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 : Horri Nassima et Adjalat Feryal

DOMAINE : Technologie

FILIERE : Electronique

OPTION : Systèmes embarqués

Thème

Conception sous « *Model composer* » d'un crypto-système chaotique pour le chiffrement des images

Jury de soutenance :

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

Promotion : 2024/2025

ملخص

يقدم هذا البحث نظام تشفير صور جديد يعتمد على نظام فوضوي تربيعي محسن، حيث تم دمج الخصائص الأساسية للأنظمة الفوضوية (مثل الحساسية الأسية للشروط الأولية والسلوك غير المتوقع) مع تقنيات التشفير المتقدمة لتطوير حل آمن وفعال. يعتمد النظام على آلية اضطراب مبتكرة تتضمن ثلاث مراحل رئيسية: تجزئة مخرج النظام، وعكس المقاطع الرقمية الخاص به، وتطبيق شبكة منطقية XOR-XNOR لزيادة الخصائص الفوضوية بشكل أحسن، هذه الآلية أدت إلى تحسين كبير في الخصائص الفوضوية.
أظهرت النتائج التجريبية أداءً متميزاً يتمثل في قيم أسس لياپونوف التي تم الحصول عليها (بين 1.45 و1.88) والتي تؤكد الخصائص الفوضوية القوية، ومعدل نجاح 100% في اختبارات NIST SP800-22بدقة 32 بت، وتأثير انهيار مثالي مع معدل خطأ في البتات يقارب 50%، وخصائص انتشار ممتازة حيث يؤثر تعديل بكسل واحد في الصورة الأصلية على كامل الصورة المشفرة. وبفضل هذه الميزات بالإضافة إلى الحساسية العالية للمفاتيح (بمساحة مفاتيح 360 بت)، يبرز هذا النظام كحل واعد لتشفير الصور، مع إمكانات كبيرة للتطبيق على وحدات FPGA لتحقيق أداء آني، مما يفتح آفاقاً جديدة في مجالات حيوية مثل أنظمة المراقبة الآمنة والتصوير الطبي السري واتصالات إنترنت الأشياء المضمنة.

الكلمات المفتاحية :التشفير الفوضوي، تشفير الصور، النظام التربيعي، تأثير الانهيار، اختباراتNIST ، تطبيقات FPGA للأمن المعلوماتي

Abstract

This thesis introduces an innovative image encryption system based on an optimized quadratic chaotic system, combining fundamental chaotic properties (exponential sensitivity to initial conditions, unpredictable behaviour) with advanced cryptographic techniques to deliver a secure and efficient solution. The system incorporates a novel perturbation mechanism involving three key steps: state vector segmentation, segment inversion, and XOR-XNOR logic network application, significantly enhancing chaotic properties. Experimental results demonstrate outstanding performance: Lyapunov exponents between 1.45 and 1.88 confirming strong chaotic characteristics, 100% success rate in NIST SP800-22 tests at 32-bit precision, optimal avalanche effect with ~50% bit error rate, and excellent diffusion properties where single-pixel modification uniformly affects the encrypted image. These features, combined with high key sensitivity (360-bit key space), position this system as a promising solution for secure image encryption. Future FPGA implementation is expected to achieve real-time performance, enabling practical applications in demanding fields such as secure surveillance, confidential medical imaging, and embedded IoT communications.

Keywords: chaotic cryptography, image encryption, quadratic system, avalanche effect, NIST tests, FPGA implementation, information security.

Résumé

Ce mémoire présente un nouveau système de chiffrement d'images basé sur un système chaotique quadratique optimisé. L'approche combine les propriétés fondamentales du chaos (sensibilité exponentielle aux conditions initiales, comportement imprévisible) avec des techniques cryptographiques avancées pour offrir une solution sécurisée et performante. Le système intègre un mécanisme de perturbation innovant comprenant trois étapes clés : découpage des vecteurs d'état, inversion des segments, et application d'un réseau logique XOR-XNOR, permettant d'améliorer significativement les propriétés chaotiques. Les résultats expérimentaux montrent des performances remarquables : des exposants de Lyapunov compris entre 1.45 et 1.88 confirmant le caractère fortement chaotique, une réussite à 100% des tests NIST SP800-22 à 32 bits, un effet avalanche optimal avec un taux d'erreur binaire proche de 50%, et une excellente propriété de diffusion où la modification d'un seul pixel affecte l'image chiffrée de manière uniforme. Ces caractéristiques, couplées à une grande sensibilité aux clés (espace de clés de 360 bits), positionnent ce système comme une solution prometteuse pour le chiffrement sécurisé d'images. Les perspectives d'implémentation sur FPGA devraient permettre d'atteindre des performances temps réel, ouvrant la voie à des applications concrètes dans des domaines exigeants comme la vidéosurveillance sécurisée, l'imagerie médicale confidentielle, ou les communications embarquées dans l'IoT.

Mots-clés : cryptographie chaotique, chiffrement d'images, système quadratique, effet avalanche, tests NIST, implémentation FPGA, sécurité informatique.

Dédicace

À celle qui a veillé sur mes nuits, sacrifié son confort pour le mien, à ma mère bien-aimée, source inépuisable de tendresse et d'amour, je te dédie ce travail avec toute ma gratitude et mon cœur.

À mon père cher, mon premier soutien, celui qui m'a toujours encouragée, merci pour ta présence, ta force et ta confiance.

À mes sœurs adorées, mes complices de toujours, merci pour votre amour, votre écoute et votre présence à mes côtés.

À mon cher mari Khaled**,** mon pilier, mon appui dans chaque étape, merci pour ta patience, ton aide précieuse et ton amour inconditionnel.

À mes enfants Tassnim, Abderrahmane trésors de ma vie, vous êtes ma lumière, ma source de motivation, ce travail est pour vous, avec tout mon amour.

À tous les membres de ma famille ….

Nassima

DEDICACE

Je dédie ce travail à :

À celle qui m'a donné la vie, qui m'a appris la patience, la persévérance et le sens du devoir...

Merci du fond du cœur, ma chère MÈRE.

À celui qui a toujours été un modèle de courage, de sagesse et de générosité...

Merci infiniment, mon PÈRE.

À mon cousin Melik Hamada, dont le soutien, l'encouragement et la présence ont toujours été pour moi une grande source de motivation.

À mon frère Ziad Adjalat, pour sa fidélité, son aide inestimable, et pour avoir toujours cru en moi, même dans les moments les plus difficiles.

Feryal

INTRODUCTION GENERALE

CHAPITRE 1 : INTRODUCTION SUR LA CRYPTOGRAPHIE

1. INTRODUCTION 3
2. DEFINITION DE LA CRYPTOGRAPHIE 3
   2.1. Objectifs de la cryptographie *4*
3. TYPES DE CRYPTOGRAPHIE 5
   3.1. Cryptographie à clé symétrique *6*
      3.1.1. Data Encryptions Standard (DES) 7
      3.1.2. Triple DES (3DES) 7
         3.1.1.1 Avantages du 3DES 8
         3.1.2.2. Limitations du 3DES 8
         3.1.2.3. Applications du 3DES 8
      3.1.3. Advanced Encryptions Standard (AES) 9
      3.1.4. Autres systèmes de chiffrement symétrique 10
   3.2. Cryptographie asymétrique *11*
      3.2.1. Algorithmes asymétriques courants 11
         3.2.1.1. RSA (Rivest-Shamir-Adleman) 11
         3.2.1.2. ElGamal 12
         3.2.1.3. Courbes elliptiques (ECC) 12
      3.2.2. Applications pratiques 12
      3.2.3. Avantages et limites de la cryptographie asymétrique 12
4. LES GENERATEURS PSEUDO-ALEATOIRES DANS LA CRYPTOGRAPHIE 13
   4.1 Définition d'un PRNG cryptographique *13*
   4.2. Utilisations en cryptographie *13*
5. CONCLUSION 14

CHAPITRE 2 : SYSTEMES CHAOTIQUES ET APPLICATION EN CRYPTOGRAPHIE .

1. INTRODUCTION 15
2. LE CHAOS : DEFINITION ET PROPRIETES 15
3. DEFINITION DES SYSTEMES DYNAMIQUES 15
   3.1. Systèmes dynamiques à temps continu *16*
   3.2. Systèmes dynamiques à temps discret *17*
4. DEFINITION DES SYSTEMES CHAOTIQUES 17
   4.1 Déterminisme et imprévisibilité *17*
   4.2 Caractéristiques Fondamentales des Systèmes Chaotiques *18*
5. EXEMPLES DE CARTES SYSTEMES CHAOTIQUES 18
   5.1. Carte Logistique *19*
   5.2. Carte de Hénon *19*
   5.3. L'attracteur chaotique de Lorenz *20*
   5.4. La carte Tent (Tent map) *21*
6. EXPLICATION DE LA DIFFERENCE ENTRE CHAOS ET PHENOMENES ALEATOIRES 22
7. AVANTAGES DE L'UTILISATION DU CHAOS EN CRYPTOGRAPHIE 23
8. APPLICATIONS DE LA CRYPTOGRAPHIQUES BASEES SUR LE CHAOS 24

9. DEFIS ET LIMITATIONS DE LA CRYPTOGRAPHIE BASEES SUR LE CHAOS....25
10. CONCLUSION....26

CHAPITRE 3 : CONCEPTION D'UN CRYPTO-SYSTEME A BASE DU CHAOS POUR LE CRYPTAGE DES IMAGES

1. INTRODUCTION....27
2. LE SYSTEME QUADRATIQUE CHAOTIQUE....27
2.1. Evaluation de comportement chaotique du system Quadratique 29
2.1.1. La fonction d'autocorrélation 30
2.1.2. Analyse par le diagramme de bifurcation.... 33
2.1.3. Analyse statistique 35
3. LE MECANISME PROPOSE POUR AMELIORER LA DYNAMIQUE DE SYSTEME CHAOTIQUE 37
4. ÉVALUATION DU MECANISME PROPOSE....38
4.1. Analyse de l'espace de phase 39
4.2. Longueur de cycle de la séquence générées.... 40
4.3. Analyse statistique.... 40
4.4. Evaluation de complexité en utilisant l'Exposant de Lyaponov 42
4.5. Diagrammes de Bifurcation de système Quadratique modifié.... 43
5. PROCESSUS DE CRYPTAGE D'UNE IMAGE....44
6. EVALUATION DE CRYPTO-SYSTEME PROPOSE....47
6.1. Analyse de clé 48
6.1.1. La taille de la clé.... 48
6.1.2. La sensibilité des clés.... 49
6.2. L'évaluation de la propriété de diffusion.... 53
7. CONCLUSION....55

CONCLUSION GENERALE

BIBLIOGRAPHIES

CHAPITRE 1 : INTRODUCTION SUR LA CRYPTOGRAPHIE

Figure 1 : Le principe de la cryptographie 3

Figure 2 : Chiffrement à clé symétrique : la même clé est utilisée pour le chiffrement et le déchiffrement 6

Figure 3 : Fonctionnement du 3DES [9] 8

Figure 4 : Chiffrement AES 10

Figure 5 : Principe de chiffrement dans la cryptographie asymétrique 11

CHAPITRE 2 : SYSTEMES CHAOTIQUES ET APPLICATION EN CRYPTOGRAPHIE

Figure 1 : Différents tracés de l'application de Hénon 20

Figure 2 : L'attracteur chaotique de Lorenz. 21

Figure 3 : Tracé de la fonction Tent map. 22

CHAPITRE 3 : CONCEPTION D'UN CRYPTO-SYSTEME A BASE DU CHAOS POUR LE CRYPTAGE DES IMAGES

Figure 1 : Espace des phases et séries temporelles du chaotique Quadratique 29

Figure 2 : Analyse de comportement de système chaotique Quadratique en utilisant la fonction d'autocorrélation 31

Figure 3 : Diagrammes de bifurcation de système chaotique Quadratique 34

Figure 4 : Architecture fonctionnelle de mécanisme proposé 38

Figure 5 : L'espace de phase du système Quadratique modifié 39

Figure 6 : Evolution de LLE en fonction des paramètres de control 42

Figure 7 : Diagrammes de bifurcation du système Quadratique modifié 43

Figure 8 : Le schéma synoptique du mécanisme de chiffrement proposé 46

Figure 9 : Résultat de cryptage et décryptage d'une image, l'image originale (gauche), l'image cryptée..... 47

Figure 10 : Le schéma de processus de génération de paramètres de contrôle a partir de la clé globale de système..... 49

Figure 11 : Résultats de cryptage et décryptage d'une image RVB, (2) : l'image cryptée, (3) à (7) : les images décrypter par des clés différentes à celle utilisée pour le cryptage, (8) : l'image décryptée par la clé correcte. 50

Figure 12 : Évolution du BER en fonction de deux clés proches : validation de l'effet avalanche..... 52

Figure 13 : Évaluation de la propriété de diffusion : 1) image originale, 2) image chiffrée, 3) image chiffrée après inversion d'un seul bit sur le premier pixel de l'image originale, 4) différence entre les images (2) et (3). 54

CHAPITRE 3 : CONCEPTION D'UN CRYPTO-SYSTEME A BASE DU CHAOS POUR LE CRYPTAGE DES IMAGES

Tableau 1 : Résultats des tests NIST SP 800-22 appliqués aux sorties binaires du système quadratique chaotique pour différentes précisions numériques 36

Tableau 2 : Résultats des tests NIST SP 800-22 appliqués aux sorties binaires du système Quadratique chaotique modifié par le MP pour différentes précisions 41

Introduction Générale

À l'ère du numérique, où les données sensibles circulent en permanence à travers des réseaux diversifiés, la sécurité informatique est devenue un pilier incontournable pour garantir la confidentialité, l'intégrité et l'authenticité des informations. La cryptographie, en tant que discipline fondamentale de la sécurité, joue un rôle essentiel dans la protection des communications et du stockage des données. Cependant, face à l'évolution des menaces cybernétiques et à la complexité croissante des systèmes informatiques, les méthodes cryptographiques traditionnelles doivent constamment se renouveler pour rester efficaces.

Dans ce contexte, les systèmes chaotiques émergent comme une alternative prometteuse, offrant des propriétés uniques telles que la sensibilité extrême aux conditions initiales, l'imprévisibilité et la complexité dynamique. Ces caractéristiques en font des candidats idéaux pour des applications cryptographiques robustes, notamment dans le domaine du chiffrement d'images, où la rapidité et la sécurité sont des exigences critiques.

Ce mémoire de fin d'études explore l'intégration des systèmes chaotiques dans la cryptographie moderne, en proposant une approche innovante pour le chiffrement symétrique par flot. Structuré en trois chapitres, il aborde successivement les fondements théoriques de la cryptographie, les propriétés des systèmes chaotiques et leur application pratique dans la conception d'un crypto-système dédié au chiffrement d'images.

Le premier chapitre introduit les principes de base de la cryptographie, en mettant l'accent sur ses objectifs fondamentaux et ses deux grandes familles d'algorithmes : symétriques et asymétriques. Il présente également les générateurs pseudo-aléatoires, essentiels pour la sécurisation des protocoles cryptographiques.

Le deuxième chapitre se concentre sur les systèmes chaotiques, en détaillant leurs propriétés mathématiques et leur potentiel en cryptographie. Des exemples classiques, tels que l'attracteur de Lorenz et la carte logistique, illustrent leur comportement dynamique, tandis que les défis liés à leur implémentation numérique sont discutés pour en cerner les limites et les opportunités.

Le troisième chapitre présente la conception d'un crypto-système basé sur un système chaotique quadratique amélioré, spécifiquement adapté au chiffrement d'images. Une analyse approfondie

permet d'évaluer sa robustesse et son efficacité, ouvrant la voie à des applications concrètes dans des environnements nécessitant une sécurité renforcée.

À travers cette étude, nous aspirons à contribuer à l'avancement des techniques cryptographiques modernes, en combinant la rigueur des approches traditionnelles avec l'innovation offerte par les systèmes dynamiques chaotiques. Ce mémoire s'adresse aussi bien aux chercheurs en cybersécurité qu'aux ingénieurs souhaitant approfondir leurs connaissances sur les méthodes émergentes de protection des données.

CHAPITRE I : INTRODUCTION SUR LA CRYPTOGRAPHIE

1. Introduction

La cryptographie est la science qui consiste à sécuriser l'information grâce à des techniques et algorithmes mathématiques. Elle joue un rôle fondamental dans la protection de la confidentialité, de l'intégrité et de l'authenticité des données dans le monde numérique. Des méthodes anciennes d'écriture secrète aux systèmes de chiffrement modernes utilisés dans les transactions bancaires en ligne et les communications, la cryptographie a considérablement évolué pour répondre aux défis croissants de la cybersécurité.

Ce chapitre propose une introduction aux principes cryptographiques, un aperçu historique et les concepts clés qui sous-tendent les systèmes cryptographiques contemporains.

2. Définition de la cryptographie

La cryptographie est la science et la pratique visant à sécuriser l'information en la convertissant sous une forme illisible pour toute personne non autorisée. Le terme provient des mots grecs kryptos (caché) et graphein (écrire), soulignant son rôle traditionnel de dissimulation des messages. Fondamentalement, la cryptographie repose sur deux processus principaux :

- Le chiffrement, qui transforme des données lisibles (texte clair) en un format illisible (texte chiffré).
- Le déchiffrement, qui restaure les données originales à l'aide d'une clé spécifique.

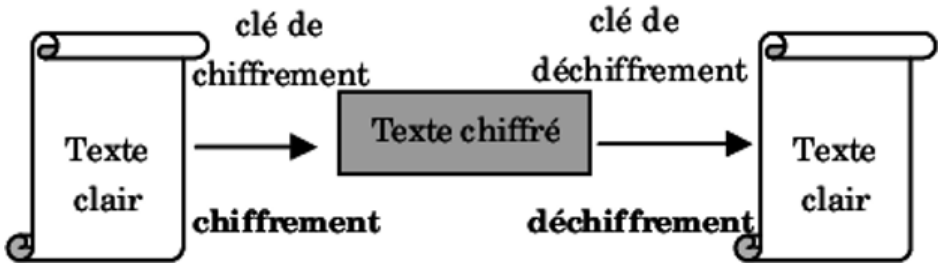

Figure 1 : Le principe de la cryptographie

.

