre piliers fondamentaux - confidentialité, intégrité, authenticité et non-répudiation - qui garantissent la sécurité des échanges numériques.

L'analyse historique a montré l'évolution constante des techniques cryptographiques, depuis les méthodes anciennes comme le chiffre de César jusqu'aux algorithmes modernes tels qu'AES et RSA. Cette progression reflète l'adaptation permanente de la cryptographie aux nouveaux défis technologiques.

La distinction entre cryptographie symétrique (performante mais nécessitant un échange sécurisé des clés) et asymétrique (plus flexible mais plus complexe) a été clairement établie. L'étude détaillée de l'AES a notamment permis de comprendre comment les principes de confusion et de diffusion sont mis en œuvre dans un algorithme concret.

Ces bases théoriques constituent un socle indispensable pour aborder dans les chapitres suivants des approches plus innovantes, comme la cryptographie chaotique qui fera l'objet de notre prochaine étude. Les concepts présentés ici seront ainsi essentiels pour comprendre comment les systèmes dynamiques complexes peuvent enrichir l'arsenal cryptographique contemporain.

CHAPITRE 02 : SIGNAUX CHAOTIQUES ET CRYPTOGRAPHIE

1. Introduction

Dans le domaine de la sécurité de l'information, l'émergence de nouvelles approches basées sur des systèmes dynamiques non linéaires a suscité un intérêt croissant. Parmi ces approches, l'utilisation des signaux chaotiques s'est révélée prometteuse en tant que complément, voire alternative, aux méthodes classiques de cryptographie. Les systèmes chaotiques, bien que déterministes, présentent des comportements apparemment aléatoires, une sensibilité extrême aux conditions initiales, et une dynamique complexe difficile à prédire à long terme. Ces caractéristiques font des signaux chaotiques des candidats idéaux pour renforcer la confidentialité, l'authenticité et l'intégrité de l'information dans les systèmes de communication sécurisés.

Ce chapitre est consacré à l'étude des signaux chaotiques et à leur application en cryptographie. Nous commencerons par définir les concepts fondamentaux du chaos déterministe et explorerons les principales propriétés des systèmes chaotiques qui les rendent compatibles avec les exigences cryptographiques. Ensuite, nous passerons en revue les différents types de générateurs chaotiques, qu'ils soient analogiques ou numériques, et les méthodes utilisées pour intégrer ces signaux dans les mécanismes de chiffrement.

2. Définition du chaos

Le monde qui nous entoure est rempli de phénomènes qui semblent irréguliers et aléatoires, tant dans l'espace que dans le temps. Explorer l'origine de ces phénomènes est généralement une tâche vaine en raison du grand nombre d'éléments impliqués ; on se contente donc souvent de considérer ces processus comme du bruit [15]. Toutefois, de nombreuses découvertes récentes ont montré que certains phénomènes complexes peuvent apparaître dans des systèmes simples. Le chaos fait partie de ces phénomènes, qui présentent des comportements complexes issus de processus déterministes simples. Il est souvent qualifié de « science des surprises », car il se caractérise par la non-linéarité, l'irrégularité, l'imprévisibilité, l'incertitude, l'instabilité, et une apparence aléatoire [16].

Le terme « chaos » est en quelque sorte l'opposé du terme « stabilité ». Lorsqu'un système est dit stable, cela signifie qu'il est prévisible et issu d'un processus déterministe. La science classique traite principalement de phénomènes supposés prévisibles comme la gravité, l'électricité ou les réactions chimiques. Les systèmes déterministes sont au cœur de la physique classique, avec les lois de Newton, l'électrodynamique ou encore la thermodynamique. En théorie, si les conditions initiales sont connues avec une précision suffisante, l'évolution future du système est totalement prévisible. Cependant, la théorie du chaos s'intéresse à des systèmes non linéaires dont

le comportement est pratiquement impossible à prévoir ou à contrôler, comme les turbulences, la météo, les marchés financiers, ou encore les états du cerveau [17].

Les scientifiques ont été surpris de constater que le chaos – où une infime perturbation peut entraîner une transformation majeure à un moment ultérieur – n'a en réalité rien à voir avec le hasard pur. Même si les événements individuels restent imprévisibles, il est souvent possible d'extraire des régularités statistiques sur de longues périodes [18]. Le chaos représente ainsi un comportement temporel complexe dans des systèmes simples. Contrairement à l'usage courant, le chaos n'est ni spatial ni un simple désordre, mais plutôt une forme d'évolution dynamique.

Ce phénomène est observable aussi bien dans les systèmes naturels (biologie, climatologie, chimie) que dans les systèmes artificiels (comme les circuits électroniques), ces derniers pouvant être modélisés à l'aide d'équations différentielles pour les systèmes continus ou de fonctions récursives pour les systèmes discrets [19]. Entre stabilité et instabilité s'étend un large spectre où différentes disciplines scientifiques trouvent leur place. À une extrémité, on retrouve les systèmes linéaires, réguliers, stables et déterministes ; à l'autre, des systèmes hautement instables, irréguliers, non déterministes et stochastiques. Le chaos se situe à mi-chemin de ce spectre. Il partage le caractère déterministe des systèmes réguliers tout en présentant une dynamique irrégulière qui le rapproche du bruit (Figure.2.1).

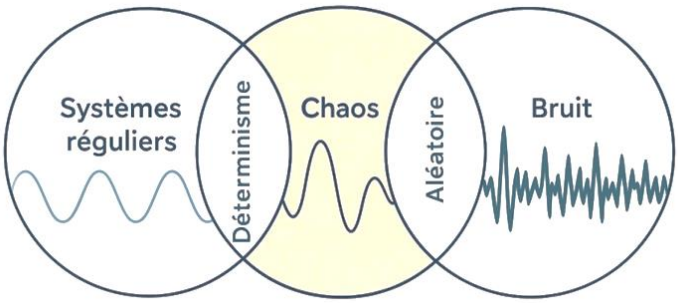

Figure.2.1 : Diagramme des propriétés partagées entre les systèmes chaotiques.

La figure 2.1 illustre, à travers un diagramme de Venn, les relations entre trois types de signaux : les systèmes réguliers, les systèmes chaotiques et le bruit. Les systèmes réguliers, tels que les signaux périodiques (ex. : sinusoïdes), sont purement déterministes et présentent un comportement parfaitement prévisible. À l'opposé, les signaux de bruit, comme le bruit blanc, sont aléatoires et totalement imprévisibles, sans structure déterminée. Les systèmes chaotiques occupent une position intermédiaire entre ces deux extrêmes. Bien qu'ils soient décrits par des équations déterministes, leur évolution est extrêmement sensible aux conditions initiales, ce qui les rend difficilement prévisibles et donne à leur comportement une apparence aléatoire. Cette

double nature, à la fois déterministe et apparemment aléatoire, distingue le chaos des autres types de signaux et en fait un outil particulièrement intéressant pour les applications en cryptographie, où la complexité et l'imprévisibilité sont recherchées sans renoncer à la reproductibilité.

3. Origines du chaos

L'histoire du chaos puise ses racines dans les travaux de Poincaré, mais ce n'est qu'avec l'avènement des ordinateurs que ses développements majeurs ont pu voir le jour. En effet, les calculs numériques ont permis l'intégration rapide d'équations différentielles complexes et la visualisation immédiate des trajectoires dynamiques, deux éléments indispensables au développement de la théorie moderne du chaos et des géométries fractales.

Au début du XX^{e} siècle, Henri Poincaré étudia la stabilité du système solaire et montra que les petits écarts dans les conditions initiales, dans des systèmes à trois corps ou plus, peuvent provoquer des divergences imprévisibles. C'est ainsi qu'il posa les premières pierres de l'imprévisibilité algorithmique dans les systèmes déterministes [20].

Ce concept fit son entrée dans la conscience scientifique en 1963 grâce à Edward Lorenz. En simulant un modèle simplifié de convection atmosphérique sur ordinateur, il remarque que de légères variations des conditions initiales entraînent des évolutions complètement différentes. Cet effet, vite baptisé « effet papillon », illustre parfaitement ce que l'on appelle désormais la sensibilité aux conditions initiales dans les systèmes déterministes non linéaires [21].

La carte logistique constitue un autre jalon théorique important. Introduite par Verhulst dès 1838 pour décrire la dynamique des populations, elle fait l'objet d'analyses plus poussées au XX^{e} siècle, notamment par Robert May, démontrant qu'elle peut exhiber des comportements chaotiques en fonction de ses paramètres [22].

Enfin, en 1990, Pecora et Carroll marquent un tournant en démontrant que deux systèmes chaotiques identiques peuvent être synchronisés. Ce résultat ouvre la voie à un contrôle actif du chaos et à des applications pratiques, notamment dans le domaine de la cryptographie [23].

Aujourd'hui, la théorie du chaos reste un champ de recherche extrêmement dynamique, couvrant la biologie, la chimie, la finance, la météorologie ou encore la neuroscience. En cryptographie, le chaos fournit une imprévisibilité déterministe que l'on exploite pour générer des signaux sécurisés.

4. Propriétés des Systèmes Chaotiques et leur Caractérisation

Les systèmes chaotiques présentent des comportements complexes et fascinants qui défient notre intuition habituelle des systèmes déterministes. Bien que ces systèmes soient gouvernés par des équations déterministes, ils exhibent des dynamiques apparemment aléatoires et imprévisibles. La caractérisation de ces propriétés chaotiques nécessite des outils mathématiques sophistiqués développés dans le cadre de la théorie ergodique et de l'analyse des systèmes dynamiques non linéaires [24].

4.1 Sensibilité aux Conditions Initiales

La propriété la plus emblématique des systèmes chaotiques est leur **sensibilité extrême aux conditions initiales,** souvent illustrée par la métaphore de l'« effet papillon ». Cette caractéristique fondamentale signifie que deux trajectoires initialement très proches dans l'espace des phases divergent exponentiellement au cours du temps. Mathématiquement, cette divergence peut être quantifiée par les exposants de Lyapunov.

Pour deux trajectoires initialement séparées par une distance δ_0, la distance δ(t) au temps t évolue selon :

$$\delta(t) \approx \delta_0 e^{(\lambda t)} \qquad (4)$$

Où λ représente l'exposant de Lyapunov dominant. Un système est considéré comme chaotique si au moins un de ses exposants de Lyapunov est positif [25].

4.2 Attracteurs Étranges

Les systèmes chaotiques sont caractérisés par l'existence d'attracteurs étranges dans leur espace des phases. Ces attracteurs présentent une structure géométrique complexe, souvent fractale, qui confine les trajectoires du système tout en permettant leur comportement chaotique. Contrairement aux attracteurs classiques (points fixes, cycles limites), les attracteurs étranges possèdent une dimension fractale non entière.

La structure géométrique de ces attracteurs peut être analysée à travers différentes dimensions fractales, notamment la dimension de corrélation et la dimension de Hausdorff, qui quantifient la complexité spatiale de l'attracteur [26].

4.3 Propriétés Ergodiques et de Mélange

Les systèmes chaotiques exhibent des propriétés statistiques remarquables liées à l'ergodicité et au mélange. L'ergodicité assure que les moyennes temporelles convergent vers les moyennes d'ensemble, permettant une description statistique cohérente du système. La propriété de mélange topologique garantit que toute région de l'espace des phases finira par intersecter toute autre région sous l'action de la dynamique.

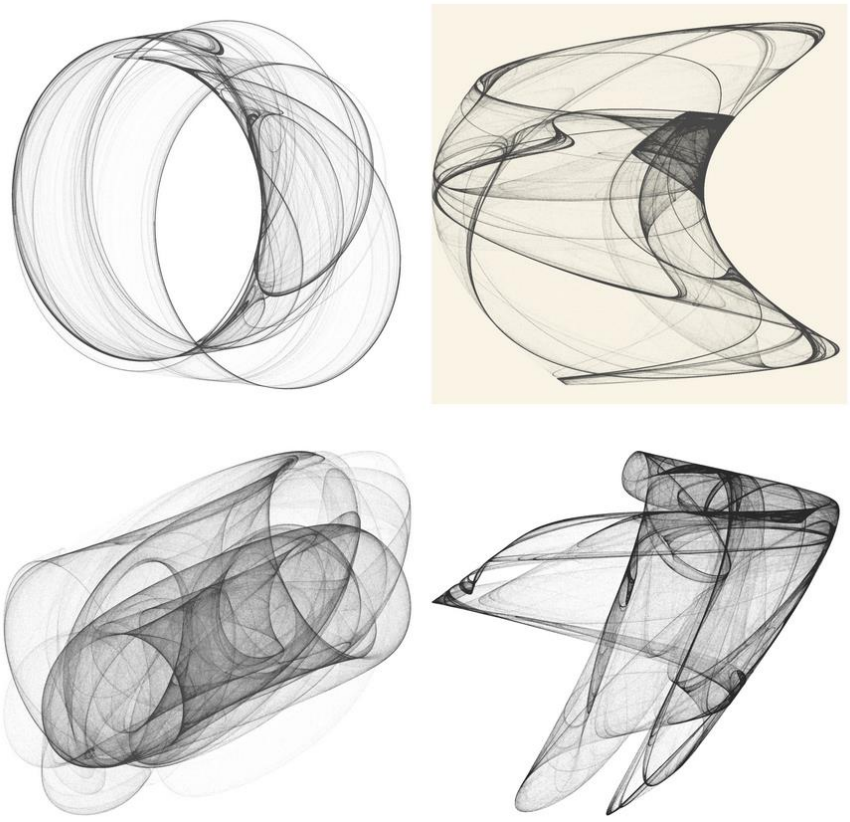

Figure.2.2 : Exemples des structures géométriques complexes attracteurs étranges.