Historiquement utilisée dans les communications militaires et diplomatiques, la cryptographie est devenue un pilier des systèmes numériques modernes. Elle garantit aujourd'hui :

- La sécurité des communications sur Internet,

- La protection des données stockées dans les systèmes et appareils,
- Le fonctionnement de technologies comme les signatures numériques et l'authentification sécurisée.

Les méthodes cryptographiques modernes s'appuient sur des algorithmes mathématiques complexes et des techniques informatiques, regroupées en deux grandes catégories :

- **Cryptographie à clé symétrique** : une même clé est utilisée pour le chiffrement et le déchiffrement.
- **Cryptographie à clé asymétrique** (ou cryptographie publique) : utilise une paire de clés mathématiquement liées (une pour chiffrer, l'autre pour déchiffrer).

Comme nous le verrons dans la section suivante, la cryptographie ne se limite pas à la confidentialité. Elle joue un rôle central dans la sécurité globale des systèmes d'information, en garantissant l'intégrité, l'authenticité et la non-répudiation des données.

2.1. Objectifs de la cryptographie

La cryptographie constitue la base de la sécurité de l'information moderne à travers quatre principes essentiels :

- **Confidentialité** : La confidentialité fait référence à la protection des informations contre tout accès ou divulgation non autorisés. Elle garantit que seules les parties autorisées peuvent lire ou comprendre les données. En cryptographie, la confidentialité est assurée par l'utilisation d'algorithmes de chiffrement tels que AES (Advanced Encryption Standard) ou RSA (Rivest–Shamir–Adleman), qui transforment le message original (texte en clair) en un format illisible (texte chiffré). Seules les parties possédant la clé de déchiffrement adéquate peuvent récupérer les informations d'origine. Même si un attaquant intercepte le message, sans la clé appropriée, il ne peut en interpréter le contenu. La confidentialité est essentielle pour sécuriser les données sensibles, telles que les informations personnelles, les dossiers financiers et les communications classifiées [1].
- **Intégrité** : L'intégrité garantit que l'information n'a pas été modifiée, intentionnellement ou accidentellement, durant son stockage ou sa transmission. Elle protège les données contre toute modification non autorisée en utilisant des fonctions de hachage cryptographique, telles que SHA-256, ou des codes d'authentification de message (MAC), qui créent une empreinte numérique unique des données. Ces empreintes permettent au récepteur de vérifier que

l'information est restée inchangée durant toute sa transmission ou son stockage. Une petite modification des données produira une valeur de hachage très différente, révélant immédiatement toute altération ou corruption. L'intégrité est cruciale dans les applications où la fiabilité des données est primordiale, comme les transactions financières, les mises à jour logicielles et les documents juridiques_[2].

Exemple : Lorsqu'un utilisateur télécharge un logiciel, il compare souvent la valeur de hachage fournie avec celle calculée à partir du fichier téléchargé pour s'assurer qu'aucune modification malveillante n'a été apportée.

- **Authentification** : L'authentification est le processus de vérification de l'identité d'un utilisateur, d'un dispositif ou d'un système, afin de s'assurer que l'entité impliquée dans la communication ou accédant à un système est bien celle qu'elle prétend être. Elle est généralement mise en œuvre par des signatures numériques, des mots de passe ou des mécanismes d'authentification multifactorielle qui combinent plusieurs formes de vérification, telles que quelque chose que l'utilisateur connaît (mot de passe), quelque chose qu'il possède (une carte à puce ou un jeton) et quelque chose qu'il est (des données biométriques comme les empreintes digitales). L'authentification joue un rôle essentiel dans la sécurisation des systèmes et des transactions en empêchant l'accès non autorisé et les attaques par usurpation d'identité. Dans les systèmes cryptographiques, les certificats numériques délivrés par des autorités de confiance (Autorités de Certification - CA) sont également fréquemment utilisés pour authentifier les identités [3].

  Exemple : Lorsque vous vous connectez à votre compte de messagerie, le système vérifie votre mot de passe pour authentifier votre identité avant d'accorder l'accès.

3. Types de cryptographie

Il existe plusieurs types de cryptographie, chacun reposant sur des techniques et des applications différentes. Les deux principales catégories de systèmes de chiffrement sont : la cryptographie à clé symétrique et la cryptographie à clé asymétrique. Les sous-sections suivantes présentent les principaux types :

3.1. Cryptographie à clé symétrique

La cryptographie à clé symétrique, également appelée cryptographie à clé privée, est une méthode cryptographique dans laquelle la même clé secrète est utilisée à la fois pour le chiffrement du texte en clair et pour le déchiffrement du texte chiffré. Cette approche suppose que l'émetteur et le récepteur partagent la même clé, laquelle doit rester confidentielle. Le concept de base est simple : les données sont chiffrées en appliquant une fonction mathématique utilisant la clé partagée, et la même clé est utilisée en sens inverse pour déchiffrer les données. Étant donné que les clés de chiffrement et de déchiffrement sont identiques, le principal défi réside dans la distribution sécurisée de la clé sur des canaux potentiellement non sécurisés. Cette méthode est l'une des plus anciennes et des plus fondamentales en cryptographie [4].

Figure 2 : Chiffrement à clé symétrique : la même clé est utilisée pour le chiffrement et le déchiffrement.

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.

Plusieurs algorithmes à clé symétrique ont été développés au fil des années, chacun avec sa propre structure, ses avantages et ses domaines d'application. Certains sont conçus pour la vitesse et l'efficacité, tandis que d'autres mettent davantage l'accent sur la robustesse de la sécurité. Voici un aperçu des systèmes cryptographiques à clé symétrique les plus notables, mettant en évidence leurs principales caractéristiques et leur pertinence pratique.

3.1.1. Data Encryptions Standard (DES)

Le *Data Encryption Standard* (DES) est un algorithme de chiffrement par blocs à clé symétrique ; il a été développé dans les années 1970 par IBM et adopté comme norme fédérale par le *National Institute of Standards and Technology* (NIST) en 1977 [5]. Le DES traite des blocs de texte en clair de 64 bits à l'aide d'une clé de 56 bits. L'algorithme comporte 16 tours d'opérations complexes de substitution et de permutation. Malgré son adoption généralisée dans les années 1980 et au début des années 1990, le DES a fini par se révéler vulnérable aux attaques par force brute en raison de la courte longueur de sa clé.

La première rupture pratique majeure du DES a eu lieu en 1998, lorsque *l'Electronic Frontier Foundation* (EFF) a construit une machine appelée "Deep Crack" capable de casser des messages chiffrés par DES en quelques jours [6]. Aujourd'hui, le DES est considéré comme non sécurisé en raison de la faible longueur de sa clé, qui le rend vulnérable aux attaques par force brute. Il a cependant jeté les bases d'algorithmes ultérieurs, bien que son utilisation soit désormais largement obsolète [7].

3.1.2. Triple DES (3DES)

Le Triple DES (3DES) a été introduit pour renforcer la sécurité du DES en appliquant ce dernier trois fois à chaque bloc : chiffrement-dé chiffrement-chiffrement, en utilisant trois clés différentes [8]. Il augmente effectivement la longueur de la clé à 168 bits lorsqu'on utilise trois clés uniques, et à 112 bits lorsqu'on en utilise deux (K1 = K3) [4].

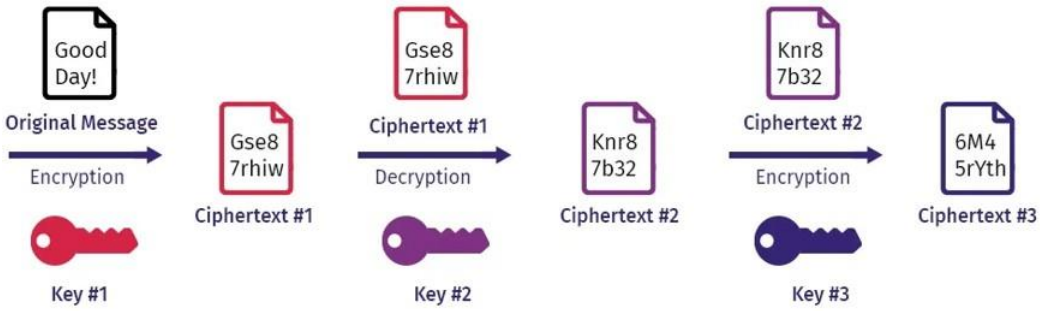

Figure 3 : Fonctionnement du 3DES [9]

3.1.1.1 Avantages du 3DES

Le 3DES (Triple DES) présente plusieurs avantages, notamment une sécurité renforcée grâce à son chiffrement en trois couches, ce qui le rend plus robuste que le DES standard. Il reste largement utilisé et est pris en charge par de nombreuses normes et protocoles de chiffrement. De plus, le 3DES est rétrocompatible avec le DES, permettant une intégration fluide dans les systèmes existants. Son support de tailles de clés personnalisables renforce également son adaptabilité à divers niveaux d'exigences en matière de sécurité.

3.1.2.2. Limitations du 3DES

Le 3DES présente des inconvénients notables, notamment une vitesse de traitement lente due à son mécanisme de triple chiffrement, le rendant nettement moins efficace que les algorithmes modernes comme l'AES. De plus, bien qu'il propose des tailles de clés variables, sa longueur maximale de 192 bits reste inférieure aux exigences de sécurité actuelles, limitant son efficacité face aux attaques cryptographiques avancées. Ces limitations ont conduit à son retrait progressif au profit d'alternatives plus robustes.

3.1.2.3. Applications du 3DES

Le Triple DES (3DES) est un algorithme de chiffrement robuste, largement utilisé dans divers secteurs pour garantir la sécurité des données. Dans les transactions financières, il protège les opérations bancaires en ligne, le traitement des cartes de crédit et les transferts de fonds électroniques en chiffrant les données sensibles. Pour les réseaux privés virtuels (VPN), le 3DES sécurise les communications à distance, assurant confidentialité et intégrité pour les entreprises et les particuliers.

Dans les systèmes de santé, il protège les données confidentielles des patients, y compris les dossiers médicaux électroniques (DME) et les images médicales, en conformité avec des réglementations comme la HIPAA.

En outre, les agences gouvernementales et militaires utilisent le 3DES pour sécuriser les communications classifiées et les transferts de données sensibles, tirant parti de ses capacités de chiffrement éprouvées. Bien qu'il soit progressivement remplacé par l'AES dans certaines applications, le 3DES reste pertinent dans les systèmes hérités grâce à sa fiabilité et à sa sécurité reconnue.

3.1.3. Advanced Encryptions Standard (AES)

La norme de chiffrement *Advanced Encryption Standard* (AES) a été sélectionnée par le NIST en 2001 à la suite d'un concours public lancé en 1997 (NIST, 2001). L'algorithme gagnant, Rijndael, a été conçu par Joan Daemen et Vincent Rijmen [10]. L'AES est un chiffrement par blocs symétrique qui comprend trois variantes selon la taille de la clé : AES-128, AES-192 et AES-256 :

- AES-128 utilise une clé de 128 bits pour chiffrer et déchiffrer les messages.
- AES-192 utilise une clé de 192 bits.
- AES-256 utilise une clé de 256 bits.

Chaque variante chiffre et déchiffre des données par blocs de 128 bits à l'aide de clés cryptographiques respectives de 128, 192 et 256 bits. Le nombre de tours de chiffrement varie en fonction de la taille de la clé :

- 10 tours pour les clés de 128 bits.
- 12 tours pour les clés de 192 bits.
- 14 tours pour les clés de 256 bits.
-

Chaque tour comprend plusieurs étapes de traitement, notamment :

- Substitution (remplacement des données par des valeurs issues d'une table de correspondance),
- Transposition (décalage des lignes ou des colonnes),
- Mélange (combinaison des données pour diffuser les motifs).

Ces étapes transforment le texte en clair en texte chiffré, assurant une sécurité renforcée grâce à de multiples couches de confusion et de diffusion.

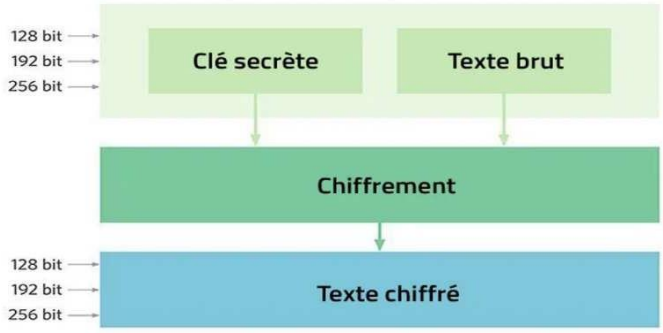

Figure 4 : Chiffrement AES.

3.1.4. Autres systèmes de chiffrement symétrique

Dans cette section, nous résumons brièvement quelques systèmes de chiffrement symétrique existants, notamment : Blowfish, Twofish et les algorithmes RC :

- **Blowfish** : Blowfish a été créé par Bruce Schneier en 1993 comme une alternative rapide, gratuite et non brevetée aux chiffrements par blocs existants [11]. Il fonctionne sur des blocs de 64 bits et accepte des longueurs de clé allant de 32 à 448 bits. L'algorithme utilise un réseau de Feistel à 16 tours avec de grandes boîtes S dépendantes de la clé. Son principal inconvénient aujourd'hui est la petite taille des blocs (64 bits), qui peut entraîner des vulnérabilités dues à des collisions de blocs dans les grands ensembles de données [7].
- **Twofish** : Twofish, également développé par Schneier et ses collaborateurs, a été soumis au concours AES en 1998 [12]. Il fonctionne sur des blocs de 128 bits et prend en charge des clés allant jusqu'à 256 bits. Twofish utilise des boîtes S pré-calculées dépendantes de la clé et un ordonnancement complexe de celle-ci. Bien qu'il n'ait pas été retenu comme norme AES, il reste un chiffrement solide, libre de droits, utilisé dans des outils comme VeraCrypt et GnuPG.
- **Algorithmes RC (RC2, RC4, RC5, RC6)** : La série RC (Rivest Cipher) comprend plusieurs algorithmes conçus par Ron Rivest chez *RSA Security* :
  - **RC2** est un chiffrement par blocs de 64 bits avec une longueur de clé variable, conçu pour répondre aux exigences d'exportation dans les années 1980 [13].
  - **RC4** est un chiffrement par flot autrefois largement utilisé dans les protocoles SSL/TLS et WEP, aujourd'hui obsolète en raison de sorties prévisibles et de failles dans son algorithme d'initialisation de clé [14].
  - **RC5** introduit des rotations dépendantes des données, des tailles de blocs et des longueurs de clé variables [15].

- **RC6** est une amélioration du RC5 soumise au concours AES. Il prend en charge des blocs de 128 bits et des clés allant jusqu'à 256 bits, mais n'a pas été sélectionné pour la standardisation [13].

3.2. Cryptographie asymétrique

La cryptographie asymétrique, également appelée cryptographie à clé publique, est un pilier fondamental de la sécurité moderne de l'information. Contrairement à la cryptographie symétrique, où une même clé est utilisée pour le chiffrement et le déchiffrement, la cryptographie asymétrique repose sur une paire de clés distinctes : une **clé publique** (partagée avec tout le monde) et une **clé privée** (gardée secrète par le propriétaire) [16].

L'idée centrale de la cryptographie asymétrique repose sur des **fonctions mathématiques unidirectionnelles**, c'est-à-dire faciles à calculer dans un sens (chiffrement), mais extrêmement difficiles à inverser sans information supplémentaire (clé privée). Lorsqu'un message est chiffré avec la clé publique d'un destinataire, seul ce dernier peut le déchiffrer grâce à sa clé privée. L'inverse est aussi vrai pour la **signature numérique** : un message signé avec une clé privée peut être vérifié par tous avec la clé publique [17].

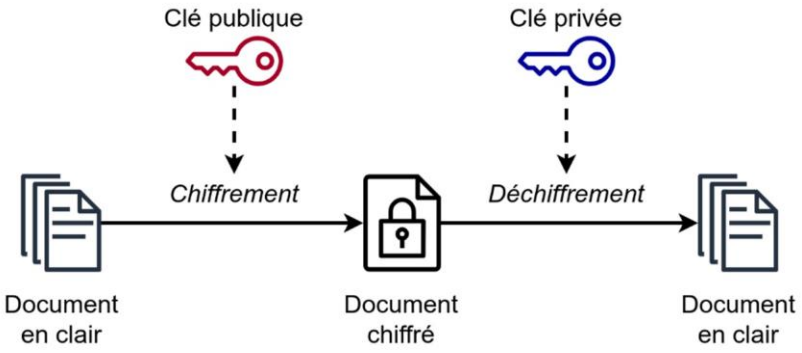

Figure 5 : Principe de chiffrement dans la cryptographie asymétrique.

3.2.1. Algorithmes asymétriques courants

Plusieurs algorithmes asymétriques ont été développés au fil du temps, chacun reposant sur des problèmes mathématiques différents considérés comme difficiles à résoudre sans la clé privée. Ces algorithmes varient en termes de sécurité, de performance, de taille de clé et d'applications. Les plus connus et les plus utilisés dans les systèmes modernes de sécurité sont présentés ci-dessous.

3.2.1.1. RSA (Rivest-Shamir-Adleman)

RSA est l'algorithme asymétrique le plus utilisé. Il repose sur la difficulté de factoriser de grands nombres premiers. Créé en 1977, il est encore largement utilisé dans les certificats SSL/TLS, les

signatures numériques et le chiffrement d'e-mails [18]. RSA utilise des tailles de clé typiquement de 2048 bits ou plus pour garantir la sécurité

3.2.1.2. ElGamal

L'algorithme ElGamal est basé sur le problème du logarithme discret. Il est souvent utilisé dans les systèmes de vote électronique et les applications nécessitant un **chiffrement probabiliste**, c'est-à-dire produisant un résultat différent même pour un même message et une même clé publique [19].

3.2.1.3. Courbes elliptiques (ECC)

La cryptographie à courbes elliptiques permet une sécurité équivalente à RSA mais avec des clés beaucoup plus courtes (ex : 256 bits ECC ≈ 3072 bits RSA). Cela améliore les performances, notamment dans les dispositifs mobiles, tout en maintenant une forte sécurité [20].