Ces propriétés sont intimement liées à la production d'entropie dans le système et à sa capacité à "oublier" l'information concernant ses conditions initiales [27].

5. Méthodes de Caractérisation

La caractérisation quantitative des systèmes chaotiques nécessite l'utilisation d'outils mathématiques spécialisés permettant de mesurer et d'analyser leurs propriétés distinctives. Ces méthodes, développées dans le cadre de la théorie des systèmes dynamiques, offrent des moyens rigoureux pour identifier et quantifier le comportement chaotique. Les principales techniques incluent le calcul des exposants de Lyapunov pour mesurer la sensibilité aux conditions initiales, l'analyse des dimensions fractales pour caractériser la géométrie des attracteurs, ainsi que diverses approches spectrales et topologiques. L'application combinée de ces méthodes permet une caractérisation complète et fiable des systèmes chaotiques [28].

6. Exemples des systèmes chaotiques

Cette section présente brièvement les attracteurs chaotiques (continue et discrets) existants, on présente L'attracteur de Lorenz le plus connu ainsi la carte Logistique, et le reste sera présenté brièvement.

6.1. L'attracteur chaotique de Lorenz

L'équation de Lorenz est formulée par le météorologue américain du même nom pour la première fois en 1963. Elle résulte alors d'une grande simplification de l'Équation de Navier-Stockes, qui décrit le mouvement des fluides newtoniens et est réputée comme étant très difficile à résoudre. Les importantes approximations réalisées pour aboutir à l'équation de Lorenz sont telles qu'elle n'a en fait plus vraiment de sens physique, mais elle présente un réel intérêt pour les mathématiques. À partir de simulations numériques, Lorenz va rapidement découvrir deux caractéristiques majeures de son équation : la grande sensibilité aux conditions initiales des solutions et l'étrange forme de "papillon" prise par toutes les solutions, que l'on appellera par la suite "attracteur étrange".C'est ce qu'il publiera dès 1963[28]. Mais l'engouement des autres mathématiciens pour cette découverte ne naîtra en 1972, lorsqu'il tiendra une conférence devant l'American Association for the Advancement of Science au titre provoquant :
« Predictability : Does the Flap of a Butterfly's Wings in Brazil Set off a Tornado in Texas » [29].

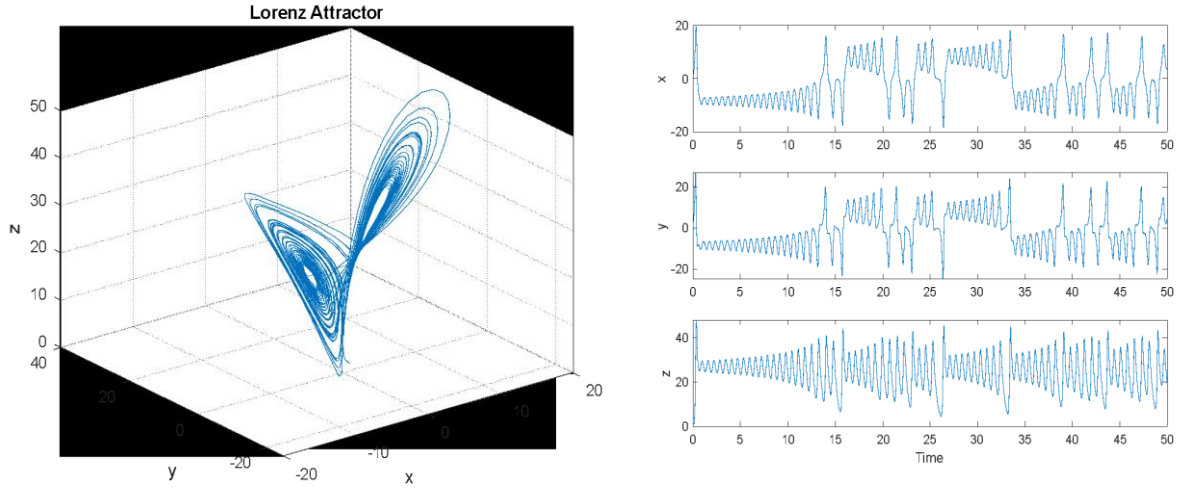

Figure.2.3 : la dynamique du système de Lorenz

La figure ci-dessus illustre le comportement chaotique du système de Lorenz à travers deux représentations complémentaires :

- À gauche, l'attracteur de Lorenz est visualisé dans l'espace tridimensionnel des phases (x,y ,z) . On y observe une trajectoire complexe, non périodique, confinée dans une région limitée de l'espace. Cette structure en double spirale caractéristique, souvent comparée à des ailes de papillon, est un exemple typique d'attracteur étrange, signature d'un chaos déterministe. Bien que la trajectoire ne repasse jamais exactement deux fois au même endroit, elle reste bornée, ce qui témoigne d'une dynamique ordonnée dans le désordre apparent.
- À droite, les graphiques montrent l'évolution temporelle des trois variables x(t), y(t) et z(t). Ces courbes illustrent la sensibilité aux conditions initiales ainsi qu'un comportement quasi-irrépétable. Les oscillations irrégulières, sans périodicité claire, confirment la nature chaotique du système. Néanmoins, on observe certaines structures récurrentes localement, ce qui distingue le chaos du bruit totalement aléatoire.

Ces visualisations permettent de valider visuellement la complexité du système de Lorenz et de justifier son utilisation comme générateur chaotique en cryptographie, grâce à sa grande entropie, sa dynamique imprévisible, et sa structure déterministe sous-jacente.

Le système de Lorenz est un modèle mathématique à trois équations différentielles non linéaires, Ce système est défini comme suit :

$$\left\{\sigma(y - x) \; = \frac{dx}{dt}\; x(\rho \; - \; z) \; - \; y = \frac{dy}{dt}\; xy \; - \; \beta z = \frac{dz}{dt}\right\} \qquad (5)$$

- x : correspond à l'intensité de la circulation convective.
- y : représente la différence de température horizontale.
- Z : mesure la variation verticale de température.
- σ, ρ et β sont des paramètres du contrôle [29].

6.2. L'attracteur chaotique de Rössler

L'attracteur de Rössler est l'attracteur associé au système dynamique de Rössler, un système de trois équations différentielles non-linéaires. Ces équations différentielles définissent un système dynamique continu et tridimensionnel qui présente des caractéristiques chaotiques. Otto Rössler conçut son attracteur en 1976dans un but purement théorique, mais ces équations s'avérèrent utiles dans la modélisation de l'équilibre dans les réactions chimiques. Ce système est minimal pour le chaos continue pour au moins trois raisons : son espace des phases a une dimension minimale de trois comme Lorenz, sa non-linéarité est minimal, car il y a un seul terme quadratique et il génère un attracteur chaotique avec un seul lobe, contrairement à l'attracteur de Lorenz qui a deux lobes [30].

Rössler s'est appuyé sur l**'intuition géométrique** des écoulements en dimension trois et sur le **principe de réinjection**, typique des systèmes de type relaxation. Ces derniers présentent souvent une **variété lente en forme de Z** dans l'espace des phases, qui permet de modéliser des dynamiques complexes avec récurrence. Les équations de ce système de Rössler sont :

$$\left\{\frac{dx}{dt} = -y - z \qquad \frac{dy}{dt} = x + ay \qquad \frac{dz}{dt} = b + z(x - c)\right\} \qquad (6)$$

Rössler étudia l'attracteur pour a = 0.2, b = 0.2 et c = 5.7, mais les propriétés de a= 0.2, b = 0.2 et c = 14 sont aujourd'hui plus étudiées. On prend ces dernières valeurs et avec x_0=0, y_0=0 et z_0=0, on aura le graphique présenté sur la Figure.2.4.

Une orbite dans l'attracteur suit une spirale proche du plan x, y autour d'un point fixe instable. S'éloignant progressivement de ce point fixe, un second point fixe provoque une élévation de cette orbite et une redescende vers le plan x, y proche du premier point fixe, réintégrant l'orbite dans la

spirale. Bien que les valeurs des différentes variables soient bornées, il est apparent que ces oscillations sont chaotiques.

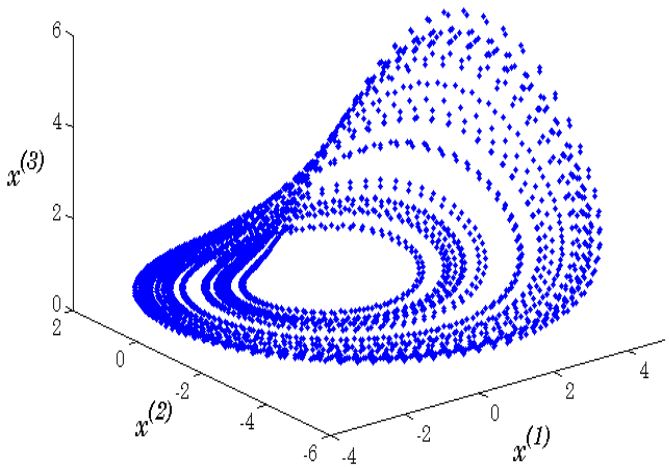

Figure.2.4 : L'attracteur chaotique de Rössler.

6.3. L'attracteur chaotique de Hénon

Michel Hénon est un astronome français. Il avait pris contact avec le chaos en 1962 avec son étudiant Carl Heiles, en étudiant à l'ordinateur les trajectories correspondant à un système d'équations différentielles hamiltoniens (sans frottement) [31].

En 1976, il connaissait l'attracteur de Lorenz et, en simplifiant les équations, aboutit à l'attracteur qui porte son nom. Il s'agit d'une application très simple, un peu analogue à l'application logistique, mais dans un plan. Ces itérations sont définies par les relations suivantes :

$$\{x_{k+1} = 1 + y_k - ax_K^2\, y_k = bx_k \qquad (7)$$

On prendra pour conditions initiales (x0, y0) = (-0.4, 0.3), conditions initiales contenues dans le bassin d'attraction. De plus, on prendra les valeurs suivantes : a = 1.4 et b = 0.3. Ces valeurs furent proposées par Michel Hénon et permettent d'observer un comportement chaotique comme montre la Figure.2.5. L'attracteur de Hénon pour les valeurs choisies et pour 50000 itérations est donné par la figure suivante :

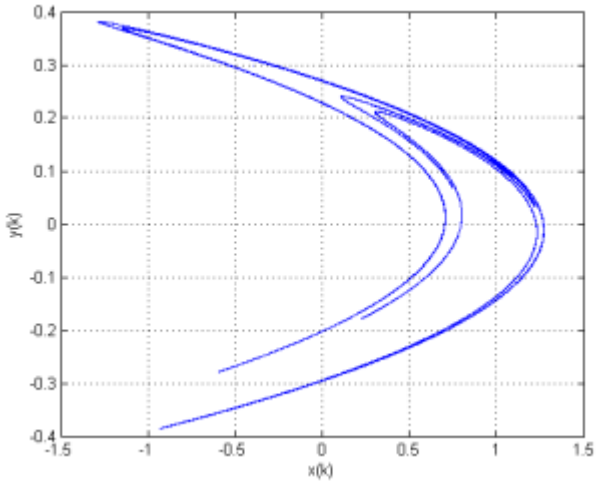

Figure.2.5 : L'attracteur chaotique de Hénon

Nous avons vu jusqu'à maintenant trois attracteurs chaotiques numériques, mais il existe d'autres attracteurs numériques que nous ne pouvons pas les étudier à la fois. On peut citer quelques-uns comme :

- L'attracteur de Curry et Yorke.
- L'attracteur de Peter de Jong.
- L'attracteur de Hénon-Lozi.
- L'attracteur d'Ikeda.
- L'attracteur de Wallpaper.
- L'attracteur de Mira.
- L'attracteur de Clifford.

7. Exposants de Lyapunov

Les exposants de Lyapunov constituent l'outil principal pour quantifier la sensibilité aux conditions initiales. Pour un système dynamique de dimension **n**, il existe **n** exposants de Lyapunov $\lambda_1 \geq \lambda_2 \geq ..... \geq \lambda_n$ qui caractérisent les taux moyens de divergence ou de convergence dans chaque direction de l'espace des phases.

Le calcul numérique des exposants de Lyapunov nécessite des algorithmes sophistiqués qui suivent l'évolution des vecteurs tangents le long des trajectoires [32]. La présence d'au moins un exposant positif constitue une signature claire du chaos déterministe.