3.2.2. Applications pratiques

La cryptographie asymétrique est omniprésente dans les technologies numériques actuelles :

- **SSL/TLS** : sécurise les connexions entre les navigateurs et les serveurs web.
- **Signature numérique** : garantit l'intégrité et l'authenticité des documents numériques (ex : eIDAS, e-signature).
- **PGP (Pretty Good Privacy)** : système de chiffrement des e-mails basé sur une infrastructure à clé publique [21].
- **Blockchain et cryptomonnaies** : les transactions Bitcoin, par exemple, sont validées via des signatures numériques utilisant ECC.

3.2.3. Avantages et limites de la cryptographie asymétrique

La cryptographie asymétrique présente plusieurs avantages notables. Elle ne nécessite pas de partage préalable de clé secrète, ce qui élimine les risques liés à la distribution sécurisée des clés. Elle permet également l'authentification des utilisateurs et des données via des signatures numériques, assurant ainsi l'intégrité et l'origine des messages. De plus, elle s'intègre aisément dans des infrastructures de grande envergure, comme les systèmes de certificats numériques ou les protocoles de sécurité sur Internet. Toutefois, cette approche comporte aussi des limites. Elle est généralement plus lente que la cryptographie symétrique en raison de la complexité des calculs mathématiques

impliqués. De surcroît, certains algorithmes asymétriques deviennent vulnérables face à l'informatique quantique, notamment à travers l'algorithme de Shor, capable de factoriser de grands nombres entiers en temps polynomial. Ces vulnérabilités justifient l'intérêt croissant pour la cryptographie post-quantique, en cours de normalisation [22].

4. Les générateurs pseudo-aléatoires dans la cryptographie

La cryptographie moderne repose fortement sur la génération de nombres aléatoires pour de nombreuses opérations : création de clés secrètes, vecteurs d'initialisation, nombres nonces, remplissage (padding), etc. Cependant, obtenir du vrai aléa à partir de phénomènes physiques est souvent difficile, coûteux ou lent. C'est pourquoi les générateurs pseudo-aléatoires (PRNG, *Pseudo-Random Number Generators*) sont largement utilisés : ils permettent de produire des séquences de nombres qui semblent aléatoires, mais qui sont en réalité déterministes à partir d'une valeur initiale appelée graine (*seed*).

4.1 Définition d'un PRNG cryptographique

Un PRNG cryptographique est un algorithme déterministe capable de générer une suite de bits qui ne peut pas être distinguée d'une suite véritablement aléatoire sans une connaissance préalable de la graine. Il doit satisfaire les propriétés suivantes [8] :

- Indistinguabilité : Il doit être computationnellement difficile de distinguer la sortie du PRNG d'une véritable suite aléatoire.
- Résistance à l'attaque par retour arrière *(backtracking resistance*) : Même si une sortie est connue, il doit être difficile de retrouver les sorties précédentes.
- Résistance à l'attaque par prédiction avant (*forward prediction resistance*) : Connaître les sorties précédentes ne doit pas permettre de deviner les suivantes.

4.2. Utilisations en cryptographie

Les PRNG sont utilisés dans de nombreuses tâches cryptographiques :

- Génération de clés secrètes (AES, RSA, etc.)
- Génération de vecteurs d'initialisation (IV) dans les modes de chiffrement comme CBC ou CTR.

- Génération de sel (salt) pour le hachage sécurisé des mots de passe.
- Protocoles cryptographiques nécessitant des défis (nonces) pour l'authentification ou l'accord de clé (ex : TLS, Diffie-Hellman)

5. Conclusion

Ce chapitre a introduit les bases de la cryptographie, un domaine vaste et en constante évolution. Nous avons abordé ses objectifs principaux (confidentialité, intégrité, authentification) et ses deux grandes catégories d'algorithmes : symétriques (AES, DES) et asymétriques (RSA, ECC).

Cependant, cette introduction ne couvre qu'une infime partie du sujet. La cryptographie s'étend à des enjeux avancés comme les protocoles sécurisés, les menaces quantiques et les applications modernes (blockchain, IoT).

En résumé, la cryptographie reste un pilier essentiel de la sécurité numérique, alliant théorie et pratique pour protéger nos données dans un monde de plus en plus connecté.

CHAPITRE II : SYSTEMES CHAOTIQUES ET APPLICATION EN CRYPTOGRAPHIE

1. Introduction

Les systèmes chaotiques sont des systèmes dynamiques déterministes dont l'évolution est extrêmement sensible aux conditions initiales, ce qui rend leur comportement à long terme difficilement prévisible. Leur complexité apparente et leur capacité à générer des séquences pseudo-aléatoires les rendent particulièrement adaptés aux applications en cryptographie. Exploités pour renforcer la confidentialité, la diffusion et la confusion des données, les systèmes chaotiques sont utilisés dans le chiffrement de textes, d'images, de vidéos, ainsi que dans la génération de clés cryptographiques. De la modélisation mathématique à leur intégration dans des algorithmes de chiffrement modernes, ils offrent des perspectives innovantes pour répondre aux enjeux croissants de la sécurité de l'information.

Ce chapitre se propose d'introduire les fondements des systèmes chaotiques en mettant en lumière leurs principales caractéristiques. Il présente un aperçu des applications du chaos en cryptographie, allant de la génération de clés à la conception de systèmes de chiffrement basés sur des réseaux chaotiques, tout en abordant les défis techniques et théoriques encore à relever, notamment en ce qui concerne la mise en œuvre numérique et la validation de la sécurité.

2. Le chaos : Définition et propriétés

Le "chaos" est le terme utilisé pour décrire le comportement apparemment complexe de ce que nous considérons être simples [23]. Le chaos est défini généralement comme un comportement particulier d'un système dynamique déterministe non linéaire. Du point de vue mathématique la notion générale de système dynamique est définie à son tour à partir d'un ensemble de variables qui forment le vecteur d'état **x** = {xi R}, i = 1...*n* où *n* représente la dimension du vecteur. Ce jeu de variables à la propriété de caractériser complètement l'état instantané du système dynamique générique. En associant en plus un système de coordonnées on obtient l'espace d'état qui est appelé également *l'espace de phase* [24], il s'agit d'un espace de dimensions deux ou trois dans lequel chaque coordonnée est une variable d'état du système considéré [25]. Conjointement avec l'espace d'état un système dynamique est défini aussi par une loi d'évolution, généralement désignée par *dynamique*, qui caractérise l'évolution de l'état du système en temps [24]. La notion de déterminisme provient du fait que le système considéré est complètement caractérisé par son état initial et sa dynamique.

3. Définition des Systèmes dynamiques

un système dynamique est un système classique qui évolue au cours du temps soit de façon discrète (à temps discret) décrits chacun par une équation de la forme $x_{k+1} = f(x_k)$, soit de façon continu (à temps continu) décrits par des équations différentielles. Les seconds, cependant, sont discrétisés pour les besoins du calcul informatique : on les simule par un pas de temps très petits par rapport à l'échelle de temps du phénomène étudié. Un système dynamique possède en général un ou plusieurs paramètres dits « de contrôle », qui agissent sur les caractéristiques de la fonction de transition. Selon la valeur du paramètre de contrôle, les mêmes conditions initiales mènent à des trajectoires correspondant à des régimes dynamiques qualitativement différents. La modification du paramètre de contrôle peut conduire à une modification de la nature des régimes dynamiques développés dans le système.

3.1. Systèmes dynamiques à temps continu

Soit l'équation différentielle $\dot{x}(t) = F(x(t), t)$ (1.1)

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

Si on associe à cette dynamique un état initial $x_0 = x(t_0)$, pour chaque couple choisi (x_0 , t_0) On peut identifier une solution unique $\Phi\ (. ; x_0, t_0) : R^+ \rightarrow R^n$ telle que :

$$\Phi_F (t_0, x_0 , t_0) = x_0 \, et \, \dot{\Phi}_F (t , x_0, t_0) = F (\Phi_F(t ; x_0 , t_0), t) \quad (1.2)$$

Cette solution unique déterminée avec l'aide des équations (1.2), et qui fournit l'ensemble d'états successifs occupés par le système à chaque instant *t*, s'appelle généralement trajectoire. Si F ne dépend pas explicitement du temps, mais seulement de *x*, le système est dit autonome. Notons qu'un système dynamique non autonome peut toujours être ramené à un système autonome en introduisant un nouveau degré de liberté $\theta = t$ régi par l'équation dθ/dt = 1 [26].

3.2. Systèmes dynamiques à temps discret

Le système dynamique dans ce cas est représenté par des équations aux différences finies, avec le modèle général suivant :

$$x(k+1) = G(x(k), k) \qquad (1.3)$$

Où G : $R^n \times R^+ \rightarrow R^n$ désigne la dynamique du système en temps discret.

De même qu'en temps continu, si on associe à cette dynamique un état initial $x_0 = x(t_0)$
Pour chaque couple choisi (x_0 , t_0) on peut identifier une solution unique
$\Phi\,(.\,;\, x_0, t_0)$ de $R^+ \rightarrow R^n$ telle que :

$$\Phi_G(k_0; x_0, k_0) = x_0 \; et \;\; \Phi_G(k+1\,;\, x_0\,, k_0) = G(\Phi_G(k; x_0\,, k_0), t) \qquad (1.4)$$

En temps discret on définit aussi le système autonome comme une dynamique qui ne dépend pas de l'instant k.

4. Définition des Systèmes Chaotiques :

Un système chaotique est un système dynamique non linéaire. Un système dynamique est simplement un ensemble de fonctions (règles, équations) qui spécifient comment les variables évoluent au cours du temps. Un système est considéré comme non linéaire si une ou plusieurs fonctions décrivant l'évolution des variables sont non linéaires [27]. Il existe deux types de systèmes chaotiques : les systèmes chaotiques continus (SCC) et les systèmes chaotiques discrets (SCD). Le premier type peut être représenté par des systèmes d'équations différentielles multidimensionnels, tandis que le second est représenté par des applications itératives. Étant donné que les SCC perdent leurs propriétés dynamiques lorsqu'ils sont implémentés sur des machines à précision finie, les SCD suscitent un plus grand intérêt de la part des chercheurs.

4.1 Déterminisme et imprévisibilité

Le déterminisme implique que le système est dépourvu d'aléa et ne comporte aucun paramètre ou entrée de nature stochastique. Chaque condition initiale détermine entièrement l'évolution future du système, car il est dépourvu de hasard, ce qui le rend déterministe. Cependant, même de légères

variations entre deux conditions initiales très proches peuvent engendrer des évolutions totalement différentes. Ainsi, l'évolution du système devient imprévisible, car une petite erreur de mesure ou un arrondi à la 15ème décimale peuvent conduire à des résultats complètement divergents après un certain temps. Ceci est ce que l'on appelle le chaos déterministe [28].

Edward Lorenz, météorologue, fut l'un des premiers à réaliser l'existence du chaos déterministe. En météorologie, cela signifie qu'il est toujours impossible de prédire avec certitude le temps qu'il fera le mois prochain.

4.2 Caractéristiques Fondamentales des Systèmes Chaotiques

Les systèmes dynamiques chaotiques suivent certaines lois particulières des systèmes déterministes non linéaires. Le chaos apparaît lors de l'évolution du système, il a un aspect désordonné qui satisfait certains critères mathématiques. Il existe un ensemble de propriétés qui résument les caractéristiques observées dans les systèmes chaotiques. Les plus appropriés sont :

- Sensibilité à l'état initial : également appelée effet de papillon, où un changement négligeable dans son état initial peuvent générer des états complètement différents.
- Mélange topologique : cela signifie que le système évoluera dans le temps de sorte que toutes les régions d'états soient transformées avec toute autres régions donnée.
- A périodicité : le système évolue sur une orbite qui ne se répète jamais sur lui-même, c'est-à-dire que ces orbites ne sont jamais périodiques.
- Orbites périodiques denses : cela signifie que le système suit une dynamique qui peut approcher arbitrairement de près chaque état asymptotique possible.
- Ergodicité : les mesures statistiques des variables donnent des résultats similaires, qu'elles soient effectuées dans le temps ou dans l'espace.
- Auto-similitude : l'évolution du système, dans le temps ou dans l'espace, montre la même apparence à différentes échelles d'observation. Cette caractéristique fait apparaître le système autorépétitif à différentes échelles d'observation.

5. Exemples de Cartes Systèmes Chaotiques

De nombreux systèmes dynamiques discrets et continus présentent un comportement chaotique. Parmi les exemples les plus étudiés en mathématiques appliquées et en physique, on distingue les cartes itératives (discrètes) et les systèmes d'équations différentielles (continus). Voici quelques exemples emblématiques.

5.1. Carte Logistique :

Plusieurs des exemples les plus classiques du chaos nous viennent de la biologie, et plus spécifiquement de la dynamique des populations en écologie [29], la carte logistique l'une des dynamiques très connues dans la théorie des systèmes non-linéaires et qui définit par l'équation (1.5), elle nous donne une explication parfaite pour un comportement d'un système dynamique :

$$y_{k+1} = r.x_k(1 - x_k) \qquad (1.5)$$

Ce système était développé par le Pr. Pierre François Verhulst (1845) pour mesurer l'évolution de population dans un environnement limité, utilisé plus tard par le biologiste Robert May en 1976 pour l'étude d'évolution de population des insectes ou :

- y_{k+1} : La génération à la venir qui est proportionnel a x_k
- x_k : La génération précédente.
- r : Constante positive incorpore tous les facteurs reliés au reproductif, succès à la survie hivernale des œufs par exemple, etc.

5.2. Carte de Hénon

La carte de Hénon est un système dynamique discret ; elle est l'un des exemples les plus étudiés des systèmes dynamiques qui présentent un comportement chaotique. L'application de la carte de Hénon a été introduite en 1976 par l'astronome français Michel Hénon, comme un modèle simplifié de la **section** de Poincaré du modèle de Lorenz. La carte de Hénon prend un point (x_n, y_n) dans le plan et le transforme en un nouveau point selon les équations suivantes :

$$\begin{cases} x_{k+1} = 1 + y_k - ax_k \\ y_{k+1} = bx_k \end{cases} \qquad (1.6)$$

Où a et b sont les paramètres de contrôle. Il s'agit d'une application non linéaire à deux dimensions, qui peut également être écrite comme une relation de récurrence à deux étapes, puisque la deuxième équation ci-dessus peut être écrite comme $y_k = y_{k-1}$:

$$x_{k+1} = 1 + y_k - ax_k + bx_{k-1} \qquad \mathbf{(1.7)}$$

Pour l'application de Hénon, nous avons deux points fixes. En prenant $(x_{k+1}, y_{k+1}) = (x_k, x_k) = (x_0, y_0)$ dans (1.6) [30], nous obtenons :

$$x_0 = \frac{-(1-b)\pm\sqrt{(1-b^2)4ac}}{2a} \qquad (1.8)$$

Qui peuvent être soit des points attractifs, soit des points selles selon le choix des paramètres (a, b) [30], l'application de Hénon (1.6) peut présenter un comportement chaotique pour (a, b) = (1.4, 0.3) [31]. Une visualisation de l'attracteur de Hénon peut être réalisée par des itérations numériques à partir de conditions initiales arbitraires, par exemple (x_0, y_0) = (0.1,0.1). Les résultats sont présentés dans la Figure.1.

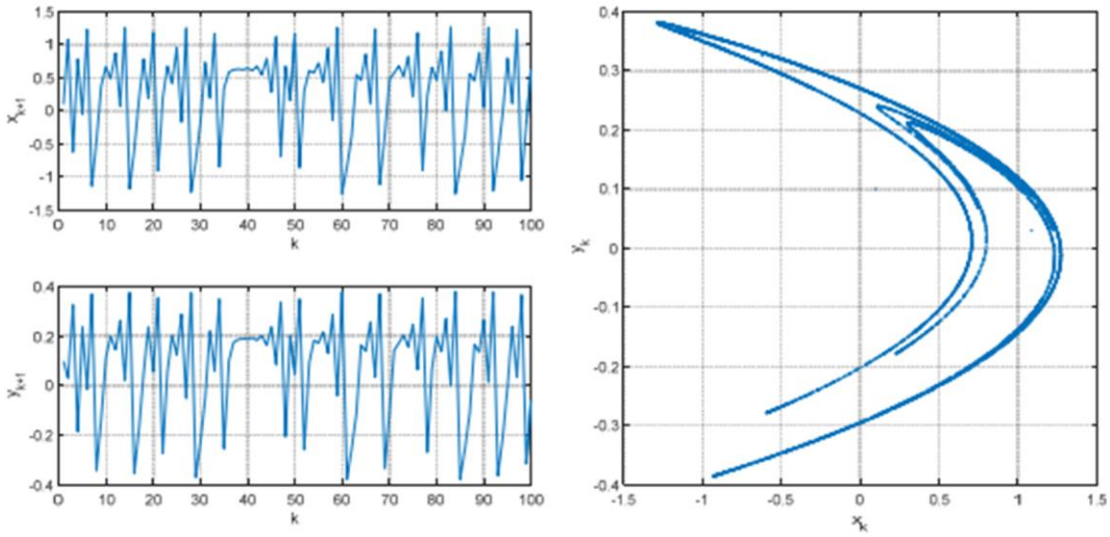

Figure 1 : Différents tracés de l'application de Hénon

5.3. L'attracteur chaotique de Lorenz

Le premier modèle météorologique développé par Edward Lorenz présentait un comportement chaotique, mais il était basé sur un système de 12 équations différentielles non linéaires. Lorenz a alors cherché à observer un comportement complexe dans un système encore plus simple, ce qui l'a conduit à étudier le phénomène de la convection thermique dans un fluide en mouvement. Le modèle physique est simple : on place un gaz dans une boîte rectangulaire solide, avec une source de chaleur placée en bas. Lorenz a simplifié certaines équations de la dynamique des fluides (appelées équations de Navier-Stokes) et a obtenu un système composé de trois équations différentielles non linéaires [32] :

$$\begin{cases} \frac{dx}{dt} = \sigma * (y - x) \\ \frac{dx}{dt} = r * x - y - x * z \\ \frac{dx}{dt} = x * y - \beta * z \end{cases} \quad (1.9)$$

- σ est le nombre de Prandtl, représentant le rapport entre la viscosité du fluide et sa conductivité thermique ;
- r représente la différence de température entre le haut et le bas du système ;
- β est le rapport entre la largeur et la hauteur de la boîte contenant le fluide.