8. Analyse Spectrale et Entropie

L'analyse du spectre de puissance révèle la nature *broadband* du signal chaotique, contrastant avec les pics discrets caractéristiques des systèmes périodiques ou quasi-périodiques. Cette analyse fréquentielle, combinée au calcul de l'entropie spectrale, permet de distinguer le chaos du bruit stochastique.

L'entropie topologique mesure le taux de production d'information par le système dynamique et est étroitement reliée à la somme des exposants de Lyapunov positifs par la formule de Pesin [32].

9. Relation entre la cryptographie et le chaos

La cryptographie et les systèmes chaotiques partagent plusieurs caractéristiques fondamentales, ce qui rend leur combinaison naturelle et puissante. Pour mieux comprendre cette relation, on peut établir des comparaisons entre les propriétés du chaos et les principes cryptographiques classiques.

Par exemple, en cryptographie, la diffusion signifie qu'un petit changement dans le message ou dans la clé doit entraîner un changement important dans le texte chiffré. Cela rappelle directement la sensibilité aux conditions initiales des systèmes chaotiques : une minuscule variation dans l'état initial du système produit une trajectoire complètement différente. Ainsi, comme une bonne méthode de chiffrement brouille totalement le message d'origine, un système chaotique rend toute prédiction impossible sans une connaissance parfaite des conditions de départ.

De même, bien que les signaux chaotiques semblent désordonnés, ils obéissent à des règles déterministes. Cela rejoint le principe selon lequel un algorithme de chiffrement est toujours déterministe : avec la même clé et le même message, il produira toujours le même résultat. Ce déterminisme caché sous une apparente complexité rend les signaux chaotiques idéaux pour synchroniser un émetteur et un récepteur dans un système de communication sécurisé.

Enfin, les systèmes chaotiques sont souvent utilisés pour générer des séquences pseudo-aléatoires, semblables aux clés cryptographiques. Leur complexité empêche un attaquant de deviner la clé ou de reconstruire le message, même s'il intercepte une partie du signal.

Ainsi, les propriétés du chaos — complexité, imprévisibilité apparente, sensibilité extrême, mais aussi déterminisme — trouvent une correspondance directe dans les exigences de la cryptographie moderne. L'un complète l'autre, et leur combinaison ouvre la voie à des méthodes de chiffrement innovantes, particulièrement résistantes aux attaques.

10. Conclusion

La cryptographie basée sur le chaos exploite des phénomènes physiques et mathématiques non-linéaires pour générer des systèmes de chiffrement puissants, robustes, et parfois plus légers à implémenter que ceux issus de l'algèbre discrète. La synchronisation, la sensibilité, la confusion et le déterminisme sont autant de passerelles naturelles entre le chaos et la cryptographie. Cette convergence ouvre de nouvelles perspectives pour la sécurité des communications, notamment dans les domaines embarqués, l'Internet des Objets (IoT), et les systèmes à contraintes temps réel.

Chapitre 03 : CHAPITRE 03 : CONCEPTION ET IMPLÉMENTATION D'UN SYSTÈME FIABLE DE CHIFFREMENT AUDIO

1. Introduction

Ce chapitre se concentre sur la conception d'un système de chiffrement par flot appliqué aux signaux audio, fondé sur l'exploitation de deux systèmes chaotiques de Hénon configurés en cascade afin de renforcer la complexité du flux pseudo-aléatoire généré. Pour pallier l'effet néfaste de la précision numérique limitée en implémentation matérielle, nous proposons un mécanisme fiable d'amélioration des caractéristiques aléatoires du système chaotique, garantissant une uniformité et une imprévisibilité accrues malgré les contraintes de représentation finie.

L'architecture repose sur l'enchaînement contrôlé de deux cartes de Hénon, de manière à amplifier l'imprévisibilité et à diversifier les états internes du générateur. Le mécanisme d'amélioration agit à chaque itération pour corriger les biais introduits par l'arithmétique à virgule fixe, assurant ainsi que le flux binaire conserve des propriétés chaotiques robustes. De plus, ce mécanisme étend les plages des paramètres de contrôle pour maintenir le comportement chaotique, ce qui se traduit par une robustesse accrue et par une augmentation de la taille de la clé, construite à partir de ces paramètres.

La méthode de génération de clés pseudo-aléatoires exploite conjointement les sorties des deux systèmes chaotiques et le mécanisme d'amélioration, produisant un flot binaire qui satisfait aux exigences d'un chiffrement par flot : non-périodicité, forte dépendance aux paramètres initiaux et bonne diffusion. Les contraintes de précision sont étudiées pour garantir la reproductibilité des séquences dans un contexte FPGA.

Pour valider le caractère chaotique et la qualité du générateur ainsi obtenu, nous évaluons plusieurs indicateurs : l'autocorrélation, batteries de tests statistiques standard (NIST SP800-22), etc. Ces analyses démontrent la pertinence du mécanisme proposé comme correctif à la dégradation chaotique due à la quantification numérique.

Enfin, le système de chiffrement par flot est appliqué à des signaux audio numériques (extraits vocaux et musicaux). Une étude de performance porte sur la qualité de restitution, la sensibilité aux paramètres, la diffusion, ainsi que la résistance à diverses attaques. Les résultats confirment que l'approche par cascade chaotique enrichie du mécanisme d'amélioration constitue une solution fiable et efficace pour le chiffrement sécurisé de contenu audio.

2. Le système chaotique de Hénon

Le système chaotique de Hénon, déjà présenté en détail au chapitre 2, est ici exploité comme base pour la conception d'un chiffrement symétrique par flot. Ce système dynamique discret à deux dimensions, régi par des équations quadratiques, présente un comportement chaotique fortement dépendant des conditions initiales et des paramètres de contrôle. Il est défini par le système suivant :

$$\begin{cases} x_{k+1} = \alpha + y_k - a x_k^2 \\ g \\ y_{k+1} = b x_k \end{cases} \quad (1)$$

Avec a et b comme paramètres de contrôle. Pour les valeurs classiques a=1.4, b=0.3 et $\alpha = 1$ (dans cette étude en considérant ce 3^{éme} paramètre) le système présente un comportement chaotique. La Figure.3.1 présente la phase d'espace et les signaux de sortie de système.

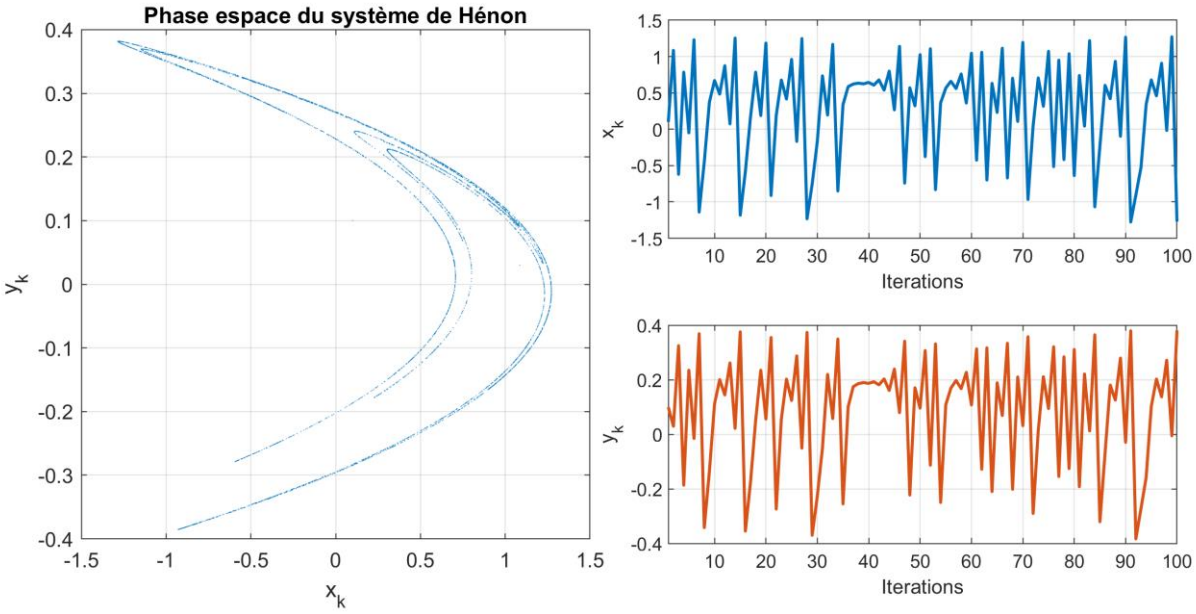

Figure.3.1 : Attracteur de Hénon : espace des phases et signaux temporels.

Le système de Hénon a été implémenté en arithmétique fixe à l'aide de ***Vitis Model Composer***, un outil de conception par modèles intégré à MATLAB/Simulink. ***Vitis Model Composer*** est conçu pour développer rapidement via des blocs optimisés pour DSP, générer automatiquement du code HDL/HLS/AI Engine, et préparer les conceptions pour une production sur FPGA/SoC AMD.

Grâce à cet outil, nous pouvons simuler l'exactitude fonctionnelle du système de Hénon tout en bénéficiant de la conversion vers l'implémentation en virgule fixe — essentielle pour l'adaptation au FPGA. L'utilisation de types de données *x_sfix…* permet de contrôler précisément la longueur des mots et la position de la virgule, garantissant la qualité numérique de l'implémentation.

Vitis Model Composer offre plus de 200 blocs prédéfinis (HDL, HLS, AI Engine), ainsi que la possibilité d'importer du code personnalisé pour enrichir les modèles. Cela a permis de prototyper et d'optimiser efficacement le générateur chaotique, avec une validation bit-par-bit et cycle-par-cycle avant génération de RTL [33].

En résumé, l'utilisation de Vitis Model Composer nous a permis de réaliser une implémentation fiable du système de Hénon en virgule fixe, avec une chaîne complète allant du prototypage MATLAB/Simulink à la production matérielle sur FPGA.

2.1. Effet de la précision numérique sur la dynamique chaotique

La quantification numérique (arithmétique à virgule fixe ou flottante de faible précision) dégrade fortement la dynamique chaotique du système de Hénon. En remplaçant l'infini des valeurs réelles par un ensemble discret, les erreurs d'arrondi et de troncature s'accumulent, provoquant l'effondrement des trajectoires sur des cycles périodiques ou points fixes, au lieu de rester dans un attracteur chaotique.

Plus spécifiquement, même avec des précisions modérées (de l'ordre de 8 à 16 bits), l'entropie diminue, et l'exposant de Lyapunov tend vers zéro ou devient négatif, indiquant la perte du comportement chaotique attendu. Les trajectoires deviennent prévisibles et la richesse pseudo-aléatoire s'effondre.

Ces phénomènes sont bien documentés dans la littérature sur les systèmes numériques à précision finie (carte logistique, Hénon, etc.). Ils constituent un risque majeur lorsqu'on les exploite dans des générateurs de clés, car ils compromettent l'imprévisibilité et la robustesse cryptographique — fondamentales pour un chiffrement sécurisé.

2.2. Evaluation de système de Hénon numérisé

Cette section a pour objectif d'évaluer le comportement chaotique du système de Hénon en tenant compte de différentes tailles de précision en virgule fixe. Nous cherchons ainsi à déterminer dans quelle mesure la quantification numérique affecte la génération de séquences

pseudo-aléatoires et l'aptitude du système à conserver son caractère chaotique. Pour ce faire, plusieurs indicateurs seront utilisés, le calcul de la longueur de cycle, les digrammes de bifurcation, et les tests statistiques standardisés. Cette analyse est essentielle pour garantir que le système conserve une qualité d'aléa suffisante pour être utilisé en tant que générateur de clés dans un chiffrement par flot sécurisé.

2.2.1. Analyse de la longueur de cycle

La longueur de cycle est un indicateur essentiel pour évaluer la qualité pseudo-aléatoire d'un système chaotique lorsqu'il est numérisé. Dans un contexte de précision finie, les trajectoires chaotiques peuvent se refermer prématurément sur des cycles périodiques, compromettant ainsi l'imprévisibilité requise pour des applications cryptographiques. Cette sous-section se propose d'analyser l'évolution des longueurs de cycle du système de Hénon en fonction de différentes tailles de mots en virgule fixe, afin de mettre en évidence les effets de la quantification sur sa dynamique. Les résultats obtenus sont présentés sur le tableau suivant :

Precision (bits)	**Longueur de cycle**
16	70
20	**76**
24	**11209**
28	**15878**
32	164702
36	1307550
40	**5748668**

Tableau 1. Influence de la précision en virgule fixe sur la longueur de cycle du système de Hénon

D'après le tableau ci-dessus, l'analyse des longueurs de cycle obtenues pour le système de Hénon montre une forte dépendance à la précision numérique. Pour des résolutions faibles telles que 16 ou 20 bits, les cycles sont extrêmement courts (70 à 76 itérations), indiquant une dynamique fortement dégradée et très éloignée du comportement chaotique attendu.