Les valeurs utilisées par Lorenz sont :

σ = 10, ρ = 28, β = 8/3, ces constantes sont également appelées paramètres de contrôle, comme mentionné précédemment .

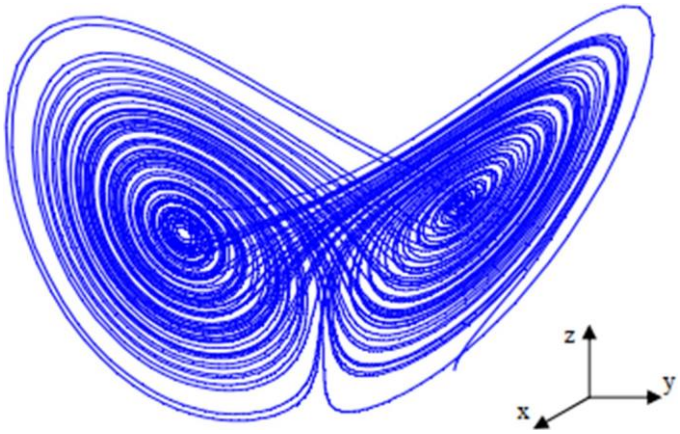

Figure 2 : L'attracteur chaotique de Lorenz.

5.4. La carte Tent (Tent map)

La 'Tent map' est un système chaotique en temps discret, définie sur l'intervalle [0, 1]. Elle est caractérisée par sa structure morceau linéaire, où elle divise l'intervalle en deux segments et applique une transformation linéaire différente sur chaque segment en fonction d'un paramètre μ. Elle est linéaire en morceaux, mais non linéaire dans l'ensemble. La Tent map est définie comme suit :

$$T(x) = \begin{cases} \mu x & si \quad 0 \leq x \leq \frac{1}{2} \\ \mu(1-x) & si \quad \frac{1}{2} \leq x \leq 1 \end{cases} \qquad 1.10)$$

où μ est un paramètre réel positif qui contrôle la pente de la fonction. Elle est utilisée pour modéliser des dynamiques chaotiques simples. Des recherches ont examiné son utilisation dans la génération de clés pour la cryptographie**.**

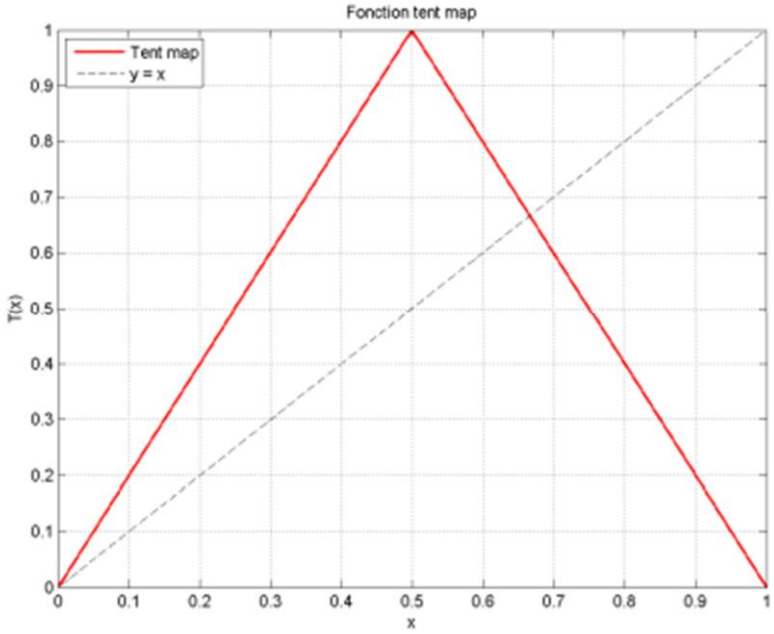

Figure 3 : Tracé de la fonction Tent map.

6. Explication de la différence entre chaos et phénomènes aléatoires

La différenciation entre chaotique et aléatoire nous a paru le point le plus important de la compréhension du chaos. En effet, on a toujours tendance à considérer qu'un phénomène tire son imprédictibilité du nombre trop importants de paramètres en jeu dans sa description, ce qui nous pousse à en donner une approche probabiliste qui, pour être parfaitement satisfaisante, garde par définition une marge d'aléatoire. Le mouvement brownien en est un exemple.

En ce qui concerne le chaos, il n'en est rien. En effet, un phénomène chaotique, comme nous l'avons vu, est décrit de manière déterministe, c'est à dire en particulier avec des outils mathématiques qui en permettent une approche précise et a priori "certaine". En réalité, il faut constater qu'aucun amalgame n'est possible entre chaos et aléatoire puisque même une approche probabiliste de

l'évolution d'un système chaotique n'aboutirait à rien. En effet, même si l'on connaît parfaitement l'évolution d'un système dans des conditions initiales données, pour des conditions initiales extrêmement proches, toutes les évolutions sont encore "équiprobables" : l'approche probabiliste n'apporte rien.

En outre, comme on le verra dans les caractéristiques exposées dans les parties suivantes, les systèmes chaotiques possèdent des propriétés qu'ils ne partagent pas plus avec les systèmes aléatoires qu'avec les systèmes déterministes non-chaotiques.

De manière concrète, il existe une définition rigoureuse qui permet de déterminer mathématiquement qu'un système est chaotique, mais son expression est assez complexe.

On peut dire en toute rigueur que, de manière générale, la part d'imprévisible est en réalité assez faible pour un système probabiliste par rapport à un système chaotique, pour lequel, au contraire, bien que le déterminisme soit total, la prévisibilité est nulle. On constate en particulier, dans l'exemple du mouvement brownien, que le déplacement reste "centré" en *A*. En outre, si on avait initialement placé un autre grain de poussière tout près de *A*, on peut penser que son déplacement aurait été assez semblable à celui de *A*, ce qui ne pourrait arriver dans un système chaotique.

7. Avantages de l'utilisation du chaos en cryptographie

L'intégration des systèmes chaotiques en cryptographie offre plusieurs avantages significatifs, en particulier pour les applications nécessitant à la fois sécurité, performance et légèreté. Parmi les bénéfices les plus notables, on peut citer :

- **La sensibilité élevée aux conditions initiales** : cette propriété permet de générer des clés de chiffrement hautement imprévisibles, ce qui rend les attaques par force brute ou par analyse différentielle extrêmement difficiles.
- **La génération de séquences pseudo-aléatoires** : les systèmes chaotiques produisent des séquences avec un comportement complexe et non répétitif, idéales pour l'encodage de données ou la création de vecteurs d'initialisation dynamiques.
- **La simplicité d'implémentation** : contrairement à certains algorithmes cryptographiques classiques, les modèles chaotiques peuvent être implémentés avec un faible coût computationnel, ce qui les rend adaptés aux systèmes embarqués et aux objets connectés.
- **L'adaptabilité aux données multimédia** : les algorithmes chaotiques sont particulièrement efficaces pour le chiffrement d'images, de vidéos et d'audio en temps réel, grâce à leur rapidité et à leur capacité à traiter de grands volumes de données sans altérer leur qualité.
- **La compatibilité avec les architectures parallèles** : certaines structures chaotiques peuvent

être parallélisées facilement, ce qui améliore les performances de chiffrement sur des plateformes modernes (GPU, FPGA, etc.).

Ces avantages positionnent les systèmes chaotiques comme une alternative crédible et compétitive aux approches traditionnelles, notamment dans les domaines émergents de la cybersécurité.

8. Applications de la cryptographiques basées sur le chaos

Les méthodes cryptographiques basées sur le chaos présentent un fort potentiel pour renforcer la sécurité des systèmes d'information. Leur efficacité repose sur les propriétés fondamentales des systèmes chaotiques : sensibilité aux conditions initiales, imprévisibilité, non-linéarité et comportement pseudo-aléatoire. Ces caractéristiques sont exploitées dans plusieurs approches cryptographiques, parmi lesquelles :

- **La génération de clés chaotiques** : elle repose sur l'utilisation de cartes chaotiques (comme la carte logistique, de Henon ou de Chebyshev) pour produire des séquences numériques complexes et difficilement prévisibles. Ces séquences sont ensuite utilisées comme clés de chiffrement, offrant un espace de clé très large et une forte résistance aux attaques par force brute.
- Le masquage chaotique : utilisé principalement dans les communications analogiques, il consiste à superposer un signal chaotique au message d'origine pour en dissimuler le contenu. La récupération du message nécessite une synchronisation précise entre les systèmes chaotiques de l'émetteur et du récepteur. Cette méthode est particulièrement adaptée aux applications en temps réel.
- Les réseaux de substitution-permutation chaotiques (chaotic SPN) : ils reprennent le schéma classique des chiffrements par blocs (confusion et diffusion), mais en y intégrant des opérations contrôlées par des séquences chaotiques. Ces réseaux permettent d'obtenir des chiffrements dynamiques, résistants aux attaques statistiques, tout en restant adaptés aux environnements à ressources limitées (IoT, systèmes embarqués, etc.).
- Ces méthodes offrent des solutions de chiffrement modernes, efficaces et flexibles, capables de répondre aux défis croissants de la cybersécurité, notamment dans le contexte de la multiplication des objets connectés et des flux de données sensibles.

9. Défis et limitations de la cryptographie basées sur le chaos

Bien que les méthodes cryptographiques basées sur le chaos présentent de nombreux avantages, leur mise en œuvre pratique soulève plusieurs défis techniques et conceptuels, qui limitent parfois leur adoption à grande échelle. Parmi les principales limitations, on peut citer :

- **La précision finie des dispositifs numériques** : les systèmes chaotiques sont très sensibles aux conditions initiales, mais cette propriété peut être altérée par les erreurs d'arrondi et la précision limitée des calculateurs numériques. Cela peut entraîner une perte de la nature chaotique du système lors de l'implémentation, affectant la qualité des séquences générées.

- **Les difficultés de synchronisation** : dans les systèmes utilisant le masquage chaotique, la synchronisation entre l'émetteur et le récepteur est essentielle pour récupérer correctement le message chiffré. En pratique, maintenir une synchronisation parfaite entre deux systèmes chaotiques peut s'avérer complexe, surtout en présence de perturbations ou de bruit.
- **Les défis liés à l'évaluation de la sécurité** : contrairement aux algorithmes cryptographiques classiques, les méthodes chaotiques ne bénéficient pas toujours d'un cadre mathématique formel permettant d'évaluer rigoureusement leur robustesse. Il est souvent difficile de prouver leur résistance face à des attaques cryptanalytiques avancées, ce qui limite leur acceptation dans les standards de sécurité.

  Ces limitations montrent que, bien que prometteuses, les approches chaotiques nécessitent encore des recherches approfondies pour garantir leur fiabilité, leur efficacité et leur sécurité dans des contextes d'application réels.

10. Conclusion

Dans ce chapitre, nous avons présenté une vue d'ensemble des systèmes chaotiques et de leur application en cryptographie. Les systèmes chaotiques trouvent leur origine dans les systèmes dynamiques non linéaires, la non-linéarité étant l'une des conditions fondamentales pour qu'un système soit qualifié de « chaotique ». Il est également essentiel que les paramètres de contrôle soient fixés dans des plages de valeurs bien définies afin de garantir le comportement chaotique du système.

Une des caractéristiques les plus marquantes des systèmes chaotiques réside dans leur sensibilité extrême aux variations infinitésimales des conditions initiales ou des paramètres de contrôle. Cette propriété rend leur comportement difficilement prévisible et alimente un fort intérêt de la part de la communauté scientifique. Les applications des systèmes chaotiques sont nombreuses, notamment dans le domaine de la sécurisation des communications, qui constitue l'objectif principal de notre étude.

Chapitre III : Conception d'un crypto-système à base du Chaos pour le cryptage des images

1. Introduction

Dans un contexte où la sécurité de l'information devient un enjeu majeur, les systèmes chaotiques offrent une alternative prometteuse aux approches cryptographiques classiques. En raison de leurs propriétés intrinsèques telles que la sensibilité aux conditions initiales, l'imprévisibilité et la complexité dynamique, les systèmes chaotiques peuvent être exploités pour concevoir des algorithmes de chiffrement efficaces et robustes, en particulier dans le cadre du chiffrement symétrique par flot.

Ce chapitre s'inscrit dans cette perspective et propose la conception d'un système cryptographique basé sur un système chaotique quadratique. Ce système est utilisé pour générer un flot de clés pseudo-aléatoires à partir de ses paramètres de contrôle, tout en préservant les caractéristiques chaotiques essentielles à la sécurité du chiffrement. Une méthode de génération de clé, adaptée à la structure du système, est proposée afin d'assurer à la fois la complexité et la reproductibilité des séquences chiffrantes.

Pour évaluer le caractère chaotique du système et la qualité de ses séquences, plusieurs critères sont étudiés : la fonction d'autocorrélation, l'exposant de Lyapunov, ainsi que des batteries de tests statistiques reconnues comme NIST SP800-22 et Dieharder. Ces analyses permettent de vérifier la pertinence du système en tant que générateur de clés pour une application cryptographique.

Le système proposé est ensuite appliqué au chiffrement d'images couleur (RGB), démontrant sa capacité à traiter des données complexes et sensibles. Une analyse de sécurité approfondie est présentée, incluant des évaluations de sensibilité, de diffusion et de résistance à diverses attaques.

2. Le système Quadratique chaotique

Le système quadratique chaotique sera utilisé ici comme exemple pour la conception d'un système cryptographique à chiffrement symétrique par flot. Il s'agit d'un système dynamique discret à deux dimensions, défini par des équations polynomiales du second degré, dont les comportements chaotiques dépendent fortement des conditions initiales et des paramètres de contrôle. Il est représenté par le système suivant :

$$\begin{cases} x_{k+1} = a + b.x_k + c.x_k^2 + d.x_k.y_k + e.y_k + f.y_k^2 \\ y_{k+1} = g + h.x_k + j.x_k^2 + k.x_k.y_k + l.y_k + m.y_k^2 \end{cases} \quad (1)$$

Dans ce chapitre, nous exploitons ce système pour générer une clé de chiffrement tout en préservant son caractère chaotique, puis nous l'intégrons dans un schéma de chiffrement par flot adapté au traitement de données sensibles, comme les images numériques.

Le système chaotique Quadratique est implémenté en utilisant une arithmétique en virgule fixe à l'aide de l'outil Vitis Model Composer. Vitis Model Composer est un outil de conception basé sur les modèles, qui facilite l'exploration rapide et le prototypage au sein des environnements MATLAB et Simulink. Il permet une transition simplifiée vers la production sur les dispositifs AMD grâce à la génération automatique de code.

Avec cet outil, il est possible de développer et d'optimiser des algorithmes de traitement du signal (DSP) en utilisant des blocs de haut niveau, performants, tout en vérifiant l'exactitude fonctionnelle via des simulations au niveau système. Vitis Model Composer optimise automatiquement les conceptions pour aboutir à des implémentations prêtes pour la production. L'outil comprend une bibliothèque complète de plus de 200 blocs, couvrant les domaines HDL, HLS et AI Engine. De plus, il offre la flexibilité d'intégrer du code personnalisé (HDL, HLS ou AI Engine) sous forme de blocs définis par l'utilisateur dans les conceptions [33].

La Figure.1 illustre l'implémentation sous Simulink/Model Composer du système chaotique quadratique. Il s'agit d'une traduction fidèle du système d'équations (1) en modèle graphique, permettant une simulation et une validation numériques du comportement dynamique.

Pour obtenir un comportement chaotique, les paramètres du système sont fixés aux valeurs suivantes :

- $a = -1.2, b = -0.6, c = -0.5, d = 0.1, e = -0.7, f = 0.2.$
- $g = -0.9, h = 0.9, j = 0.1, k = -0.3, l = -1.0, m = 0.3.$

Avec les conditions initiales $(x_0, y_0) = (0.1, 0.1)$, ce choix de paramètres induit une dynamique chaotique, caractérisée par une sensibilité extrême aux conditions initiales et une évolution imprévisible des trajectoires. Ce comportement est illustré par la Figure.2, qui montre l'attracteur étrange du système ainsi que son entropie élevée, deux propriétés essentielles pour

une application cryptographique robuste.

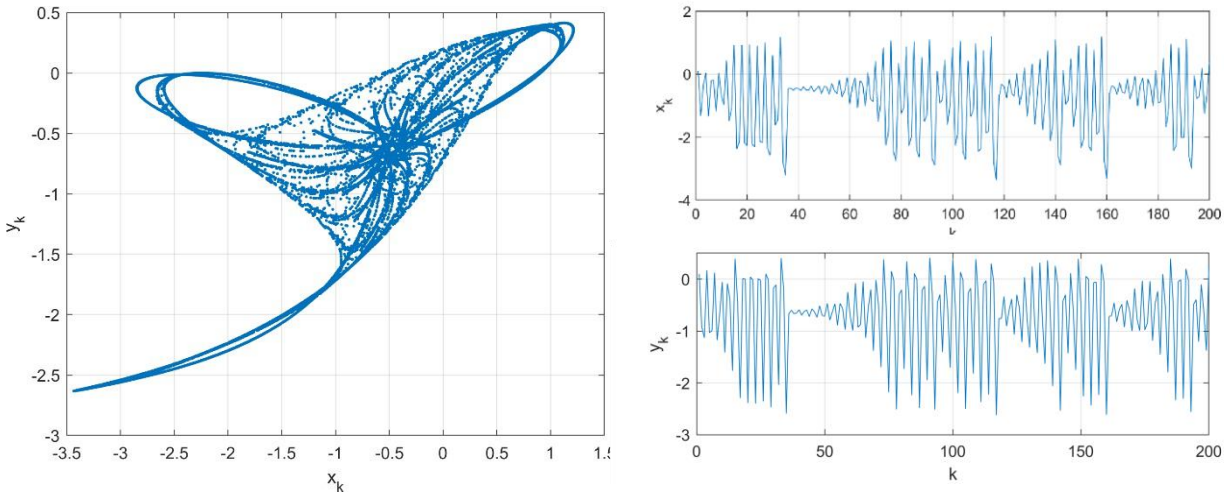

Figure 1 : Espace des phases et séries temporelles du chaotique Quadratique.

Les résultats simulés du système quadratique chaotique présentent des trajectoires erratiques pour les variables x et y, oscillant de manière imprévisible entre des valeurs positives et négatives ($x_k \in$ [-3.5, 1.4], ($x_k \in$ [-3, 1]). Cette dynamique complexe, combinée à la sensibilité apparente aux conditions initiales, suggère un comportement chaotique prometteur pour des applications cryptographiques. Bien que ces observations visuelles soient encourageantes, une validation quantitative rigoureuse reste nécessaire - incluant le calcul des exposants de Lyapunov et des tests statistiques (NIST, autocorrélation) - pour confirmer que ces signaux satisfont aux exigences cryptographiques (imprévisibilité, uniformité statistique).

2.1. Evaluation de comportement chaotique du system Quadratique

L'observation visuelle de l'attracteur étrange et des séries temporelles présentées précédemment suggère un comportement chaotique prometteur du système quadratique. Cependant, une validation rigoureuse et quantitative de ce comportement est indispensable pour garantir la robustesse cryptographique du système proposé.

L'efficacité d'un système chaotique dans un contexte cryptographique repose en grande partie sur la qualité de son comportement dynamique. En particulier, les propriétés telles que l'imprévisibilité, la sensibilité aux conditions initiales et la complexité des trajectoires générées doivent être préservées même après l'implémentation numérique du système. Dans notre cas, le

système quadratique chaotique a été implémenté en virgule fixe à l'aide de Vitis Model Composer, ce qui soulève la question de l'impact de la précision numérique sur ses propriétés chaotiques.

Cette section a pour objectif d'évaluer le comportement chaotique du système quadratique 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, notamment la fonction d'autocorrélation, l'exposant de Lyapunov, et des 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.

2.1.1. La fonction d'autocorrélation

La fonction d'autocorrélation est un outil mathématique essentiel pour l'analyse des séquences temporelles, notamment dans l'évaluation de leur caractère aléatoire. Elle mesure le degré de ressemblance entre une séquence et une version décalée d'elle-même, en fonction du décalage (ou "lag"). Dans le cadre de la cryptographie basée sur le chaos, cette fonction permet d'analyser la prévisibilité et la structure interne des séquences pseudo-aléatoires générées par un système dynamique.

Idéalement, une séquence destinée à des applications cryptographiques doit présenter une fonction d'autocorrélation qui est très faible (voire nulle) pour tous les décalages non nuls. Cela garantit l'absence de motifs réguliers ou de corrélations internes pouvant compromettre la sécurité du système. Un pic unique au décalage nul est attendu, tandis que les autres valeurs doivent se rapprocher du bruit blanc.

Dans cette étude, nous évaluons la fonction d'autocorrélation des séquences issues du système quadratique chaotique implémenté en virgule fixe, en faisant varier la précision utilisée : 16 bits, 24 bits, 32 bits et 48 bits. Cette comparaison a pour objectif de déterminer dans quelle mesure la précision numérique influence la qualité aléatoire des séquences produites. En effet, une précision insuffisante peut induire une dégradation du comportement chaotique, menant à des cycles courts, à une perte d'imprévisibilité, voire à une convergence prématurée du système. Inversement, des précisions plus élevées devraient mieux préserver la complexité dynamique du système. L'analyse des résultats obtenus via la fonction d'autocorrélation permettra donc de

juger de l'effet de la quantification numérique sur la qualité des clés générées, et d'orienter le choix d'une précision optimale pour concilier complexité, performance matérielle et sécurité cryptographique. La Figure.2 présente les résultats obtenus :

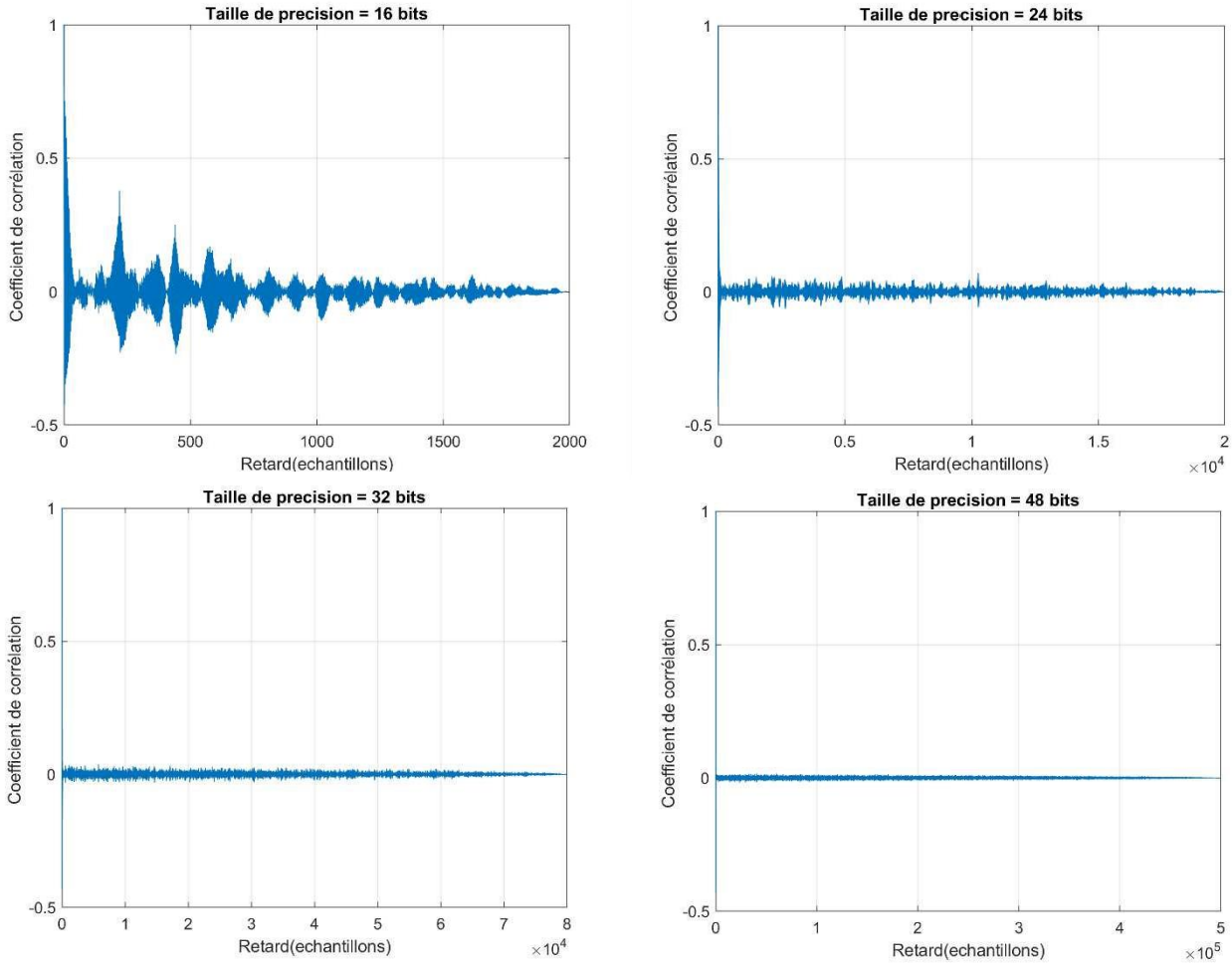

Figure 2 : Analyse de comportement de système chaotique Quadratique en utilisant la fonction d'autocorrélation.

La figure ci-dessus illustre l'évolution du coefficient d'autocorrélation des séquences générées par le système quadratique chaotique, pour différentes tailles de précision (16, 24, 32 et 48 bits). Cette analyse permet d'évaluer l'effet de la quantification sur le comportement pseudo-aléatoire du système.

- **Précision 16 bits** : À faible précision, le système présente des coefficients d'autocorrélation relativement élevés pour plusieurs valeurs de retard. On observe des pics réguliers qui révèlent une forte corrélation à court terme, conséquence directe d'un effet

de quantification important.

- Une périodicité claire apparaît dès l'échantillon **220**, traduisant une perte rapide du caractère chaotique du système.
- Ce comportement montre que la dynamique est fortement dégradée à cette précision, menant à l'apparition de cycles courts et à une perte de l'imprévisibilité essentielle à la sécurité cryptographique.

- **Précision 24 bits** : À 24 bits, l'autocorrélation diminue nettement, bien que l'on puisse encore détecter certaines irrégularités. Le comportement chaotique est partiellement préservé, mais le système reste vulnérable à une dynamique finie.
  - Des périodicités sont détectées à partir de l'échantillon **46485**, indiquant une amélioration significative, mais encore limitée pour des applications sécurisées exigeantes.
- **Précision 32 bits** : La courbe d'autocorrélation présente une structure proche de celle d'un bruit blanc : les coefficients sont proches de zéro, à l'exception du pic initial. Cela reflète une quasi-absence de corrélation temporelle, preuve d'un comportement pseudo-aléatoire riche et non cyclique.
  - Les premières périodicités n'apparaissent qu'à partir de l'échantillon **132970**, ce qui démontre une dynamique chaotique robuste, compatible avec les exigences de la cryptographie.
- **Précision 40 bits** : Le comportement observé ici est le plus proche d'un processus parfaitement aléatoire : la fonction d'autocorrélation reste nulle (hors pic initial) sur l'ensemble de la séquence analysée.
  - Aucune périodicité détectée sur une séquence de 23 774 851 échantillons, confirmant un comportement pleinement chaotique et non cyclique.
  - Cela démontre que l'utilisation de 48 bits permet de préserver intégralement la dynamique chaotique du système, ce qui est idéal pour un générateur de clés à haute sécurité.

Il est important de noter que l'augmentation de la taille de précision a un impact positif direct sur la qualité aléatoire des séquences, en prolongeant la période, en réduisant les corrélations, et en améliorant la complexité dynamique du système. Cependant, cet avantage s'accompagne d'un coût matériel croissant :

- Plus la précision est élevée, plus les ressources FPGA consommées sont importantes

(LUTs, registres, DSP).

- Le temps de latence et la fréquence d'horloge peuvent être affectés négativement.
- La consommation énergétique augmente également.

Il est donc nécessaire de trouver un compromis optimal entre la sécurité (qualité pseudo-aléatoire) et la performance matérielle, notamment dans les applications embarquées.

2.1.2. Analyse par le diagramme de bifurcation

Le diagramme de bifurcation est un outil fondamental pour l'analyse des systèmes dynamiques, permettant de visualiser l'évolution qualitative du comportement d'un système en fonction d'un paramètre de contrôle. En représentant les valeurs asymptotiques d'une variable du système pour différentes valeurs d'un paramètre, ce diagramme fait apparaître les transitions entre les régimes dynamiques : points fixes, périodicité et chaos [34].

Dans le domaine de la cryptographie chaotique, cette analyse est essentielle pour identifier les plages de paramètres — qui seront ici exploitées comme clés — générant un comportement véritablement chaotique. Un crypto-système basé sur le chaos doit garantir que les clés issues des paramètres de contrôle conduisent à des productions de séquences imprévisibles, complexes et sensibles aux conditions initiales, sans zones de périodicité exploitables.

Dans cette section, nous analysons le diagramme de bifurcation du système quadratique chaotique en utilisant exclusivement une implémentation en virgule fixe 32 bits. L'objectif est d'identifier précisément les intervalles de paramètres de contrôle où le système reste dans un régime chaotique, garantissant ainsi que toute clé définie dans ces zones produira un comportement dynamique riche et sécurisé malgré la quantification numérique.

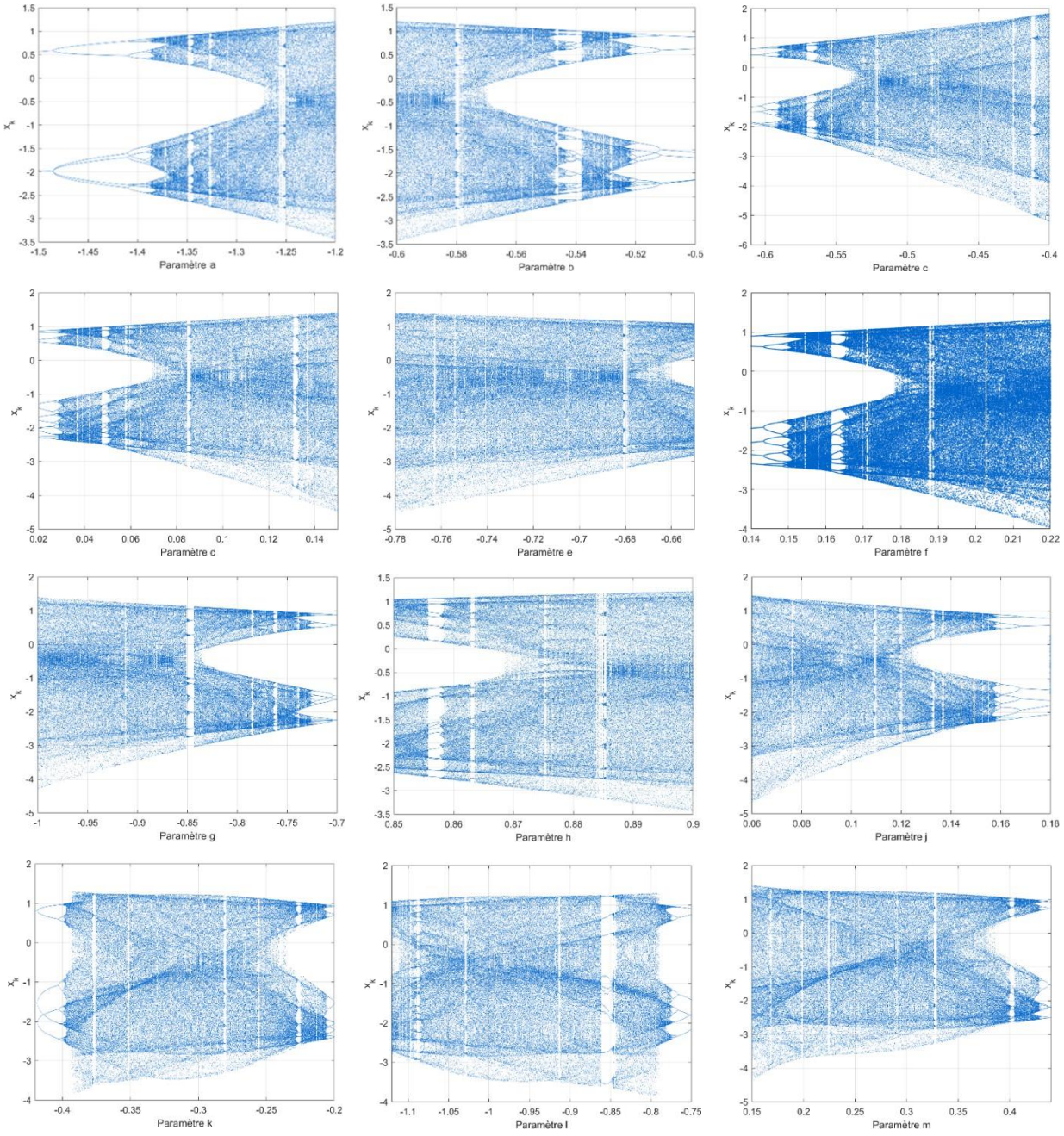

Figure 3 : Diagrammes de bifurcation de système chaotique Quadratique.

D'après la Figure.3 on peut conclure que les diagrammes de bifurcation obtenus pour le système quadratique original (en virgule fixe 32 bits) montrent que tous les paramètres de contrôle peuvent conduire à un comportement chaotique, mais uniquement dans des plages très restreintes.

Dans le cadre de la cryptographie, où les paramètres du système servent directement à générer les clés, cette limitation est critique : une petite variation peut facilement faire sortir le système du régime chaotique, compromettant la qualité aléatoire et la sécurité des séquences générées. Ainsi, malgré la présence de zones chaotiques, le système quadratique dans sa forme actuelle présente une

vulnérabilité structurelle, en raison de la faible étendue des intervalles chaotiques et de leur instabilité.

Ces résultats soulignent la nécessité de proposer, dans la suite de ce travail, des améliorations au système — notamment des mécanismes de perturbation — afin d'étendre et stabiliser les zones chaotiques, renforçant ainsi la fiabilité et l'efficacité du générateur de clés.

2.1.3. 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 [35]. 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 [36]. 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 quadratique chaotique, 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 quadratique, générée pour différentes tailles de précision fixe (16, 24, 32 et 40 bits). Les résultats obtenus sont présentés dans le Tableau.1, 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**	**Passed**	**Passed**
Rank	**Passed**	**Passed**	**Passed**	**Passed**
Spectral DFT	**Failed**	**Failed**	**Failed**	**Passed**
Non-Overlapping Template (m = 9)	**Failed**	**Passed**	**Passed**	**Passed**
Overlapping Template (m = 9)	**Failed**	**Failed**	**Failed**	**Failed**
Universal	**Failed**	**Passed**	**Passed**	**Passed**
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)	**Passed**	**Passed**	**Passed**	**Passed**
Serial (m = 16, WT_m^2)	**Failed**	**Passed**	**Passed**	**Passed**
	13,3 %	**33,3 %**	**40 %**	**46,6 %**

Tableau 1 : Résultats des tests NIST SP 800-22 appliqués aux sorties binaires du système quadratique chaotique pour différentes précisions numériques

D'après le tableau ci-dessus, on peut conclure que l'évaluation du système chaotique quadratique à l'aide de la suite NIST SP 800-22 met en évidence une forte dépendance entre la qualité aléatoire des séquences produites et la précision numérique utilisée :

- À 16 bits, seuls 2 tests sur 15 ont été validés, soit un taux de réussite de 13,3 %. Cela reflète un comportement largement prévisible, inadapté à la cryptographie.
- À 24 bits, seulement 5 tests sur 15 sont réussis (soit 33,3 % de réussite),
- À 32 bits, 6 tests sur 15 ont été validés, soit un taux de réussite de 40 %, traduisant une amélioration significative du comportement pseudo-aléatoire.
- À 40 bits, 7 tests sur 15 sont passés, portant le taux de réussite à 46,6 %. Ce progrès souligne l'effet bénéfique de la précision accrue sur l'entropie et la dispersion des séquences générées.