À partir de 24 bits, une amélioration significative est observée, avec des cycles de plus de 11 000 itérations, qui s'allongent progressivement jusqu'à dépasser 5 millions à 40 bits. Cette croissance exponentielle des longueurs de cycle avec la précision reflète le fait que l'espace d'état devient suffisamment vaste pour retarder l'apparition de cycles périodiques, redonnant au

système un caractère pseudo-aléatoire plus exploitable. Ces résultats confirment que la quantification numérique altère sérieusement la nature chaotique du système à basse précision, et qu'une précision minimale (au moins 32 à 36 bits) est requise pour garantir une diversité suffisante des trajectoires.

Dans une optique cryptographique, cela justifie la nécessité soit d'utiliser une haute résolution mais Il convient de souligner que l'adoption d'une haute précision numérique, bien qu'efficace pour restaurer le comportement chaotique du système de Hénon, n'est pas sans inconvénients. En effet, l'augmentation du nombre de bits entraîne une complexité matérielle plus importante, une consommation de ressources accrue (en termes de mémoire, de logique et de bande passante), ainsi qu'un ralentissement potentiel du traitement, notamment dans les environnements embarqués et les implémentations sur FPGA. Ces contraintes peuvent limiter l'applicabilité pratique du système dans des contextes où la vitesse et l'optimisation matérielle sont critiques. Par conséquent, il est souvent préférable d'explorer des solutions alternatives, comme l'intégration de mécanismes de perturbation, afin de préserver la qualité chaotique tout en maintenant un compromis acceptable entre performance et sécurité.

2.2.2. Analyse par le diagramme de bifurcation

Le diagramme de bifurcation est un outil fondamental en analyse des systèmes dynamiques, car il permet de visualiser l'évolution qualitative de l'orbite d'un système en fonction de variations d'un paramètre de contrôle. En représentant les valeurs asymptotiques d'une variable du système en fonction d'un paramètre, il met en évidence les transitions entre différents régimes dynamiques : stabilité, périodicité, bifurcations successives, et chaos [34].

Dans le contexte de la cryptographie chaotique, cette analyse est cruciale pour identifier les plages de paramètres générant une dynamique suffisamment complexe et imprévisible. Ces plages servent ensuite d'espace de définition pour les clés cryptographiques, assurant ainsi que les séquences générées possèdent les propriétés souhaitées : sensibilité aux conditions initiales, imprédictibilité, et absence de structures périodiques exploitables [35].

Dans cette sous-section, nous procédons à l'analyse du diagramme de bifurcation du système de Hénon, simulé en arithmétique fixe sur 32 bits. L'objectif est d'identifier les zones de l'espace des paramètres de contrôle (α, a, b) dans lesquelles le système conserve un comportement chaotique robuste, malgré les effets de la quantification. Ce repérage permet de restreindre l'espace des clés possibles à des régions dynamiquement sûres, garantissant la

sécurité et la performance du chiffrement par flot implémenté sur cette base [36].

Afin d'évaluer les plages de contrôle dans lesquelles le système de Hénon présente un comportement véritablement chaotique, nous avons procédé à la simulation des diagrammes de bifurcation pour ses différents paramètres. Les résultats obtenus sont illustrés dans la **Figure 1**, où chaque sous-figure présente l'évolution asymptotique de la variable xkx_kxk en fonction d'un paramètre de contrôle donné : a, b, et α. Cette analyse vise à identifier les intervalles dans lesquels le système manifeste une dynamique instable, complexe et sensible aux conditions initiales — autant de caractéristiques essentielles pour une utilisation sécurisée en cryptographie chaotique. Les zones périodiques ou stationnaires, en revanche, doivent être évitées lors de la définition des clés. Les observations issues de ces diagrammes guideront le choix des plages valides pour les paramètres dans le générateur de clés pseudo-aléatoires.

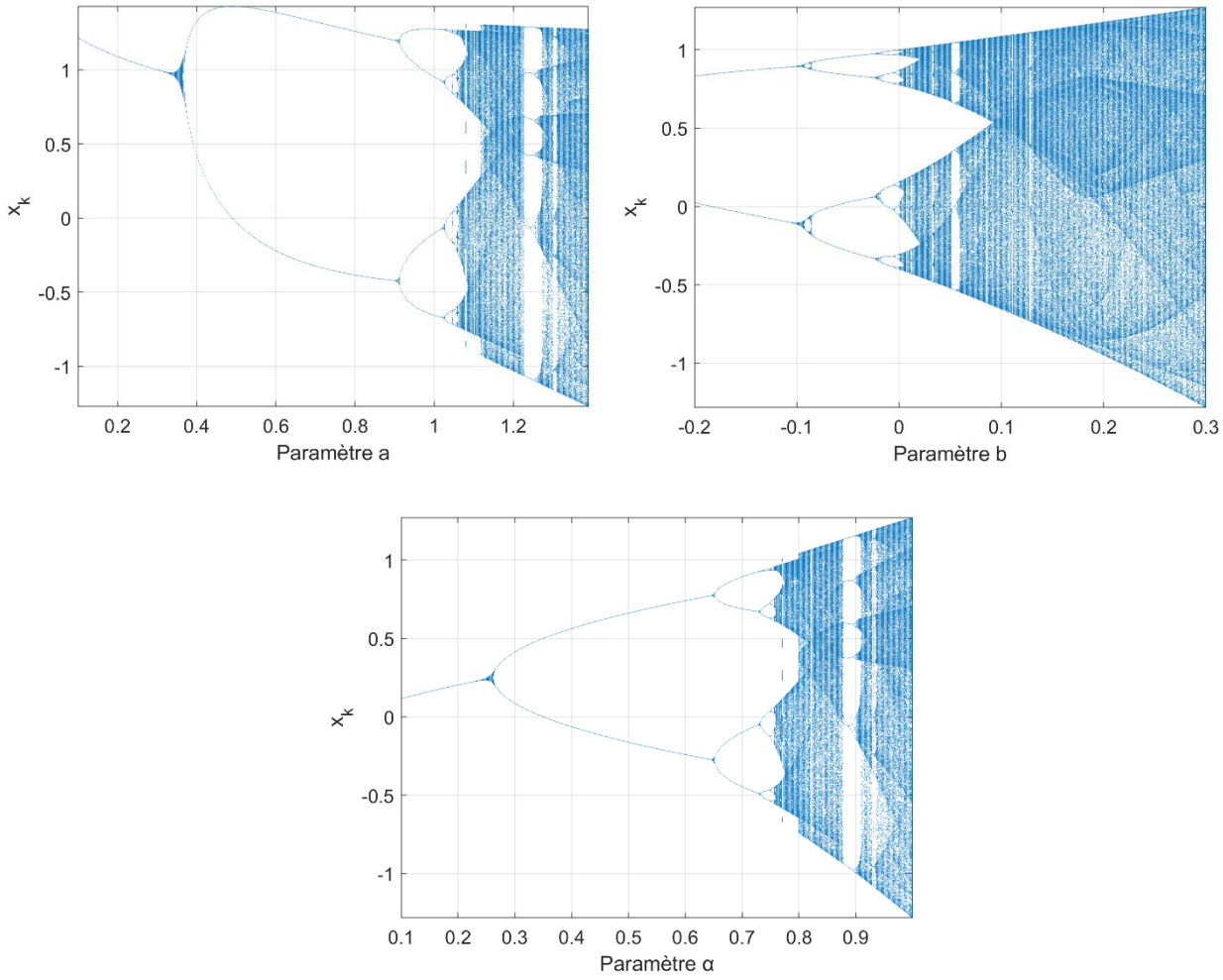

Figure.3.2 : Diagrammes de bifurcation du système chaotique de Hénon.

D'après la figure ci-dessus, le premier diagramme illustre l'évolution asymptotique de la variable x_k en fonction du paramètre de contrôle a, dans l'intervalle [0.2,1.3]. On y observe une dynamique typique de bifurcation, marquée par une transition progressive entre un régime stable (point fixe) pour les faibles valeurs de a, et un régime chaotique à partir d'environ $a = 0.9$. La région $a \in [1.06,1.25]$ montre un comportement chaotique dense, caractérisé par une forte sensibilité aux conditions initiales et une grande richesse dynamique. Cependant, certaines zones intermédiaires révèlent l'apparition de fenêtres périodiques, qu'il convient d'exclure lors du choix des clés afin d'éviter toute prévisibilité dans le chiffrement.

Le second diagramme présente l'effet du paramètre b, exploré ici dans l'intervalle $[-0.2,0.3]$. Les résultats indiquent que les comportements périodiques dominent pour $b < 0$, tandis que le chaos devient bien plus manifeste dès que $b > 0$, notamment à partir de $b \approx 0.15$. Ces résultats suggèrent que les plages de valeurs positives de b sont plus favorables à une utilisation cryptographique, car elles induisent une complexité accrue dans les trajectoires du système. En revanche, les faibles valeurs négatives engendrent des cycles limités ou des régimes quasi-stationnaires peu utiles pour la génération de séquences pseudo-aléatoires.

Enfin, le troisième diagramme illustre l'impact du paramètre α, potentiellement introduit dans un cadre de cascade ou de pondération du système Hénon. Dans l'intervalle $\alpha \in [0.1,1]$, la transition vers le chaos est clairement identifiable à partir de $\alpha \approx 0.6$. Cette section du diagramme révèle une bifurcation rapide vers des régimes hautement chaotiques, propices à la sécurisation d'un chiffrement par flot. L'intérêt d'un tel paramètre réside dans sa capacité à ajuster finement le comportement global du système chaotique et à diversifier les clés produites tout en renforçant leur imprévisibilité.

2.2.3. Analyse statistique

Dans le cadre de l'évaluation de la qualité aléatoire des séquences générées par un système chaotique, l'application de tests statistiques rigoureux est essentielle. La suite de tests NIST SP800-22, développée par le *National Institute of Standards and Technology*, constitue une référence internationale pour analyser le caractère pseudo-aléatoire des séquences binaires [37]. Elle regroupe 15 tests distincts visant à détecter d'éventuelles régularités ou structures dans une suite : fréquence des bits, corrélations, motifs répétitifs, compressibilité, etc.

Ces tests permettent de déterminer si une séquence peut être considérée comme suffisamment aléatoire pour un usage cryptographique. Chaque test repose sur une hypothèse

nulle d'aléa, et une séquence la réussit si la valeur p du test est supérieure à un **seuil de signification** α, généralement fixé à $\alpha = 0{,}01$ ou plus dans les pratiques courantes [38]. Un bon générateur doit réussir l'ensemble ou la majorité des tests avec une proportion statistiquement acceptable.

Dans cette section, la suite NIST est appliquée à des séquences issues du système chaotique de Hénon, en variant la taille de précision arithmétique (16, 24, 32, 40 bits). L'objectif est d'évaluer l'impact de cette précision, en virgule fixe, sur la qualité aléatoire des séquences, afin de vérifier la fiabilité du système comme générateur de clés pseudo-aléatoires pour un chiffrement par flot.

La suite de tests NIST SP 800-22 est appliquée à la sortie binaire du système chaotique de Hénon, générée pour différentes tailles de précision fixe (16, 24, 32 et 40 bits). Les résultats obtenus sont présentés dans le Tableau.2, mettant en évidence l'impact direct de la quantification numérique sur la qualité aléatoire des séquences produites.

Test	Precision			
	16	**24**	32	**40**
Frequency	Failed	Failed	Failed	Failed
Block Freq (m = 128)	Failed	Failed	Failed	Failed
Cumulative-Forward	Failed	Failed	Failed	Failed
Cumulative -Reverse	Failed	Failed	Failed	Failed
Runs	Failed	Failed	Failed	Failed
Long Runs of Ones	Failed	Failed	Failed	Failed
Rank	Failed	Failed	Failed	**Passed**
Spectral DFT	Failed	Failed	**Passed**	**Passed**
Non-Overlapping Template (m = 9)	Failed	Failed	**Passed**	**Passed**
Overlapping Template (m = 9)	Failed	Failed	Failed	Failed
Universal	Failed	Failed	Failed	Failed
Approximate Entropy (m = 10)	Failed	Failed	Failed	Failed
Random Excursion (x = +1)	Failed	Failed	Failed	Failed
Random Excursion Var (x = -1)	Failed	Failed	Failed	Failed
Linear Comp (M = 500)	Failed	Failed	**Passed**	Failed
Serial (m = 16, $\boldsymbol{\nabla\Psi_m^2}$)	Failed	Failed	**Passed**	**Passed**
	0 %	**0 %**	**25 %**	**25 %**

Tableau.2 : Résultats des tests NIST SP 800-22 appliqués aux sorties binaires du système chaotique de Hénon pour différentes précisions numériques.

Les résultats du Tableau 2 illustrent clairement l'influence de la précision arithmétique sur la qualité aléatoire des séquences binaires générées par le système chaotique de Hénon. L'application de la suite NIST SP 800-22 à ces séquences permet de juger de leur aptitude à servir de base pour un générateur pseudo-aléatoire fiable en cryptographie.

Pour les précisions de 16 et 24 bits, aucun test n'a été validé. Cette absence totale de conformité indique que les séquences générées présentent une forte régularité et un comportement prédictible, en grande partie à cause des erreurs de quantification engendrées par la faible résolution. La dynamique chaotique du système est alors fortement altérée, ce qui empêche l'émergence d'un comportement aléatoire exploitable pour des applications sécurisées.