Cependant, plusieurs tests majeurs tels que *Frequency*, *Runs*, *Approximate Entropy* ou *Overlapping Template* échouent pour toutes les précisions testées. Ces échecs récurrents traduisent l'existence de régularités structurelles non négligeables dans les séquences, compromettant leur caractère aléatoire du point de vue cryptographique.

On peut conclure que bien que l'augmentation de la précision améliore le comportement chaotique observé statistiquement, le système quadratique présente encore des vulnérabilités importantes, notamment en raison de la quantification en virgule fixe. Ces limitations confirment la nécessité de proposer des mécanismes de renforcement afin d'assurer une meilleure conformité aux standards de sécurité aléatoire.

3. Le Mécanisme Proposé pour améliorer la dynamique de système chaotique

Malgré les propriétés intéressantes du système quadratique chaotique, les analyses précédentes ont mis en évidence certaines limitations liées à la quantification numérique et à la restriction des plages de paramètres chaotiques, réduisant son efficacité en tant que générateur de clés.

Dans cette section, nous proposons un mécanisme d'amélioration visant à étendre la dynamique chaotique, à renforcer la sensibilité aux paramètres et à améliorer la qualité aléatoire des séquences produites. Cette amélioration constitue une étape essentielle pour renforcer la sécurité et la robustesse du crypto-système basé sur ce système chaotique.

Le schéma de base du MP (mécanisme proposé) est représenté sur la Figure.4. Le schéma représente un générateur chaotique qui produit deux vecteurs d'état binaires, $x_k$et y_k, chacun de longueur N bits avec le MP. Le MP est constitué de :

- **Un bloc tranchage (Slice)** : Chaque vecteur x_k et 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 deux 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.

Ce mécanisme permet d'améliorer considérablement la qualité aléatoire du système quadratique original, notamment en atténuant certaines régularités ou structures indésirables dues aux limitations arithmétiques. Cette amélioration est justifiée par les évaluations expérimentales du nouveau système modifié, qui révèlent une progression significative des indicateurs statistiques : augmentation de l'entropie, baisse de l'autocorrélation, allongement des longueurs de cycles, ainsi qu'un meilleur taux de réussite aux batteries de tests NIST.

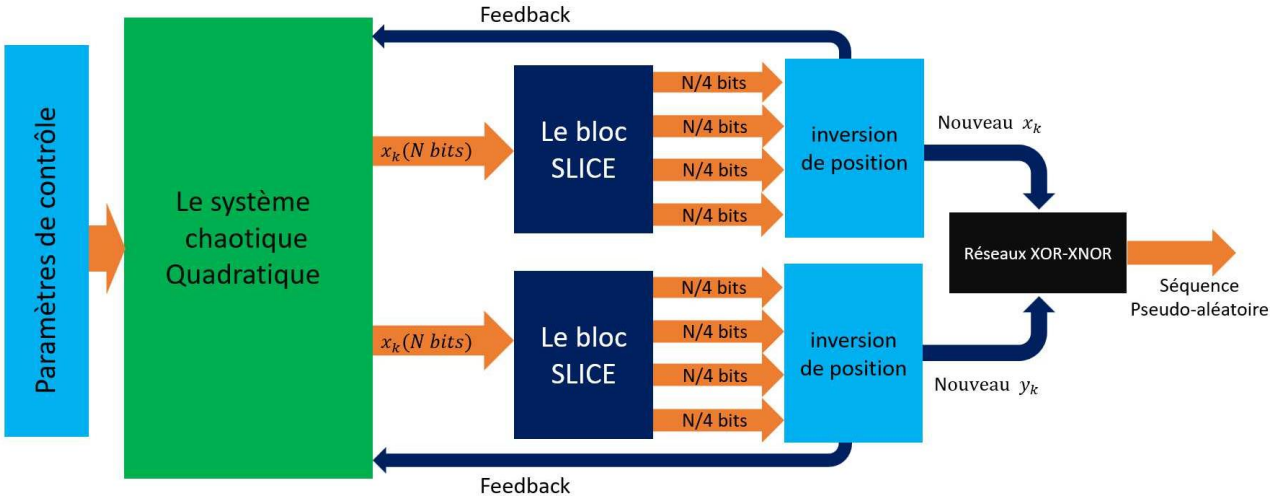

Figure 4 : Architecture fonctionnelle de mécanisme proposé.

4. Évaluation du 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. Cette analyse vise à mesurer l'impact du schéma de perturbation — basé sur le découpage, l'inversion et la combinaison XOR–XNOR — sur la richesse du comportement

chaotique, la qualité aléatoire des séquences générées, ainsi que sur la robustesse globale du générateur.

Les résultats obtenus permettront de déterminer si le mécanisme améliore réellement la diversité des états internes et étend les plages de paramètres conduisant à un régime chaotique exploitable pour la cryptographie.

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.5.

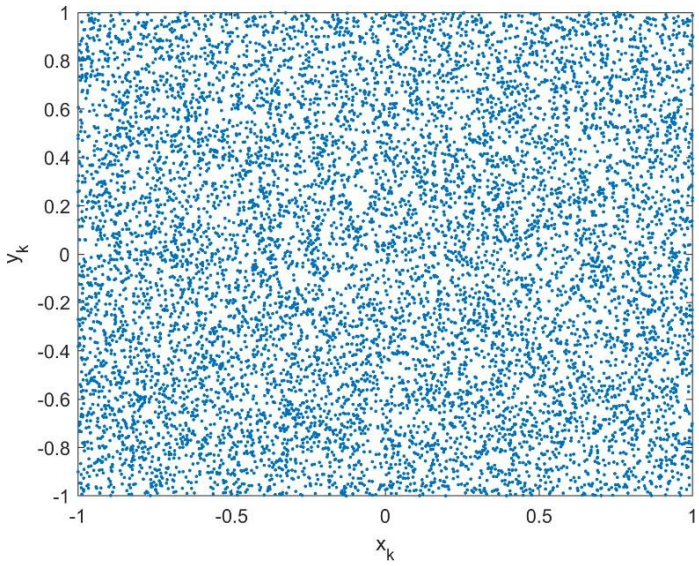

Figure 5 : L'espace de phase du système Quadratique modifié.

La figure ci-dessus montre le nouvel espace de phase du système quadratique après l'intégration du mécanisme proposé (MP). Contrairement à un attracteur classique resserré ou périodique, on observe désormais :

- Une répartition dense et homogène des points dans la zone $[-1,1]^2$, indiquant une couverture quasi uniforme du plan de phase.
- Absence de structures périodiques visibles, comme des cycles fermés ou des zones creuses : ce qui suggère une montée en ergodicité et une dynamique plus riche.

- Un attracteur "bien rempli", typique d'une dynamique chaotique forte, condition souhaitée pour renforcer la diffusion et la complexité du flux de clés

4.2. Longueur de cycle de la séquence générées

Comme déjà discuté, la longueur de cycle (période) d'un générateur chaotique est cruciale en cryptographie : plus la période est longue, plus l'usage d'un cycle trop court est impossible, préservant l'imprévisibilité du flux de clés. Après insertion du mécanisme proposé (MP), les longueurs de cycle observées sont :

- 16 bits : cycle = 641 782 (contre ~220 initialement).
- 24 bits : cycle ≈ 58 931 275 (contre ~46 485 initialement).
- 32 bits : non détecté durant la simulation (contre ~132 976 initialement).

Ces résultats démontrent clairement que le MP allonge considérablement la durée avant répétition, surtout à faible précision.

4.3. Analyse statistique

Dans le but d'évaluer rigoureusement l'amélioration apportée par le mécanisme de perturbation (MP) introduit dans notre système chaotique quadratique, nous avons réalisé une analyse statistique approfondie des séquences générées après modification. Rappelons que le système original a déjà été soumis à la batterie de tests NIST SP 800-22, et qu'il n'a satisfait que partiellement aux critères d'aléa requis.

Dans cette section, nous présentons donc les résultats obtenus pour le système modifié, en considérant plusieurs précisions numériques (16, 24 et 32 bits). L'objectif est de démontrer que l'introduction du MP permet d'améliorer significativement les propriétés statistiques du générateur, en le rendant plus apte à la cryptographie. Le tableau suivant résume les valeurs de *p* obtenues pour chaque test, que nous interprétons dans la suite.

Test	**Précision**		
	16	**24**	**32**
Frequency	**0.83366**	**0.28823**	**0.40203**
Block Freq (m = 128)	**0.79268**	**0.40292**	**0.80404**
Cumulative-Forward	**0.87425**	**0.48072**	**0.45275**
Cumulative -Reverse	**0.68483**	**0.28581**	**0.40203**
Runs	**Failed**	**0.12087**	**0.05014**
Long Runs of Ones	**0.35456**	**0.01765**	**0.03889**
Rank	**0.84591**	**0.46000**	**0.45503**
Spectral DFT	**Failed**	**Failed**	**0.61375**
Non-Overlapping Template (m = 9)	**0.77865**	**0.84251**	**0.97615**
Overlapping Template (m = 9)	**0.05003**	**0.13537**	**0.87734**
Universal	**0.09680**	**0.86091**	**0.47589**
Approximate Entropy (m = 10)	**Failed**	**0.05685**	**0.32627**
Random Excursion (x = +1)	**Failed**	**0.61417**	**0.50371**
Random Excursion Var (x = -1)	**Failed**	**0.75663**	**0.98533**
Linear Comp (M = 500)	**0.64174**	**0.10479**	**0.35279**
Serial (m = 16, WT_m^2**)**	**Failed**	**0.19375**	**0.70544**
	62.5 %	**93.75 %**	**100 %**

Tableau 2 : Résultats des tests NIST SP 800-22 appliqués aux sorties binaires du système Quadratique chaotique modifié par le MP pour différentes précisions.

Le tableau ci-dessus présente les résultats de la suite NIST SP 800-22 appliquée aux séquences générées avec le système modifié, pour différentes précisions numériques (16, 24 et 32 bits) :

- À 16 bits, 62,5 % des tests ont été validés, ce qui marque une amélioration par rapport au système original mais reste partiellement insuffisant pour des applications hautement sécurisées.
- À 24 bits, le taux de réussite atteint 93,75 %, traduisant une structure pseudo-aléatoire nettement plus solide et adaptée à un usage cryptographique.
- À 32 bits, les séquences passent 100 % des tests, ce qui confirme la robustesse statistique du générateur et la qualité du mécanisme de perturbation proposé.

Ces résultats montrent que l'augmentation de la précision, combinée à la structure introduite

par le mécanisme de perturbation, permet d'atteindre une qualité de génération conforme aux standards de sécurité.

4.4. Evaluation de complexité en utilisant l'Exposant de Lyaponov

Dans le cadre de l'évaluation dynamique du système chaotique modifié, l'exposant de Lyapunov constitue un indicateur fondamental. Il mesure la sensibilité aux conditions initiales — caractéristique essentielle du chaos. Plus précisément, un plus grand exposant de Lyapunov (Largest Lyapnov Exponent - LE) positif indique une divergence exponentielle entre trajectoires initialement proches, traduisant un comportement chaotique intense. Cette sous-section examine comment le mécanisme proposé influence cet exposant, et dans quelle mesure il améliore la dynamique instable du système, condition favorable pour un chiffrement robuste.

Dans notre étude, ce test a été réalisé sur 25 cas distincts, en utilisant des ensembles de paramètres de contrôle choisis arbitrairement dans l'intervalle [0, 1]. Cette approche permet d'évaluer la robustesse du système sur une large variété de conditions et de confirmer la stabilité chaotique induite par le mécanisme proposé. Le résultat obtenu est présenté sur la Figure.6.

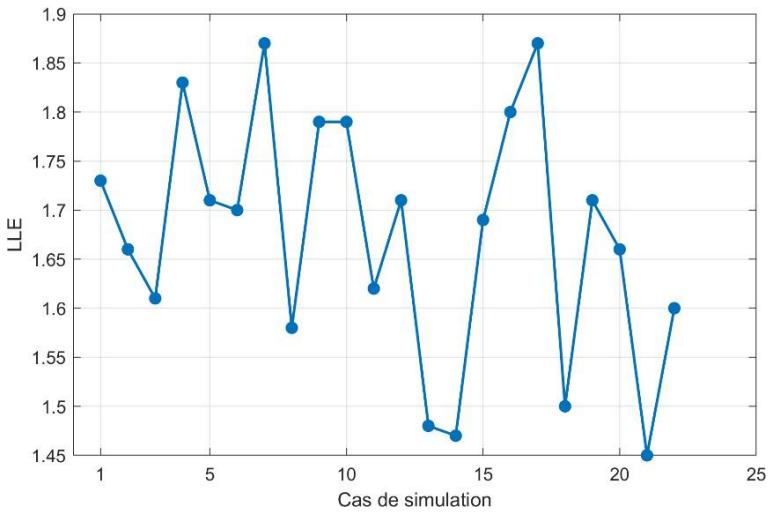

Figure 6 : Evolution de LLE en fonction des paramètres de control.

D'après la figure ci-dessus, on peut conclure que le résultat obtenu montre que les valeurs du plus grand exposant de Lyapunov (LLE) varient entre environ 1.45 et 1.88 selon les cas simulés. Cette plage confirme une dynamique fortement chaotique, caractérisée par une divergence exponentielle entre trajectoires initialement proches. Ces valeurs élevées du LLE indiquent que le système reste hautement sensible aux conditions initiales, une propriété clé pour garantir l'imprévisibilité dans un contexte cryptographique.

On observe en particulier que la majorité des cas étudiés présentent un LLE supérieur à **1.6**, traduisant une bonne robustesse du comportement chaotique, même sous différentes configurations de paramètres. Cette dispersion contrôlée mais soutenue dans les valeurs du LLE traduit également la richesse dynamique du système perturbé.

Ces résultats confirment que, malgré les modifications introduites par le mécanisme de perturbation, le système conserve un comportement **fortement non linéaire et instable,** favorable à une génération efficace de séquences pseudo-aléatoires.

4.5. Diagrammes de Bifurcation de système Quadratique modifié

Dans cette sous-section, nous analysons l'évolution dynamique du système quadratique après l'intégration du mécanisme de perturbation (MP) à travers l'étude de ses diagrammes de bifurcation (Figure.7). Ces derniers permettent d'évaluer la stabilité et l'extension des régimes chaotiques en fonction des paramètres de contrôle. Cette analyse visuelle est essentielle pour apprécier les améliorations introduites par le MP, notamment en termes de robustesse et de richesse du comportement chaotique sur des plages paramétriques élargies.

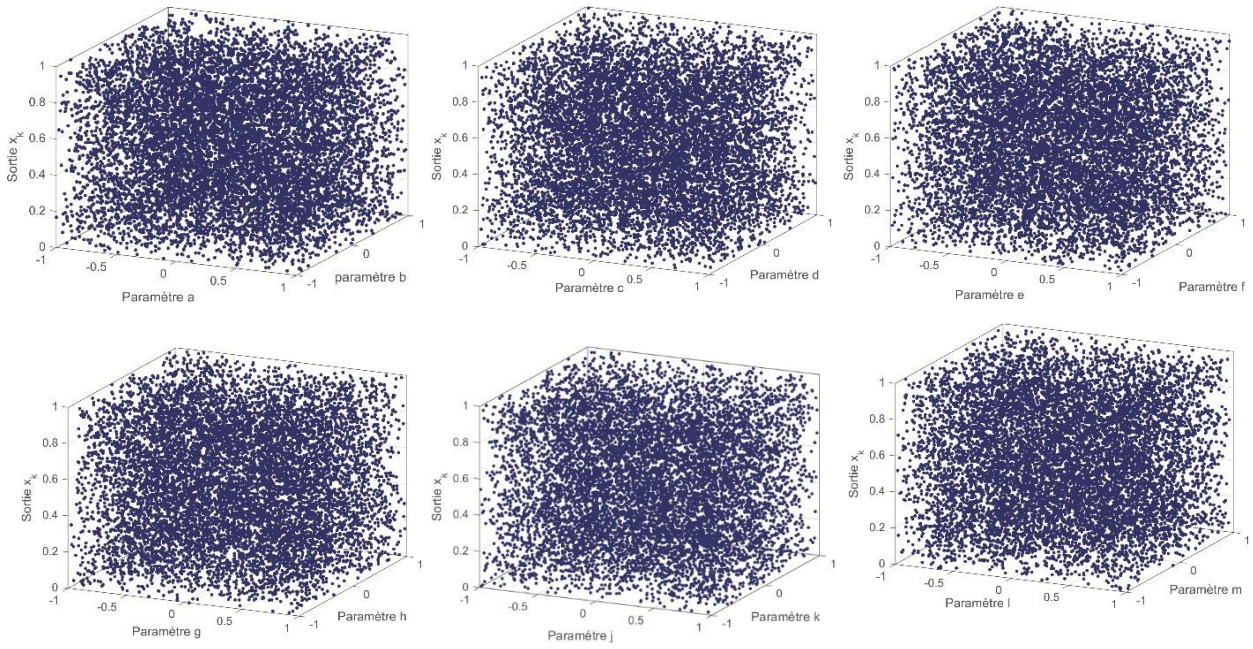

Figure 7 : Diagrammes de bifurcation du système Quadratique modifié.

La figure ci-dessous présente les diagrammes de bifurcation 3D du système modifié, simulés en virgule fixe 32 bits, en fonction de différentes paires de paramètres : (a, b), (c, d), (e, f), (g, h), (j, k) et (l, m).

Contrairement au système original, où les zones chaotiques étaient limitées à des plages très restreintes de paramètres, ces nouveaux diagrammes montrent une distribution dense et étendue des valeurs de sortie x_k sur l'intervalle [0,1]. Cette densité, observée dans presque toutes les configurations de paramètres, suggère que :

- Le comportement chaotique est désormais atteint sur une plage beaucoup plus large des paramètres.
- Le système est globalement très sensible aux petites variations des paramètres.
- Les sorties x_k présentent une meilleure répartition, renforçant leur qualité pseudo-aléatoire.

Les paramètres de contrôle ne sont pas simplement utilisés pour ajuster le comportement du système, mais serviraient directement à construire les clés cryptographiques. Ainsi, la sécurité repose sur la difficulté à retrouver ou prédire ces paramètres à partir des sorties.

Le système modifié présente ici un avantage significatif : l'élargissement des plages chaotiques augmente le nombre de configurations valides pour les clés. Cela permet d'exploiter un espace de clés beaucoup plus vaste, ce qui est fondamental en cryptographie pour empêcher les attaques par force brute.

Ces résultats confirment que les modifications apportées au système quadratique ne se limitent pas à une amélioration dynamique : elles augmentent aussi la robustesse cryptographique du système. En rendant plus accessible le régime chaotique et en permettant une plus grande diversité de clés valides, ce système devient un candidat sérieux pour des générateurs de clés pseudo-aléatoires sécurisés dans les applications cryptographiques modernes.

5. Processus de Cryptage d'une image

Une image numérique est une représentation discrète d'une scène visuelle, composée d'un ensemble fini de pixels organisés en lignes et en colonnes. Chaque pixel contient des informations de couleur ou de luminance, généralement codées sur plusieurs bits. Dans les images en niveaux de gris, chaque pixel est défini par une seule valeur d'intensité, tandis que dans les images couleur (par exemple RVB), chaque pixel est représenté par trois composantes (Rouge, Vert, Bleu), chacune codée sur 8 bits.

Grâce à cette structure binaire, les images numériques peuvent être facilement manipulées par des algorithmes, ce qui les rend vulnérables à l'analyse, à la copie ou à l'altération. D'où l'importance de concevoir des mécanismes de chiffrement efficaces pour garantir la confidentialité et l'intégrité de ces données visuelles, notamment dans des contextes sensibles comme les télécommunications, la

vidéosurveillance ou la médecine.

La Figure.8 présente le crypto-système proposé. Comme mentionné précédemment, le système cryptographique proposé repose sur un schéma de chiffrement par flot, dans lequel une séquence pseudo-aléatoire est générée à l'aide du système chaotique perturbé. Cette séquence agit comme un flux de clés qui sera combiné bit à bit avec les données de l'image.

Concrètement, les bits de chaque pixel de l'image sont mélangés avec les bits correspondants du flux chaotique à l'aide d'une opération XOR. Ce mécanisme garantit que le moindre changement dans la clé ou dans l'image d'entrée produit une sortie totalement différente, renforçant ainsi la sécurité contre les attaques statistiques et différentielle.

Comme présenté dans le premier chapitre, deux propriétés fondamentales doivent être assurées dans tout système de chiffrement sécurisé : la confusion et la diffusion, telles que formulées par Claude Shannon :

- La confusion vise à rendre la relation entre la clé et le texte chiffré aussi complexe que possible, afin de masquer toute structure exploitable. Dans notre système, elle est obtenue grâce à la sensibilité extrême du générateur chaotique aux conditions initiales et aux paramètres, rendant le flux de clés hautement imprévisible.
- La diffusion, quant à elle, consiste à propager l'influence de chaque bit de l'image claire sur de nombreux bits de l'image chiffrée. Cela permet d'éliminer les redondances et les structures perceptibles dans l'image originale. Dans notre système, cette propriété est assurée par un processus reposant sur un principe essentiel : chaque pixel de l'image claire est non seulement mélangé avec la séquence pseudo-aléatoire générée, mais également influencé directement par les paramètres de contrôle du système chaotique. Cette double dépendance renforce la complexité du chiffrement et contribue à une dispersion plus efficace de l'information dans l'image chiffrée.

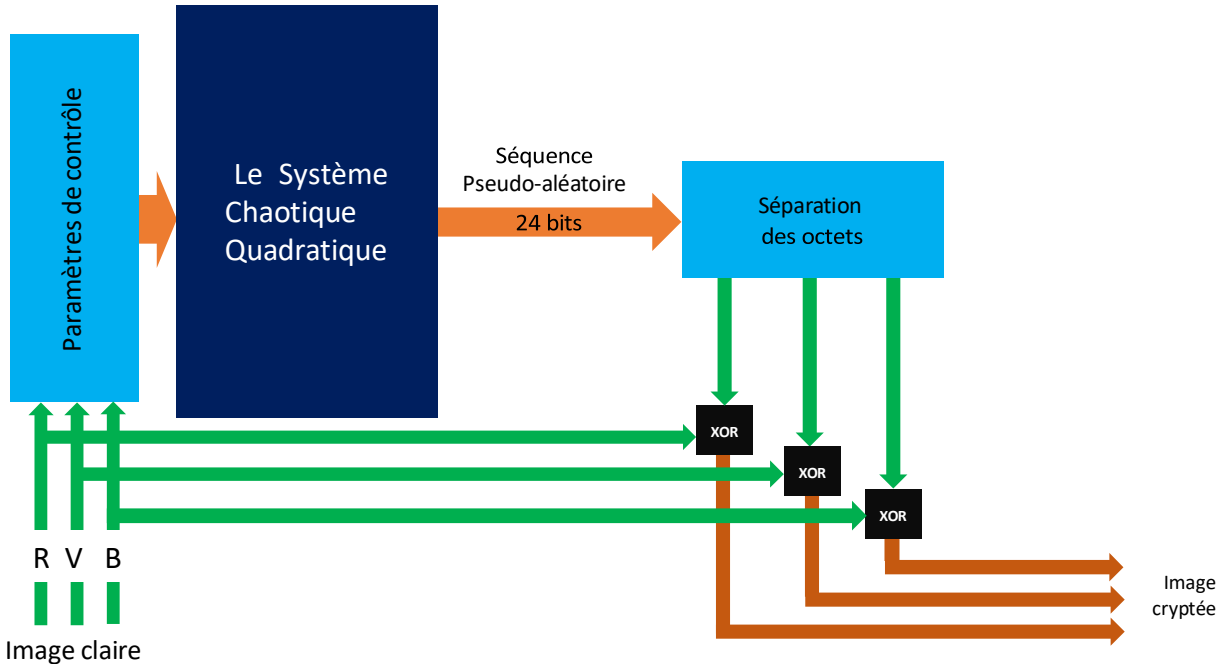

Figure 8 : Le schéma synoptique du mécanisme de chiffrement proposé.

La figure ci-dessus illustre le mécanisme de chiffrement proposé, intégrant la diffusion par un couplage étroit entre les données de l'image et les paramètres du système chaotique quadratique. Chaque pixel de l'image (composé des composantes R, V, B) est injecté, avec les paramètres de contrôle, dans le système chaotique. Ce dernier génère une séquence pseudo-aléatoire de 24 bits, ensuite décomposée en trois octets distincts. Ces octets sont combinés avec les canaux couleur de l'image claire à l'aide d'opérations XOR, assurant une transformation non linéaire des données d'origine.

Dans ce processus, trois paramètres de contrôle sont choisis arbitrairement pour être influencés dynamiquement par le message clair. Plus précisément, les 8 bits de poids faible (LSB) de chacun de ces paramètres sont combinés par l'opérateur logique XOR avec des bits extraits de l'image claire. Ce mécanisme introduit une dépendance directe entre le contenu de l'image et la clé de chiffrement, renforçant à la fois la diffusion et la sensibilité aux modifications minimales de l'image d'entrée.

Ce procédé garantit que chaque pixel chiffré dépend simultanément de l'image originale et des paramètres chaotiques. La boucle de rétroaction implicite via l'ajustement des paramètres accentue encore cette dynamique, rendant le système hautement résistant à toute tentative d'analyse statistique ou différentielle. L'opération de décryptage dans le système proposé s'effectue selon le principe de

symétrie inhérent aux chiffrements par flot. Elle repose sur l'utilisation de la même séquence pseudo-aléatoire que celle utilisée lors du chiffrement, générée à partir des mêmes conditions initiales et paramètres de contrôle du système chaotique. Dans notre implémentation, les paramètres de contrôle sont effectivement modifiés à chaque itération durant le chiffrement à travers les 8 bits de poids faible (LSB) extraits des pixels de l'image claire. Lors du décryptage, cette même stratégie de rétroaction est rigoureusement reproduite, garantissant une parfaite synchronisation entre les deux processus. Cette cohérence assure la restitution exacte de l'image originale. La Figure.9 présente le résultat de cryptage et décryptage d'une image RVB.

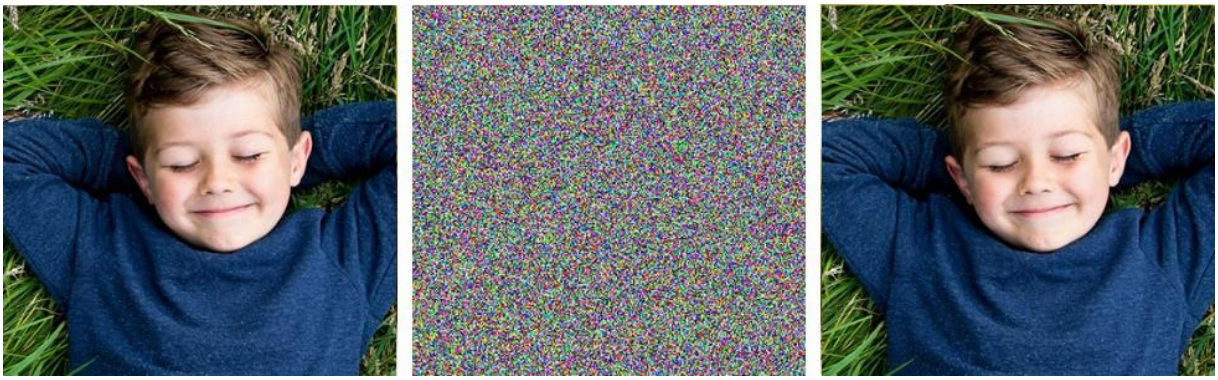

Figure 9 : Résultat de cryptage et décryptage d'une image, l'image originale (gauche), l'image cryptée

6. Evaluation de crypto-système proposé

Afin de valider l'efficacité et la robustesse du système de chiffrement par flot basé sur le système chaotique quadratique, 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 pixel) influence l'image 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 d'images numériques.

6.1. Analyse de clé

L'efficacité d'un système de chiffrement repose fondamentalement sur la robustesse de sa clé. Deux critères essentiels permettent d'évaluer cette robustesse : la taille de la clé, qui détermine l'espace de recherche pour un attaquant, et la sensibilité de la clé, qui traduit la capacité du système à produire des sorties totalement différentes en réponse à une variation minime de la clé. Cette sensibilité est un indicateur direct de la propriété de confusion, indispensable pour garantir qu'aucune corrélation exploitable n'existe entre la clé et le texte chiffré. Dans cette section, nous évaluons ces deux aspects afin de vérifier que le système proposé assure une sécurité suffisante face aux attaques par force brute et aux tentatives d'analyse différentielle.

6.1.1. La taille de la clé

D'après les diagrammes de bifurcation obtenus après l'intégration du mécanisme proposé (MP), nous avons pu constater que le système chaotique modifié permet une dynamique chaotique sur l'ensemble de l'intervalle $[-1,1]$ pour chacun des paramètres de contrôle. Cette amélioration élargit considérablement l'espace des clés exploitables, car elle autorise la génération de clés à partir de l'ensemble complet des paramètres sur toute cette plage. Chaque paramètre de contrôle est représenté en virgule fixe sur 32 bits. Le système utilise 12 paramètres de contrôle indépendants, ce qui correspond à une taille de clé théorique de : $12 \times 32 = 384$ bits.

Cependant, 3 de ces paramètres sont partiellement utilisés pour assurer la diffusion du message, en injectant les 8 bits de poids faible (LSBs) de chaque pixel clair dans les 8 LSBs de ces paramètres à chaque itération. Par conséquent, 8 bits × 3 = 24 bits de la clé sont dynamiquement modifiés par l'image claire et ne peuvent être considérés comme faisant partie de la clé statique. La taille effective de la clé fixe devient donc : $384 \text{ bits} - 24 \text{ bits} = 360$ bits ce qui constitue un espace de clé très vaste.

Selon les principes de la cryptographie symétrique, la longueur de la clé définit directement le niveau de sécurité contre les attaques par force brute, puisque le nombre de clés possibles est exponentiel en fonction du nombre de bits (2^{360} combinaisons dans notre cas). De plus, les recommandations actuelles considèrent qu'une clé symétrique de 128 bits (et jusqu'à 256 bits) offre une sécurité suffisante pour les besoins modernes .Notre clé de 360 bits excède largement ces standards, offrant ainsi une marge de sécurité significative face aux menaces actuelles et futures.

Le schéma suivant représente le processus de génération ou d'initialisation de paramètres de contrôle pour un système chaotique quadratique à partir de la clé globale du système, en plusieurs étapes :

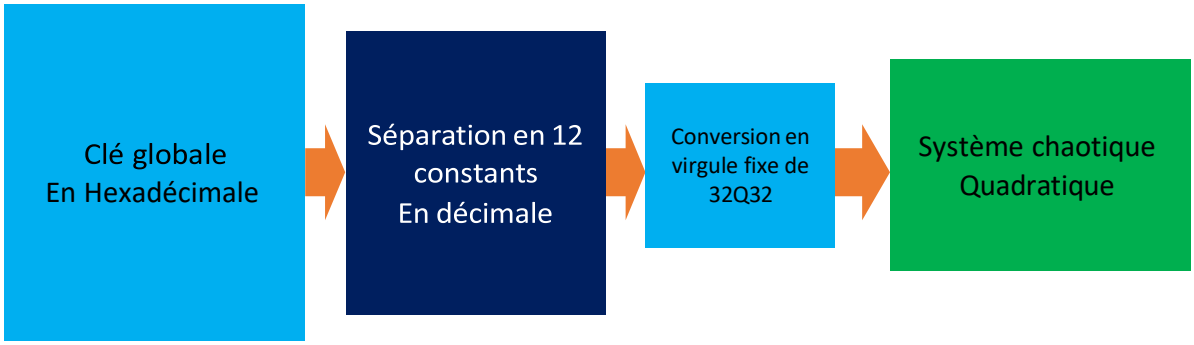

Figure 10 : Le schéma de processus de génération de paramètres de contrôle a partir de la clé globale de système.

Voici une explication étape par étape :

- **Clé globale en Hexadécimale** : Il s'agit d'une clé d'entrée exprimée en format hexadécimal (base 16), souvent utilisée dans des contextes de sécurité ou de cryptographie.
- **Séparation en 12 constantes en décimale** : La clé hexadécimale est découpée en 12 segments, puis convertie en valeurs décimales (base 10). Ces 12 constantes serviront ensuite dans les étapes suivantes comme paramètres du système.
- **Conversion en virgule fixe 32Q32 :** Les 12 valeurs décimales sont converties au format virgule fixe sur 64 bits : 32Q32 signifie que les 32 bits sont tous réservés pour la partie fractionnaire.

En somme, l'espace de clé proposé est largement supérieur aux recommandations cryptographiques usuelles, assurant une protection extrêmement forte contre les attaques par force brute, tout en conservant la cohérence avec le modèle de chiffrement par flot employé.

6.1.2. La sensibilité des clés

La sensibilité aux clés est une propriété essentielle d'un bon système de chiffrement chaotique, directement liée au principe de confusion. Elle implique qu'un léger changement dans la clé — même d'un seul bit — doit entraîner une transformation radicale du message chiffré, rendant toute tentative de retrouver le message original à partir d'une clé approximative totalement inefficace.

Dans le cadre de notre système, cette propriété est évaluée en modifiant un seul bit parmi les paramètres de contrôle utilisés comme clé, puis en comparant l'image chiffrée obtenue à celle générée avec la clé initiale. Deux images chiffrées sont ainsi dites « sensibles » si elles présentent des différences significatives pour une variation minime de la clé. Cela garantit que l'accès à une clé proche de la bonne ne permet pas à un attaquant de récupérer même partiellement l'image originale, renforçant la sécurité globale contre les attaques par analyse différentielle ou recherche exhaustive. A titre d'exemple, la Figure.11 présente le résultat de cryptage d'une image RVB avec la clé suivante : « 34CB2CCE7203A2EE66190D3F816128463CB07936E81D273AFC12ECA0C71CB2137BCAED191CCDD257 »

Nous avons tenté de reconstituer l'image originale en utilisant des clés très proches de la clé initiale. Toutes les clés testées ne différaient de la clé originale que par un seul bit. Comme le démontre la Figure.11, une variation d'un seul bit dans la clé empêche toute récupération de l'image originale, ce qui met en évidence l'extrême sensibilité du système cryptographique à la clé initiale exacte.

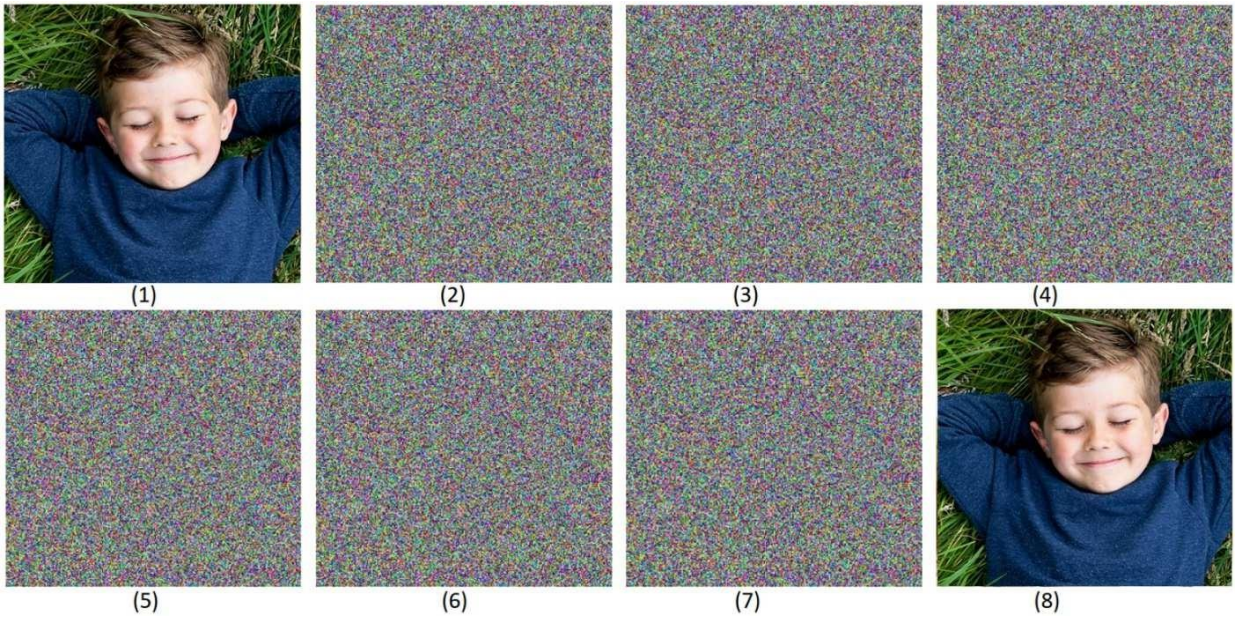

Figure 11 : Résultats de cryptage et décryptage d'une image RVB, (2) : l'image cryptée, (3) à (7) : les images décrypter par des clés différentes à celle utilisée pour le cryptage, (8) : l'image décryptée par la clé correcte.