Une nette amélioration est constatée lorsque la précision passe à 32 bits. Un quart des tests sont alors validés, ce qui montre une meilleure dispersion statistique des bits générés. Cela suggère que le système commence à retrouver une partie de sa complexité dynamique, bien que certaines régularités persistent. Cette précision marque un seuil à partir duquel la quantification n'écrase plus totalement le comportement chaotique du système.

À 40 bits, les résultats sont équivalents à ceux obtenus à 32 bits. Aucune amélioration supplémentaire n'est observée, ce qui indique que l'augmentation de la précision n'apporte plus de bénéfice significatif. Le comportement chaotique semble donc limité par la structure même du système, indépendamment de la finesse de la représentation arithmétique.

Ces observations montrent que la précision numérique a un impact direct sur la capacité du système de Hénon à générer des séquences aléatoires de qualité. Les faibles précisions produisent des séquences déterministes et donc inexploitables pour la cryptographie, tandis qu'une précision intermédiaire permet d'atteindre un niveau minimal de qualité aléatoire. Néanmoins, cette amélioration reste insuffisante, et des techniques complémentaires seraient nécessaires pour atteindre un niveau de sécurité acceptable.

3. Le Mécanisme Proposé

Le mécanisme proposé dans cette section vise à surmonter les limitations dynamiques observées lors de la numérisation du système de Hénon. En effet, l'implémentation numérique à précision finie entraîne souvent des comportements non désirés, tels que la réduction de la longueur des cycles, la perte de chaos ou encore l'émergence de régimes périodiques. Pour remédier à ces problèmes, nous proposons de cascader deux instances distinctes du système de Hénon, chacune configurée avec un ensemble différent de paramètres de contrôle. Cette

approche permet d'augmenter la complexité globale du système. En complément, des blocs de post-traitement non linéaires sont intégrés afin d'améliorer les propriétés statistiques et aléatoires des séquences générées, contribuant ainsi à restaurer un comportement chaotique plus riche, plus imprévisible et mieux adapté aux exigences du chiffrement par flot sécurisé.

Le schéma du mécanisme proposé est présenté à la Figure.3.3. Celui-ci est constitué de deux systèmes chaotiques de Hénon, configurés avec des paramètres de contrôle différent.

Le mécanisme proposé repose sur une interconnexion bidirectionnelle entre deux systèmes chaotiques de Hénon :

Le premier système : $$\begin{cases} x_{k+1} = \alpha_1 + y_k - a_1 x_k^2 \\ g \\ y_{k+1} = b_1 \hat{x}_k \end{cases} \quad (2)$$

Le deuxième système : $$\begin{cases} \hat{x}_{k+1} = \alpha_2 + \hat{y}_k - a_2 x_k \hat{x}_k \\ g \\ \hat{y}_{k+1} = b_2 \hat{x}_k \end{cases} \quad (3)$$

Contrairement à une simple cascade unidirectionnelle, ici chaque système influence l'autre, ce qui augmente davantage la complexité du comportement dynamique global.

- Premier système : génère x_{k+1} à partir de ses propres variables, mais met à jour y_{k+1} en fonction de la sortie du second système $\hat{x}_k$.
- Deuxième système : met à jour $\hat{x}_{k+1}$ en utilisant à la fois sa propre variable $\hat{x}_k$ et la variable x_k du premier système (croisement direct), puis génère $\hat{y}_{k+1}$.

Afin de garantir un comportement chaotique robuste pour une large plage de valeurs, les paramètres utilisés dans les deux systèmes de Hénon sont dérivés à partir de nouveaux paramètres de contrôle indépendants $\alpha, a, b, \beta, c, et\ d$, selon les relations suivantes :

- Pour le premier système : $\alpha_1 = \alpha + 0.5,\ a_1 = a + 0.9,\ b_1 = b + 0.9$.
- Pour le deuxième système : $\alpha_2 = \beta + 0.8,\ a_2 = c + 0.9,\ b_2 = d + 0.9$.

Les constantes additives (0.5, 0.8, etc.) ont été choisies de manière arbitraire mais stratégique dans le but d'éloigner les paramètres de contrôle des valeurs trop proches de zéro, lesquelles sont connues pour favoriser des comportements non chaotiques.

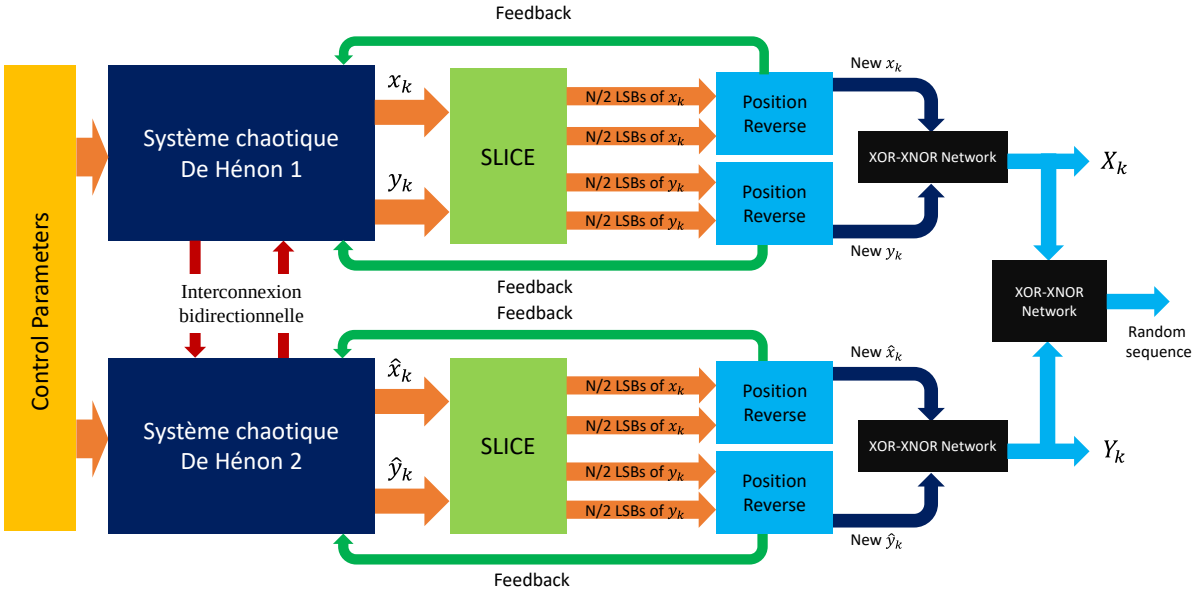

Figure.3.3 : Architecture fonctionnelle de mécanisme proposé.

Grâce à cette transformation, toute valeur des paramètres de contrôle de base dans l'intervalle [0, 1] est projetée dans une zone du plan paramétrique qui induit un comportement chaotique soutenu. Ce choix renforce ainsi la fiabilité du mécanisme pour une utilisation cryptographique, notamment en assurant une richesse dynamique même sous quantification numérique.

L'étape suivante sert à améliorer le comportement aléatoire de système. Les vecteurs d'état binaires, x_k, y_k, $\hat{x}_k$, et $\hat{y}_k$ chacun de longueur N bits sont subits à des changements :

- **Un bloc tranchage (Slice)** : Chaque vecteur x_k, y_k, $\hat{x}_k$, et $\hat{y}_k$ est découpé en quatre segments de taille égale, soit $\frac{N}{4}$ bits chacun. Ce découpage est effectué des bits de poids faible (LSB) vers les bits de poids fort (MSB), ce qui permet une segmentation fine de l'information binaire. Ainsi, le premier segment contient les $\frac{N}{4}$ bits LSB, et le quatrième segment contient les $\frac{N}{4}$ bits MSB. Cette étape prépare les données pour une réorganisation structurelle lors de l'inversion de position, renforçant la complexité binaire avant l'opération logique finale.
- **Un bloc pur l'inversion de position des segments** : Les quatre segments de chaque vecteur sont ensuite réassemblés dans l'ordre suivant (par exemple : 1 → 3 → 2 → 4). Cela crée un vecteur binaire réordonné avec une structure interne remaniée.

- **Réseau XOR–XNOR**: Les quatre nouveaux vecteurs — issus de chaque inversion — sont injectés dans un réseau logique : Les bits en position impaire sont combinés entre eux via des opérations XOR. Les bits en position paire sont combinés via des opérations XNOR. Cette étape génère une séquence binaire pseudo-aléatoire avec une bonne distribution en sortie du réseau.
- **Boucle de rétroaction (Feedback) :** Les vecteurs transformés sont renvoyés au départ du système chaotique, bouclant ainsi le processus d'itération et assurant un remaniement continu de l'état.

Les deux réseaux XOR-XNOR génèrent ainsi deux nouvelles séquences X_k et Y_k, qui représentent les deux sorties principales du système global. L'ensemble de ce mécanisme peut alors être interprété comme un nouveau système chaotique bidimensionnel, dont le comportement hérite de la richesse dynamique des deux systèmes de Hénon originaux, tout en intégrant une couche supplémentaire de non-linéarité et de désordre par le traitement binaire.

La dernière étape, représentée dans la Figure.3.3, consiste à injecter les deux vecteurs binaires issus des réseaux XOR-XNOR (correspondant aux nouvelles sorties X_k et Y_k dans un dernier réseau XOR-XNOR. Ce réseau combine les deux flux pour générer une séquence binaire pseudo-aléatoire de N bits, présentant une entropie élevée et une excellente dispersion. Grâce à cette structure, la séquence obtenue hérite de la complexité dynamique du système global, assurant des propriétés statistiques robustes pour des usages cryptographiques.

4. Evaluation de Mécanisme proposé

Afin de valider l'efficacité du mécanisme proposé, une évaluation approfondie est menée pour comparer les performances dynamiques et statistiques du système chaotique amélioré par rapport au système original.

4.1. Analyse de l'espace de phase

L'analyse du portrait de phase permet de visualiser les trajectoires et d'identifier la densité, la couverture et la structure de l'attracteur chaotique. Un attracteur bien rempli, sans zones creuses ni trajectoires périodiques visibles, indique une dynamique riche et idéale pour le chiffrement chaotique, assurant une forte diffusion et complexité du flux de clés.

Après l'insertion du mécanisme proposé (MP), le système chaotique quadratique gagne en complexité structurale. Le nouvel espace de phase, représenté sur la Figure.3.4.

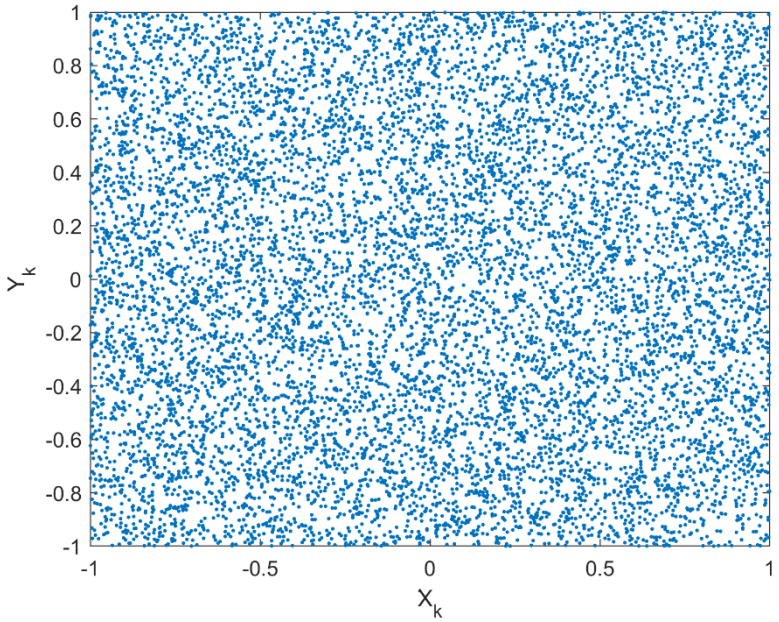

Figure.3.4: L'espace de phase du système de Hénon modifié.

La figure.3.4 montre l'espace de phase X_k et Y_k du système de Hénon modifié. On observe une dispersion uniforme et dense des points, sans structure apparente, ce qui témoigne d'un comportement hautement chaotique. Cette absence de motifs réguliers reflète une complexité accrue du système et une bonne couverture de l'espace d'état. Ces propriétés confirment l'efficacité du mécanisme proposé dans l'amélioration des dynamiques du système original, notamment en vue d'applications en cryptographie.

4.2. La longueur de cycle

Cette sous-section est consacrée à l'analyse du comportement des longueurs de cycle du système chaotique après l'application du mécanisme proposé (MP). Partant des limitations identifiées précédemment pour la carte de Hénon originale en arithmétique à précision finie, l'objectif ici est de vérifier si le MP permet effectivement d'allonger les cycles et de rompre les périodicités courtes. Pour assurer la cohérence de l'évaluation, la même méthode basée sur l'autocorrélation est utilisée. Le tableau suivant résume les résultats obtenus pour différentes tailles de précision arithmétique :

Précision (bits)	Longueur de cycle
16	308052
20	Ne pas détecté
24	Ne pas détecté
32	Ne pas détecté

Tableau 3 : Longueur de cycle obtenue en fonction de la taille de la précision.

Les résultats présentés dans le Tableau 3 témoignent d'une amélioration notable des propriétés dynamiques du système de Hénon suite à l'application du mécanisme proposé. En effet, pour une précision de 16 bits, un cycle a été détecté avec une longueur de 308052 itérations. Bien que cette valeur soit relativement élevée, elle indique que le système demeure sujet à une certaine forme de périodicité lorsque la précision numérique est faible.

Cependant, à partir de 20 bits de précision, aucun cycle n'a pu être détecté durant l'expérimentation. Cette absence de détection suggère que le système devient plus résistant au phénomène de cycles courts, caractéristique des artefacts numériques induits par la quantification. Ainsi, le mécanisme proposé semble jouer un rôle crucial dans la préservation du caractère pseudo-aléatoire du système sur des plages temporelles étendues.

Cette stabilité accrue du comportement chaotique, observée notamment pour les précisions de 20, 24 et 32 bits, confirme l'efficacité du mécanisme introduit pour atténuer les effets du repliement numérique et renforcer la robustesse du générateur face à l'effondrement de la dynamique chaotique. Ces résultats sont particulièrement encourageants pour une utilisation sécurisée du système dans des applications de génération de clés pseudo-aléatoires.

4.3. Analyse des diagrammes de bifurcation

Cette sous-section est consacrée à l'analyse du comportement bifurcationnel du système de Hénon modifié intégrant le mécanisme proposé. L'étude est réalisée sous une précision arithmétique de 32 bits, afin d'observer l'évolution des trajectoires à long terme en fonction de la variation d'un paramètre de contrôle. Le diagramme de bifurcation permet ici d'évaluer dans quelle mesure le MP améliore la dynamique du système, notamment en maintenant un comportement chaotique stable sur une plage plus large de valeurs paramétriques. La comparaison avec le système original met en évidence l'impact du mécanisme sur la complexité globale du système et la richesse de ses régimes dynamiques. Les diagrammes obtenus sont présentés sur la Figure.3.5.

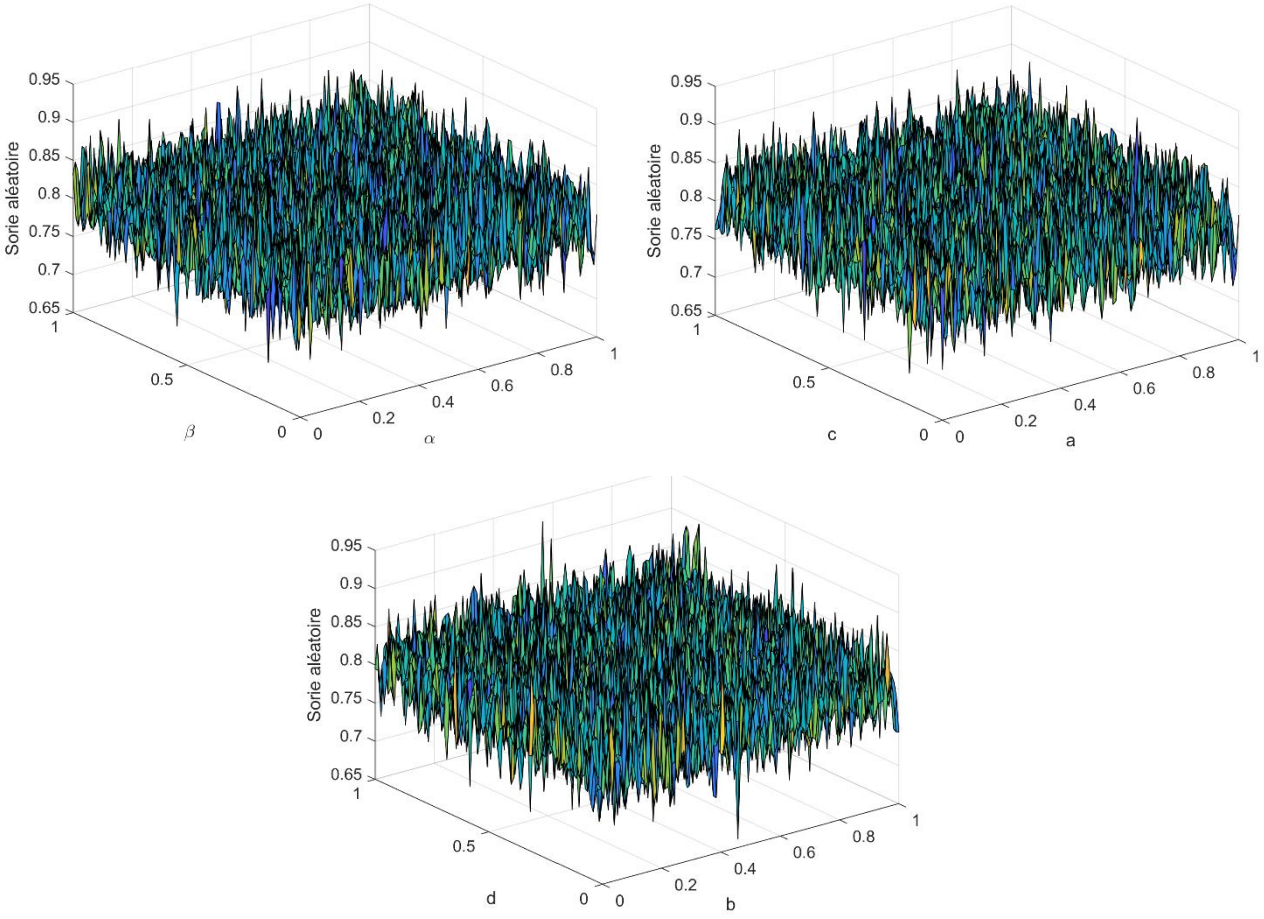

Figure.3.5 : Diagrammes de bifurcation du système chaotique de Hénon modifié.

Les diagrammes de bifurcation du système modifié illustrés ci-dessus révèlent une dynamique globalement dense et complexe pour l'ensemble des plages de variation des paramètres. L'irrégularité et la dispersion des valeurs de sortie aléatoire en fonction des différents couples de paramètres $(\alpha, \beta, a, b, c, d)$ traduisent un comportement fortement non linéaire et sensible aux conditions initiales — caractéristiques fondamentales d'un système chaotique robuste.

On remarque l'absence de régularité évidente ou de structures périodiques dominantes, ce qui confirme que le système modifié conserve une nature chaotique sur une large gamme de paramètres. Cette propriété est essentielle pour un générateur pseudo-aléatoire, car elle garantit une imprévisibilité élevée et une bonne entropie des séquences générées.

Les diagrammes de bifurcation montrent aussi que le système modifié génère un comportement chaotique dense et régulier sur de larges plages de paramètres. Cela supprime les combinaisons faibles du système original, où certains paramètres produisaient des sorties

périodiques. Le générateur offre désormais une qualité aléatoire constante, indépendamment des clés choisies. Cette uniformité renforce considérablement la sécurité : l'espace des clés s'élargit, rendant les attaques par force brute plus complexes, tout en assurant une robustesse même en cas de divulgation partielle de la clé. Le système devient ainsi plus fiable pour des applications cryptographiques exigeantes.

4.4. Analyse statistique

La suite de tests NIST SP 800-22 est appliquée à la sortie binaire générée du système chaotique de Hénon modifé par le MP pour différentes tailles de précision fixe (16, 24, et 32 bits). Les résultats obtenus sont présentés dans le Tableau.4.

Test	Precision		
	16	**24**	32
Frequency	0.57957	0.01486	0.35861
Block Freq (m = 128)	0.77676	0.18443	0.99122
Cumulative-Forward	**Fialed**	**Fialed**	0.50978
Cumulative -Reverse	**Fialed**	**Fialed**	0.39250
Runs	**Fialed**	**Fialed**	0.27755
Long Runs of Ones	0.41607	0.29945	0.60352
Rank	0.46639	0.43998	0.30150
Spectral DFT	0.94147	0.13470	0.55099
Non-Overlapping Template (m = 9)	0.95384	0.64027	0.56852
Overlapping Template (m = 9)	0.01846	0.52897	0.20453
Universal	0.16731	0.42248	0.63127
Approximate Entropy (m = 10)	**Fialed**	0.44897	0 85543
Random Excursion (x = +1)	**Fialed**	**Fialed**	0.36298
Random Excursion Var (x = -1)	**Fialed**	**Fialed**	0.43179
Linear Comp (M = 500)	0.76764	0.23018	0.42902
Serial (m = 16, $\nabla\Psi_m^2$)	0.34202	0.68631	0.85254
	62.5 %	**68.75 %**	**100** %

Tableau.4 : Résultats des tests NIST SP 800-22 appliqués aux sorties binaires du système chaotique de Hénon modifié pour différentes précisions numériques.

Les résultats du tableau ci-dessus mettent en évidence la remarquable efficacité du mécanisme proposé appliqué au système de Hénon :

À 16 bits, les valeurs de p obtenues pour plusieurs tests dépassent le seuil $\alpha = 0{,}01$ fixé par le NIST. Cela représente un progrès considérable par rapport au système original, qui échouait systématiquement dans tous les tests. À 24 bits, près de 69 % des tests sont réussis, un niveau qui s'approche des recommandations NIST (≈95 % de réussite sur 100 séquences) . Enfin, à 32 bits, 100 % des tests sont validés, un résultat exceptionnel pour tout PRNG, qu'il soit chaotique ou standard.

Ce mécanisme transforme un système initialement incapable de générer des séquences acceptables (0 %) en un générateur fiable dès la précision moyenne (24 bits), culminant à une conformité totale à 32 bits. Ces performances confirment que notre approche fournit une base solide pour un générateur de clés pseudo-aléatoires apte pour des applications cryptographiques exigeantes.

5. Le crypto-système proposé pour le chiffrement d'audio

Dans cette section, nous exploitons le système chaotique modifié de Hénon comme cœur d'un crypto-système de chiffrement par flot dédié aux signaux audio. Pour être sécurisée, une telle solution doit assurer deux propriétés fondamentales, définies par Claude Shannon : la confusion et la diffusion.

- **Confusion** : cela consiste à rendre la relation entre la clé (ici les paramètres du système chaotique) et le texte chiffré aussi complexe que possible. Chaque bit de sortie doit dépendre de manière non triviale de plusieurs paramètres, empêchant toute déduction directe de la clé à partir du texte chiffré.
- **Diffusion** : cette propriété vise à étaler l'information du signal clair sur une large portion du texte chiffré. Ainsi, une modification infime (un bit) dans l'entrée doit se répercuter sur environ la moitié des bits du message chiffré, conformément au principe dit de l'effet d'avalanche.

La Figure.3.6 présente le schéma de base du crypto-système proposé pour le chiffrement de signaux audio, dans lequel les propriétés fondamentales de *confusion* et de *diffusion* sont rigoureusement assurées. Ces deux propriétés essentielles en cryptographie, introduites par Claude Shannon, visent respectivement à masquer les relations entre la clé et le message chiffré (*confusion*) et à répartir uniformément l'influence de chaque bit du message clair sur le message chiffré (*diffusion*), ce qui renforce la robustesse contre les attaques statistiques.

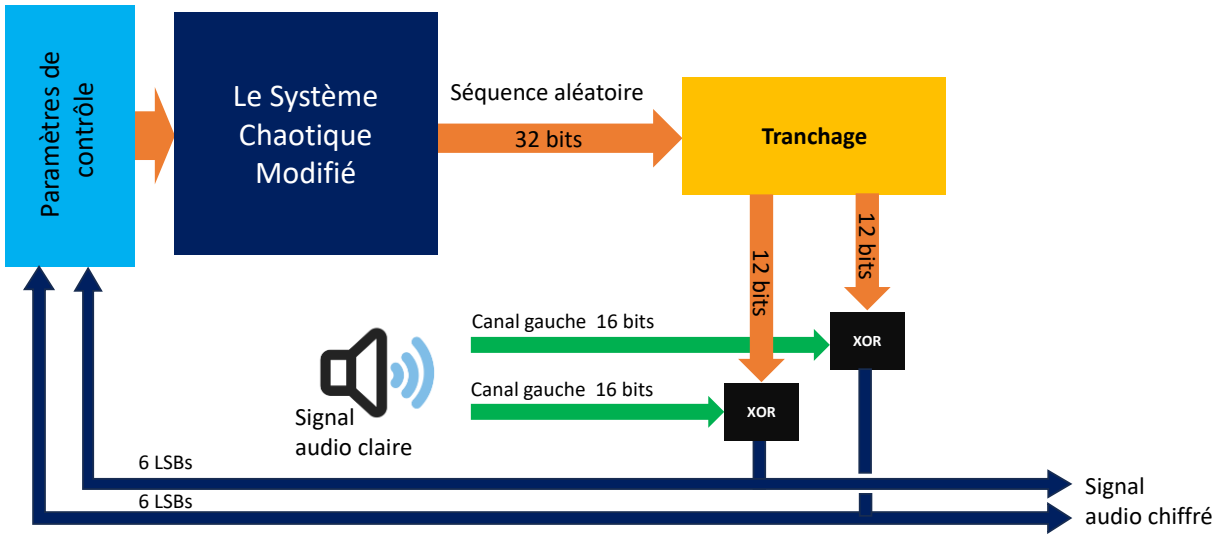

Figure.3.6 : Le schéma de crypto-système proposé pour le chiffrement d'audio.

Dans ce schéma, les paramètres de contrôle alimentent un système chaotique modifié, générant une séquence aléatoire de 32 bits. Cette séquence, dotée de hautes propriétés d'entropie grâce au caractère imprévisible du système chaotique, est ensuite découpée (ou *tranchée*) en segments de 12 bits. Chaque segment de 12 bits est combiné via une opération XOR avec un canal du signal audio clair (canaux gauche et droit de 16 bits chacun),

La figure ci-dessus illustre le schéma fondamental du crypto-système proposé pour le chiffrement de signaux audio, dans lequel les deux propriétés cryptographiques majeures — confusion et diffusion — sont rigoureusement assurées. La propriété de confusion est garantie par la sensibilité extrême du système chaotique modifié à ses paramètres de contrôle : une légère variation dans ces derniers provoque un changement radical dans la séquence générée, rendant le lien entre la clé et le message chiffré imprévisible. Quant à la diffusion, elle est assurée par un mécanisme adaptatif intégré au schéma : les 6 bits de poids faible (LSBs) de chaque canal audio clair (soit 12 bits au total) sont extraits puis segmentés en six paires de 2 bits. Chacune de ces paires est ensuite combinée avec les 2 bits de poids faible de chacun des paramètres de contrôle du système chaotique. Cette rétroaction dynamique implique que la moindre modification dans le signal audio clair — même au niveau d'un seul bit — impacte directement les paramètres de contrôle et, par conséquent, le comportement du système chaotique. Ce processus amplifie considérablement l'effet de diffusion, en rendant le système hautement sensible aux variations du message en clair, et donc plus résistant aux attaques par analyse différentielle.

6. Evaluation de crypto-système proposé

Afin de valider l'efficacité et la robustesse crypto-système proposé pour le chiffrement d'audio, une série d'analyses est menée sur les images chiffrées. Cette évaluation repose sur plusieurs critères fondamentaux qui visent à tester la sécurité, la sensibilité et le comportement statistique du schéma proposé. Les analyses incluent :

- L'analyse de la clé, englobant la taille de l'espace de clé et la sensibilité aux légers changements de cette dernière, ce qui permet d'évaluer la propriété de confusion.
- L'évaluation de la propriété de diffusion, qui examine dans quelle mesure une modification minime de l'image claire (par exemple, un seul échantillon) influence le signal audio chiffrée dans son ensemble.

Ces tests visent à démontrer que le système proposé offre un niveau de sécurité élevé, adapté aux exigences de la cryptographie dessignaux audio numériques.

6.1. Analyse de clé

La sécurité d'un algorithme de chiffrement dépend en grande partie de la solidité de sa clé de chiffrement. Deux éléments déterminants permettent d'en juger : d'une part, la longueur de la clé, qui influe directement sur la difficulté d'une attaque par force brute ; d'autre part, la sensibilité du système aux variations infimes de cette clé. Un bon système doit réagir de manière drastiquement différente à des clés presque identiques, ce qui témoigne d'un haut niveau de confusion — une propriété essentielle pour empêcher toute relation détectable entre la clé utilisée et les données chiffrées. Cette section se concentre sur l'analyse de ces deux critères afin de démontrer la capacité du schéma proposé à résister aux attaques cryptanalytiques classiques et à assurer un chiffrement fiable.

6.1.1. Taille de la clé

L'analyse des diagrammes de bifurcation (Figure.3.5) du système chaotique modifié par le mécanisme proposé (MP) a mis en évidence une dynamique chaotique stable sur toute l'étendue de l'intervalle [0, 1] pour chacun des paramètres de contrôle. Cette extension significative du domaine chaotique rend possible l'exploitation complète de ces plages dans la génération des clés, augmentant ainsi considérablement l'espace clé théorique. Dans cette configuration, chaque paramètre est codé en virgule fixe sur 32 bits, et le système repose sur 6 paramètres indépendants,

ce qui donne lieu à une clé de taille initiale de 192 bits (6 × 32). Un tel espace clé reste extrêmement vaste. En cryptographie symétrique, la robustesse face aux attaques par force brute est directement liée à la taille de la clé, car le nombre de combinaisons possibles croît de manière exponentielle avec le nombre de bits (soit 2^{192} possibilités ici). À titre de comparaison, une clé de 128 bits ou plus est déjà considérée comme sécurisée pour la plupart des applications actuelles pour le chiffrement à flot [3-03]. Le système proposé dépasse donc largement ces seuils, offrant une résistance accrue aux attaques futures et une marge de sécurité confortable.

Le schéma ci-dessous illustre le processus d'initialisation des paramètres de contrôle d'un système chaotique modifié à partir de la clé principale, en plusieurs étapes structurées :

Figure.3.7 : Le schéma de processus de génération de paramètres de contrôle à partir de la clé globale de système.

Détail du processus de génération des paramètres :

- **Clé globale en format hexadécimal** : La clé initiale, saisie sous forme hexadécimale (base 16), représente une manière compacte et sécurisée de définir les valeurs d'entrée du système chaotique.
- **Extraction de 6 constantes en base 10** : Cette clé est segmentée en 6 portions égales, chacune étant ensuite traduite en une valeur entière en base décimale. Ces constantes serviront directement à alimenter le système chaotique en tant que paramètres de contrôle.
- **Encodage en format fixe 32Q32** : Les constantes obtenues sont transformées en nombres à virgule fixe, codés sur 32 bits selon le format 32Q32, c'est-à-dire avec 32 bits dédiés à la partie fractionnaire, garantissant une grande précision dans les calculs.

Ce mécanisme de génération permet de tirer pleinement parti de la clé globale, en assurant un large espace de clé et une forte granularité des paramètres. Il contribue ainsi à renforcer considérablement la résistance du système contre les attaques de type force brute, tout en maintenant la compatibilité avec les exigences du chiffrement par flot.

6.1.2. Sensibilité à la clé

La sensibilité à la clé est une caractéristique fondamentale des systèmes de chiffrement fondés sur le chaos, étroitement liée au concept de confusion. Elle suppose qu'un changement infime dans la clé — même d'un seul bit — doit produire un résultat chiffré complètement différent, rendant impossible toute approximation du texte original à partir d'une clé incorrecte, même très proche.

Dans notre cas, cette propriété a été évaluée en modifiant un seul bit au sein des paramètres de contrôle constituant la clé, puis en comparant le message chiffré obtenu à celui généré avec la clé d'origine. Si les deux versions chiffrées présentent une différence marquée malgré une variation minime de la clé, cela démontre la haute sensibilité du système, un critère essentiel pour résister aux attaques différentielles ou par recherche exhaustive.

Pour illustrer ce comportement, la Figure.3.8 présente le chiffrement d'un signal audio avec une clé hexadécimale spécifique. Plusieurs variantes de cette clé ont été testées, chacune différant uniquement par un bit :

Clé 1 : FA1D25A55F656FD63C3AEBD5D4139FA687F27DA0EB9127E2

Clé 2 : FA1D25A55F656FD63C3AEBD5D4139FA687F27DA0EB9127E**1**

Clé 3 : **E**A1D25A55F656FD63C3AEBD5D4139FA687F27DA0EB9127E2

Clé 4 : FA1D25A55F656FD63C**2**AEBD5D4139FA687F27DA0EB9127E2

Clé 5 : FA1D25A55F656FD63C3AEBD5D4139FA68**6**F27DA0EB9127E2

Clé 6 : FA1D25A55F656**E**D63C3AEBD5D4139FA687F27DA0EB9127E2

La clé 1 est utilisé pour chiffrer un signal audio de format *.wav avec une fréquence d'échantillonnage de 44100 Hz (on sélectionne seulement le canal gauche pour avoir un seul signal). Sur la Figure.3.8, on a :

- La séquence 1 est le signal audio original,
- La séquence 2 et le signal audio chiffré,
- La séquence 3 est la différence entre le signal audio original et le signal déchiffré par la clé 2.
- La séquence 4 est la différence entre le signal audio original et le signal déchiffré par la clé 3.
- La séquence 5 est la différence entre le signal audio original et le signal déchiffré par la clé 4.

- La séquence 6 est le résultat de déchiffrement de la séquence 2 par la clé exacte (clé 1).

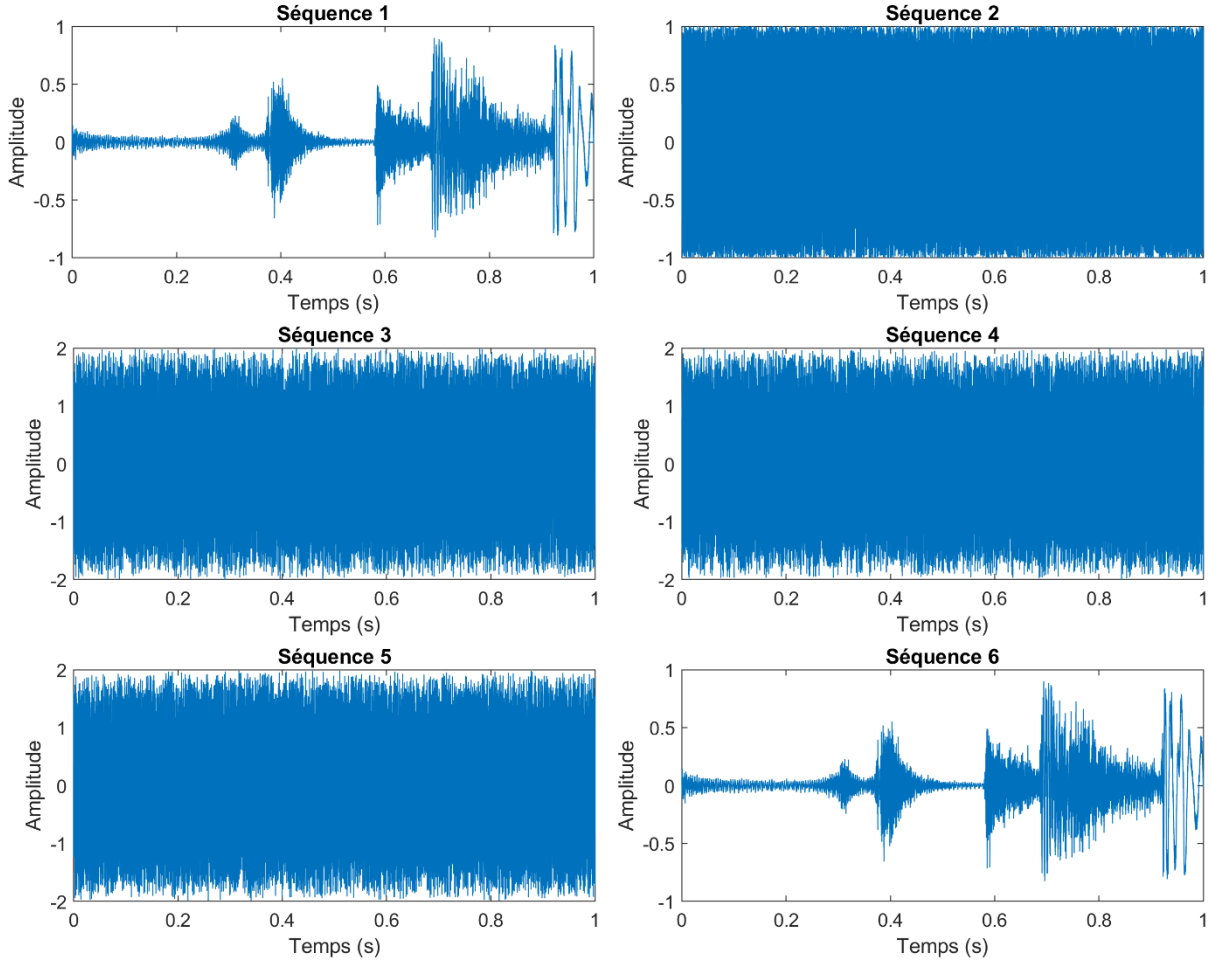

Figure.3.8 : Analyse de la sensibilité à la clé du système de chiffrement audio.

La figure ci-dessus illustre de manière convaincante la robustesse du système de chiffrement face aux variations infimes de la clé. Les différences très marquées entre le signal original et les signaux déchiffrés avec des clés erronées montrent que le système présente une sensibilité extrême à la clé, propriété essentielle des schémas chaotiques. Malgré le changement d'un seul bit, les séquences obtenues sont totalement désordonnées, ce qui empêche toute tentative de reconstitution partielle du signal initial. Par ailleurs, la parfaite superposition entre le signal original et celui déchiffré avec la clé exacte confirme la capacité du système à assurer une réversibilité fiable sans dégradation. Ce comportement valide la qualité cryptographique du système, notamment sa capacité à résister aux attaques par clé presque correcte ou à toute forme d'analyse différentielle.

6.2. Évaluation de la propriété de diffusion

Après avoir défini et souligné l'importance de la propriété de diffusion dans les sections précédentes, nous proposons ici une analyse expérimentale visant à évaluer l'efficacité du crypto-système proposé à propager les modifications d'un signal audio clair dans sa version chiffrée. L'objectif est de mesurer la sensibilité du chiffrement à une perturbation minimale de l'entrée, et de vérifier que cette modification se diffuse à travers l'ensemble du flux chiffré.

Plus précisément, l'expérience consiste à introduire un changement d'un seul bit dans un échantillon audio, puis à comparer le fichier audio chiffré obtenu à celui généré à partir du signal original. Une diffusion efficace se manifeste par un taux élevé de bits modifiés dans la séquence chiffrée, idéalement proche de 50 %. Ce comportement traduit une excellente capacité du système à brouiller l'information et à empêcher toute corrélation exploitable entre l'entrée claire et sa version chiffrée.

Ainsi, cette approche permet de valider la capacité du système à neutraliser les attaques basées sur des modifications ciblées du message clair. Un bon résultat indique que même un changement infime dans le signal d'entrée affecte de manière significative l'ensemble du signal chiffré, renforçant la robustesse du système face aux attaques par analyse différentielle. Le résultat obtenu est présenté sur la Figure.3.9.

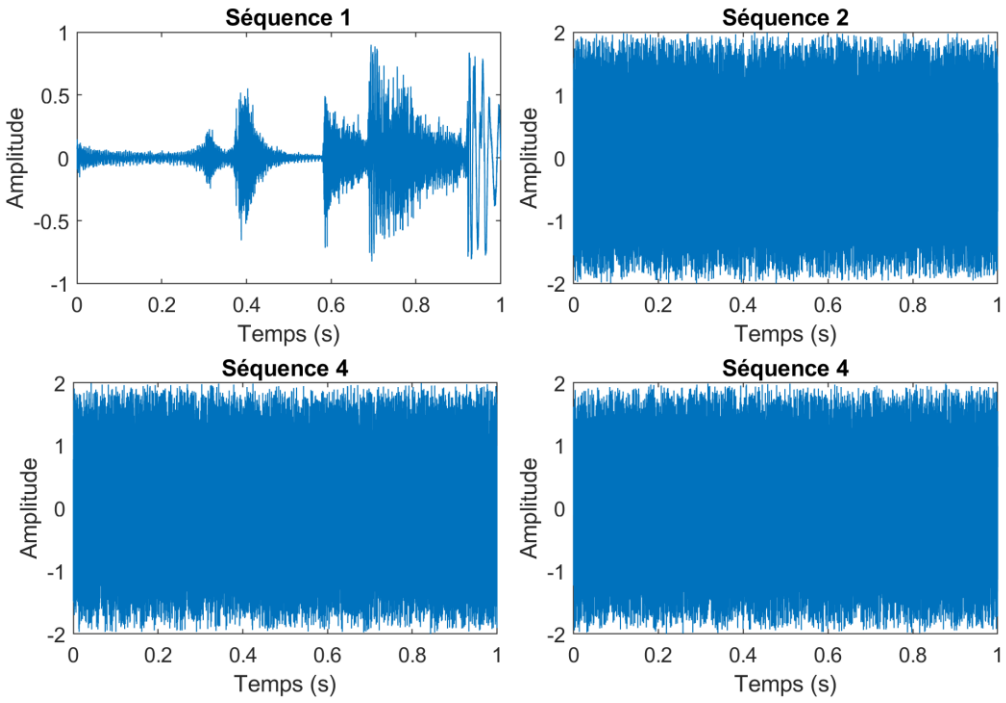

Figure.3.9 : Évaluation de la propriété de diffusion.

Sur la Figure.3.9, la séquence 1 est le signal audio original, la séquence 2 est le signal audio chiffré, la séquence 3 est le signal audio chiffré par un changement d'un seul bit sur le premier échantillon de signal audio original, et la séquence 4 est la différence entre la séquence 2 et 3.

La Figure 9 illustre clairement l'efficacité du mécanisme de chiffrement proposé en termes de propriété de diffusion, un critère fondamental en cryptographie. En modifiant un seul bit du premier échantillon du signal original, on observe que le signal chiffré résultant (séquence 3) diffère de manière significative du signal chiffré initial (séquence 2), ce qui traduit une forte sensibilité au message en clair. De plus, la différence entre les deux signaux chiffrés (séquence 4) présente une apparence totalement bruitée, traduisant une propagation rapide et étendue de l'effet du bit modifié sur l'ensemble du signal. Cela démontre que le mécanisme proposé contribue efficacement à disséminer toute petite variation dans l'entrée à travers toute la séquence chiffrée, assurant ainsi une excellente diffusion et complexification du processus de chiffrement.

7. Conclusion

Ce chapitre a présenté un système innovant de chiffrement audio basé sur une cascade de deux systèmes chaotiques de Hénon, renforcé par un mécanisme améliorant les propriétés aléatoires. Les résultats démontrent une nette amélioration des performances : les cycles deviennent indétectables dès 20 bits de précision, et les tests NIST SP800-22 sont validés à 100 % à 32 bits. Le crypto-système proposé intègre efficacement les propriétés de confusion et de diffusion, garantissant une sensibilité élevée aux clés et une propagation optimale des modifications du signal. Implémenté en virgule fixe sur FPGA, ce système offre une solution robuste et sécurisée pour le chiffrement audio, avec des perspectives prometteuses pour des applications pratiques. Les évaluations statistiques et dynamiques confirment sa fiabilité pour des usages cryptographiques exigeants.

Conclusion générale

Conclusion Générale

Ce mémoire a présenté une étude approfondie sur la conception et la simulation d'un système de chiffrement par flot innovant basé sur une architecture chaotique. Nos travaux se sont articulés autour de trois axes principaux : l'analyse théorique des systèmes chaotiques et leur applicabilité en cryptographie, la conception détaillée d'un générateur pseudo-aléatoire utilisant deux cartes de Hénon couplées, et enfin la validation expérimentale par simulation du système complet.

Les résultats obtenus démontrent que notre approche permet de générer des séquences présentant d'excellentes propriétés cryptographiques. La sensibilité extrême aux conditions initiales, caractéristique fondamentale des systèmes chaotiques, a été préservée et même renforcée par notre mécanisme de post-traitement. Les tests statistiques exhaustifs (NIST SP800-22) confirment la qualité aléatoire des séquences produites, tandis que les analyses de diffusion et de confusion attestent de la robustesse du système face aux attaques cryptanalytiques classiques.

L'application au chiffrement de signaux audio a permis de valider concrètement notre approche. Les simulations montrent une parfaite réversibilité du processus (déchiffrement sans dégradation) et une sensibilité marquée aux paramètres de contrôle, essentielle pour garantir la sécurité. La structure modulaire du système offre par ailleurs une grande flexibilité pour son adaptation à différents contextes d'utilisation.

Perspectives de Recherche

Les performances encourageantes de ce travail ouvrent plusieurs pistes intéressantes pour des développements futurs. Une implémentation sur FPGA constituerait une étape naturelle, permettant d'évaluer les performances réelles du système dans un environnement matériel contraint. Cette implémentation pourrait notamment bénéficier des capacités de traitement parallèle des FPGA pour optimiser les calculs des itérations chaotiques.

Par ailleurs, l'intégration de ce système dans des architectures de communication existantes, avec une attention particulière portée à l'interopérabilité avec les protocoles standards, représenterait une avancée significative vers des applications pratiques. Des études complémentaires pourraient également explorer l'adaptation du système à d'autres types de données que l'audio, comme les flux vidéo ou les données IoT.

En conclusion, cette recherche contribue à démontrer le potentiel des systèmes chaotiques dans le domaine de la cryptographie moderne. Les résultats obtenus, bien que se limitant à une validation par simulation, posent des bases solides pour des développements ultérieurs vers des applications concrètes. La voie ouverte par ces travaux mérite d'être approfondie, notamment pour répondre aux défis croissants de la sécurité informatique dans un monde de plus en plus connecté.

Références

Bibliographie

[1]. Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.

[2]. Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms and Source Code in C. John Wiley & Sons.

[3]. Katz, J., & Lindell, Y. (2020). *Introduction to Modern Cryptography*. CRC Press.

[4]. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. Pearson Education.

[5]. Hodges, A. (1983). Alan Turing: The Enigma. Simon & Schuster.

[6]. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. Pearson Education.

[7]. Menezes, A., van Oorschot, P., & Vanstone, S. (1996). *Handbook of Applied Cryptography*. CRC Press.

[8]. Ferguson, N., Schneier, B., & Kohno, T. (2010). Cryptography Engineering: Design Principles and Practical Applications. Wiley Publishing.

[9]. NIST. (2001). Announcing the Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

[10]. Daemen, J., &Rijmen, V. (2002). The Design of Rijndael: AES - The Advanced Encryption Standard. Springer.

[11]. Kocher, P., Jaffe, J., & Jun, B. (1999). Differential Power Analysis. In Advances in Cryptology — CRYPTO'99, LNCS 1666.

[12]. Chen, L., et al. (2016). Report on Post-Quantum Cryptography. National Institute of Standards and Technology (NIST).

[13]. Paar, C., & Pelzl, J. (2010). *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer.

[14]. Grover, L. (1996). A fast quantum mechanical algorithm for database search. In Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC).

[15]. Ott, E. (2002). *Chaos in Dynamical Systems*. Cambridge University Press.

[16]. Strogatz, S. H. (2015). *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering*. Westview Press.

[17]. Pecora, L. M., & Carroll, T. L. (1990). Synchronization in chaotic systems. *Physical Review Letters*, 64(8), 821–824.

[18]. Sprott, J. C. (2003). *Chaos and Time-Series Analysis*. Oxford University Press.

[19]. S. Boccaletti, C. Grebogi, Y.-C. Lai, H. Mancini & D. Maza, « The Control of Chaos: Theory and Applications », *Physics Reports*, 329(3), 2000, pp. 103–197.

[20]. H. Poincaré, Les Méthodes Nouvelles de la Mécanique Céleste, 1905.

[21]. P.-F. Verhulst, « Notice sur la loi que la population suit » (1838) ; R. M. May, « Simple mathematical models with very complicated dynamics », *Nature* 261 (1976), 459–467.

[22]. Eckmann, J.-P., & Ruelle, D. (1985). Ergodic theory of chaos and strange attractors. Reviews of Modern Physics, 57(3), 617-656.

[23]. Pecora & Carroll (1990) – Synchronisation de systèmes chaotiques

[24]. Walters, P. (1982). *An Introduction to Ergodic Theory*. Springer-Verlag.

[25]. *Using chaos synchronization … largest Lyapunov exponent* Stefański & Kapitaniak, 1999

[26]. *Cryptosystems Based on Chaos Theory* Alia, 2018 — logistic, Julia, Mandelbrot, attracteurs

[27]. *A review of cryptosystems based on multi layer chaotic mappings* arXiv, 2022.

[28]. **Lorenz, E. N.** (1963). *Deterministic Nonperiodic Flow*. *Journal of the Atmospheric Sciences*, 20(2), 130–141.

[29]. Parrow, C. (1982). *The Lorenz Equations: Bifurcations, Chaos, and Strange Attractors*. Springer-Verlag.

[30]. Pierre Gaspard, “Rossler systems”, Encyclopedia of Nonlinear Science

[31]. Sylvain Reynal et François MICHAUD, “L’attracteur de Hénon: introduction aux

[32]. Sandri, M. (1996). Numerical calculation of Lyapunov exponents. The Mathematica Journal, 6(3), 78-84.

[33]. AMD Vitis Model Composer, Design, simulate, generate code, and deploy to AMD Adaptive FPGAs and SoCs, https://www.mathworks.com/products/connections/product_detail/amd-vitis-model-composer.html

[34]. Luo, Y., Liu, Y., Liu, J., Tang, S., Harkin, J., & Cao, Y. (2021). Counteracting dynamical degradation of a class of digital chaotic systems via Unscented Kalman Filter and perturbation. *Information Sciences*, *556*, 49-66. https://doi.org/10.1016/j.ins.2020.12.065

[35]. Alvarez, G., & Li, S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. *International journal of bifurcation and chaos*, *16*(08), 2129-2151.https://doi.org/10.1142/S0218127406015970

[36]. Suneel, M. (2009). Cryptographic pseudo-random sequences from the chaotic Hénon map. *Sadhana*, *34*(5), 689-701. https://doi.org/10.1007/s12046-009-0040-y

[37]. Rukhin, A. et al. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, NIST SP800-22, Rev.1a, 2010. DOI : https://www.doi.org/10.6028/NIST.SP.800-22r1a

[38]. Soto, J. (1999). Statistical Testing of Random Number Generators. Proceedings of the 22nd National Information Systems Security Conference, NIST. https://csrc.nist.gov/pubs/nissc/1999/99papers.htm