Pour évaluer la sensibilité aux clés, on mesure généralement le taux d'erreur binaire (BER– Bit Error Rate) entre deux images chiffrées obtenues à partir de deux clés très proches (différant d'un seul bit), voici comment cela fonctionne :

1- Chiffrement avec une clé originale ⟶ on obtient une première image chiffrée C_1.
2- Chiffrement avec une clé modifiée d'un seul bit ⟶ on obtient une seconde image chiffrée C_2.
3- Calcul du BER entre C_1 et C_2, en comparant bit à bit leurs représentations binaires.

La formule est :

$$\mathrm{BER} = \frac{1}{L}\sum_{i=1}^{L} \mathrm{XOR}(C_1(i), C_2(i)) \qquad (2)$$

Où:

- L représente le nombre total de bits dans l'image (par exemple, pour une image RGB de taille M×N : L=3×M×N×8),
- C_1et C_2 désignent respectivement les $i^{éme}$ bits des deux images chiffrées.

Un BER proche de 0,5 indique une bonne propriété de confusion, c'est-à-dire qu'un léger changement dans la clé produit un effet massif et imprévisible sur le texte chiffré. Cela renforce la résistance du système contre les attaques par analyse de clé.

Dans ce contexte, on rappelle ici ce que l'on appelle l'effet d'avalanche. Il désigne en cryptographie la propriété selon laquelle un changement minime d'un bit — que ce soit dans la clé ou dans le texte clair — entraîne une modification drastique d'environ 50 % des bits du texte chiffré. En d'autres termes, chaque bit de sortie dépend de manière complexe et forte du moindre détail d'entrée.

Quand on mesure le BER entre deux images chiffrées obtenues avec des clés ne différant que d'un bit, on quantifie précisément cet effet avalanche. Un BER proche de 0,5, c'est-à-dire qu'environ la moitié des bits changent, confirme que l'effet avalanche est pleinement respecté : un petit changement de clé provoque une cascade de différences dans le chiffrement, rendant toute corrélation exploitable extrêmement difficile.

La Figure.12 présente les résultats de mesure de BER en fonction des variations sur la clé ; les variations appliquées sont autour de la clé initiale. Dans cette figure, la clé est divisée en deux moitiés juste pour pouvoir présenter le résulta en 3D.

La Figure.12 présente les résultats de la mesure du taux d'erreur binaire (BER) en fonction de variations introduites sur la clé de chiffrement. Pour permettre une visualisation en trois dimensions, la clé initiale a été divisée en deux moitiés, chacune représentant un axe de variation dans l'espace de la figure. Les modifications appliquées concernent des perturbations autour de la clé de référence. Cette représentation permet de visualiser de manière synthétique l'impact des légères variations sur la qualité du chiffrement, et donc sur la propriété de confusion du système proposé.

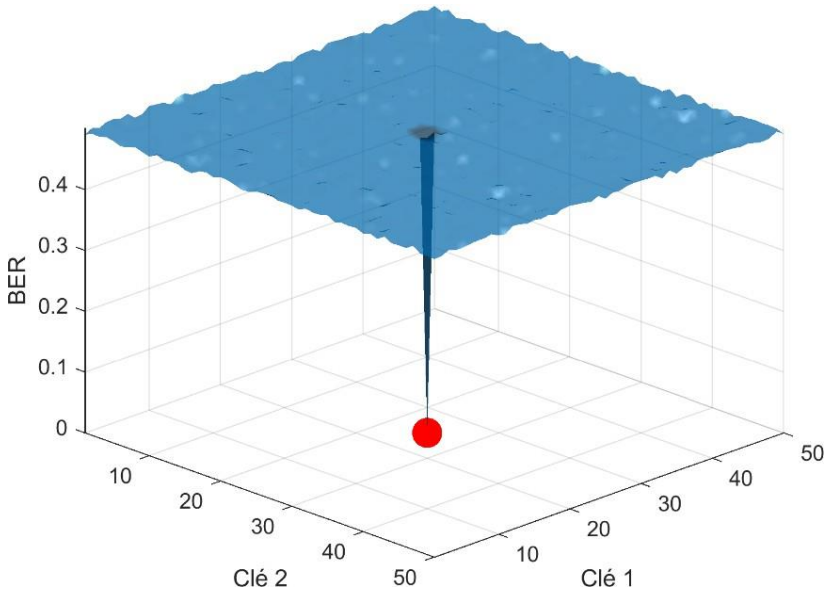

Figure 12 : Évolution du BER en fonction de deux clés proches : validation de l'effet avalanche

La figure ci-dessus révèle une excellente sensibilité du système à la clé de chiffrement, ce qui est une propriété cruciale en cryptographie. On observe que :

- Le BER (Bit Error Rate) est très proche de 0,5 dans presque toute la surface, indiquant qu'un léger changement de la clé (Clé 1 ou Clé 2) entraîne une modification massive et imprévisible du texte chiffré.

- Le seul point où le BER tombe à zéro est représenté par le point rouge (Clé 1 et Clé 2 = valeur de la clé de référence), ce qui est attendu : deux clés identiques produisent le même texte chiffré.
- Cette configuration confirme un effet avalanche bien respecté : chaque bit de la sortie dépend fortement de chaque bit de la clé. Ainsi, même une inversion d'un seul bit de la clé provoque un changement d'environ 50 % des bits dans le résultat, ce qui rend toute tentative d'attaque par analyse différentielle extrêmement difficile.

En résumé, ce comportement témoigne d'un haut niveau de confusion et d'imprédictibilité, garantissant une bonne sécurité du crypto-système face aux attaques par force brute ou corrélation.

6.2. L'évaluation de la propriété de diffusion

Après avoir introduit et expliqué l'importance de la propriété de diffusion dans les sections précédentes, nous procédons ici à son évaluation expérimentale. Cette analyse vise à vérifier dans quelle mesure le système de chiffrement proposé parvient à propager efficacement les modifications d'un message clair à l'ensemble du message chiffré. Plus précisément, nous étudions l'impact d'un changement d'un seul bit dans l'image d'entrée, en observant la proportion de bits modifiés dans les images chiffrées correspondantes. Un comportement idéal se traduit par un taux de changement proche de 50 %, confirmant une bonne capacité de diffusion du crypto-système.

Pour évaluer de manière quantitative la propriété de diffusion du système de chiffrement proposé, une méthodologie couramment adoptée consiste à observer l'impact d'une modification minime dans l'image claire sur le résultat du chiffrement.

Dans ce cadre, l'expérience consiste à générer deux images chiffrées à partir de deux images originales identiques, à l'exception du premier pixel. Cette modification localisée permet d'analyser la propagation du changement à travers toute l'image chiffrée.

Une bonne propriété de diffusion implique que cette légère variation dans l'entrée (un seul pixel) engendre une différence significative et étendue entre les deux images chiffrées, rendant difficile toute tentative d'analyse différentielle.

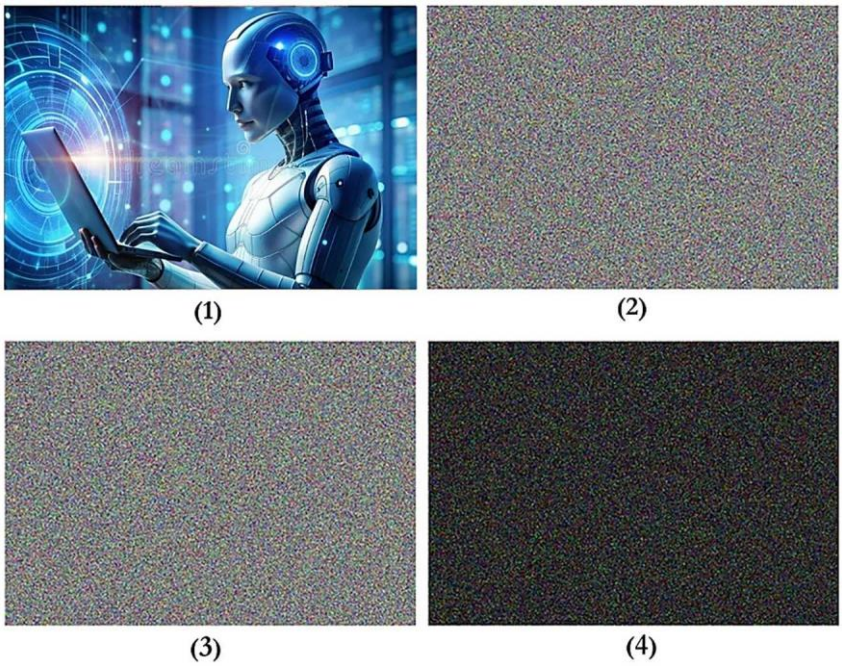

Figure 13 : Évaluation de la propriété de diffusion : 1) image originale, 2) image chiffrée, 3) image chiffrée après inversion d'un seul bit sur le premier pixel de l'image originale, 4) différence entre les images (2) et (3).

Les résultats illustrés dans la Figure 13 confirment clairement l'efficacité de la propriété de diffusion dans le système de chiffrement proposé. L'image (4), représentant la différence entre les deux images chiffrées — l'une issue de l'image originale et l'autre d'une version ne différant que par l'inversion d'un seul bit du premier pixel — montre une dispersion dense et aléatoire des pixels modifiés.

Cette observation indique que le changement minime effectué en entrée s'est propagé à travers toute l'image chiffrée, affectant de manière significative la quasi-totalité des bits de sortie. Visuellement, aucune structure ou motif ne permet de relier les deux versions chiffrées, ce qui atteste d'une forte non-linéarité du processus de chiffrement.

Autrement dit, le système réagit de manière hautement sensible à toute perturbation dans l'image d'entrée, ce qui est une caractéristique essentielle pour résister aux attaques différentielles. Ce comportement valide pleinement l'effet de diffusion cryptographique attendu, conformément au principe de confusion-diffusion de Shannon.

7. Conclusion

Ce chapitre a présenté la conception et l'évaluation d'un système de chiffrement par flot basé sur un système chaotique quadratique modifié à l'aide d'un mécanisme de perturbation (MP). À partir des limites observées dans le système quadratique original — notamment l'étroitesse et l'instabilité des zones chaotiques en représentation fixe 32 bits —, nous avons proposé une solution visant à élargir et stabiliser les comportements chaotiques.

L'analyse approfondie du système modifié, notamment à travers les diagrammes de bifurcation et les exposants de Lyapunov, a montré que le mécanisme de perturbation permet d'obtenir des dynamiques globalement plus robustes et mieux réparties dans l'espace des paramètres. Ceci renforce la fiabilité du générateur chaotique dans le contexte cryptographique.

Les séquences pseudo-aléatoires issues du système perturbé ont ensuite été soumises à une série d'évaluations, confirmant leur qualité aléatoire et leur stabilité dans différentes précisions numériques. L'étude du taux d'erreur binaire (BER) a mis en évidence une sensibilité élevée à la clé, illustrant un fort effet avalanche, caractéristique souhaitable dans tout système de chiffrement sécurisé. De plus, les tests de diffusion ont montré que des différences minimes sur un seul bit de l'image originale se propagent de manière étendue dans l'image chiffrée, ce qui renforce la résistance du système aux attaques par différentiation.

En résumé, les résultats obtenus montrent que le générateur chaotique modifié, couplé au mécanisme de perturbation, constitue un noyau robuste pour la conception de chiffrements à base de chaos. Ce système satisfait les propriétés dynamiques, de sensibilité et de diffusion attendues, et peut ainsi être considéré comme une solution prometteuse pour les applications de cryptographie d'images.

Conclusion générale

Ce mémoire a exploré l'intégration des systèmes chaotiques dans la cryptographie moderne, aboutissant à la conception d'un crypto-système innovant pour le chiffrement d'images. Les résultats obtenus démontrent la viabilité de cette approche, avec des performances remarquables en termes de sécurité et d'efficacité.

L'analyse approfondie du système quadratique chaotique modifié a révélé des propriétés cryptographiques exceptionnelles. Le mécanisme de perturbation proposé a significativement amélioré la dynamique chaotique, comme en témoignent :

- Des exposants de Lyapunov élevés (entre 1.45 et 1.88), confirmant une sensibilité optimale aux conditions initiales
- Une excellente réussite aux tests NIST SP800-22 (100% de validation à 32 bits)
- Un effet avalanche prononcé (BER proche de 50%) garantissant une diffusion optimale
- Une grande sensibilité aux clés, avec un espace de clés étendu (360 bits)

Les tests sur le chiffrement d'images RGB ont validé l'efficacité pratique du système, montrant sa capacité à transformer radicalement les images tout en permettant une restitution parfaite lors du déchiffrement. La propriété de diffusion a été particulièrement remarquable, avec une modification minime de l'image originale affectant de manière uniforme l'ensemble de l'image chiffrée.

Perspectives Futures

La prochaine étape de ce travail consistera en l'implémentation matérielle du système sur FPGA. Cette plateforme offrira plusieurs avantages cruciaux :

1. **Accélération matérielle** : L'architecture parallélisable des FPGA permettra d'atteindre des performances temps réel adaptées aux applications embarquées
2. **Optimisation des ressources** : La logique reconfigurable permettra d'implémenter efficacement les opérations mathématiques complexes du système chaotique
3. **Sécurité renforcée** : L'implémentation matérielle offrira une protection supplémentaire contre les attaques par canaux auxiliaires
4. **Adaptabilité** : La nature reconfigurable des FPGA facilitera l'évolution et l'optimisation du système.

Cette implémentation ouvrira la voie à des applications concrètes dans divers domaines exigeants :

- Sécurisation des flux vidéo en temps réel

- Protection des images médicales
- Chiffrement embarqué pour l'IoT
- Systèmes de surveillance sécurisés

En conclusion, ce travail a démontré le potentiel des systèmes chaotiques pour renouveler les approches cryptographiques traditionnelles. La combinaison entre robustesse théorique et perspectives d'implémentation matérielle positionne cette solution comme une alternative prometteuse pour répondre aux défis croissants de la sécurité numérique. Les résultats obtenus et les développements envisagés contribuent ainsi à l'émergence d'une nouvelle génération de systèmes cryptographiques adaptés aux exigences du monde connecté.

Bibliographie

[1] Stallings, W. (2018). Effective cybersecurity: a guide to using best practices and standards. Addison-Wesley Professional.

[2] Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (2018). Handbook of applied cryptography. CRC press.

[3] Trnka, Michal, Tomas Cerny, and Nathaniel Stickney. "Survey of Authentication and Authorization for the Internet of Things." Security and Communication Networks 2018.1 (2018): 4351603.

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

[5] National Institute of Standards and Technology. (1977). FIPS PUB 46: Data Encryption Standard (DES).

[6] EFF. (1998). Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design. O'Reilly.

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

[8] Menezes, A., van Oorschot, P., & Vanstone, S. (1996). Handbook of Applied Cryptography.

[9] Downloaded on 05/23/2025 from : https://cyberw1ng.medium.com/triple-des-3des-encryption-features-process-advantages-and-applications-2023-587e5a092789

[10] Daemen, J., & Rijmen, V. (2002). The Design of Rijndael.

[11] Schneier, B. (1993). Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish).

[12] Schneier, B., et al. (1998). The Twofish Encryption Algorithm.

[13] Rivest, R. (1998). RSA Laboratories Technical Reports.

[14] RFC 7465. (2015). Prohibiting RC4 Cipher Suites in TLS

[15] Menezes, A., van Oorschot, P., & Vanstone, S. (1996). Handbook of Applied Cryptography.

[16] Diffie, W., & Hellman, M. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644-654.

[17] Stallings, W. (2023). Cryptography and Network Security: Principles and Practice (8th ed.). Pearson.

[18] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126.

[19] ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 31(4), 469-472.

[20] Hankerson, D., Vanstone, S., & Menezes, A. (2004). Guide to Elliptic Curve Cryptography. Springer.

[21] Zimmermann, P. (1995). The Official PGP User's Guide. MIT Press.

[22] Bernstein, D. J., et al. (2017). Post-quantum cryptography. Nature, 549(7671), 188–194.

[23] Robert C.Hilborn, "Chaos and nonlinear Dynamics, second edition", page 03, Oxford university press, 2000.

[24] Mihai Bogdan Luca, "Apports du chaos et des estimateurs d'états pour la transmission sécurisée de l'information", l'Université de Bretagne Occidentale, novembre 2006

[25] ODEN Jérémy, "Le chaos dans les systèmes dynamiques", juillet 2007, chapitre2 , téléchargée le 15/05/09 de : www.spectrosciences.com

[26] François Charru, "Instabilités Hydrodynamiques", Page 317, EDP sciences 2007, CNRS edition

[27] H. Shun-Cheng and al, The Cycle Length, Statistical and Key Sensitivity Properties of a Perturbed Couple Chaotic PRBG, IEEE Conference Publications, International Conference on Multimedia Technology (ICMT), 2011, 26-28 July 2011, Hangzhou, pp.3268 – 3272, P.ISBN: 978-1-61284-771-9.

[28] Kathleen Alligood, Tim Sauer, and James A. Yorke. Chaos : An Introduction to Dynamical Systems. Springer, 1996.

[29] G.L . Baker et J.P Gollub, "Chaotic dynamics", seconde edition page 76

[30] Haoran, Wen. "A review of the Hénon map and its physical interpretations." Georgia Tech PHYS 7224: nonlinear dynamics, course project, spring semester 2014.

[31] Hénon, Michel. "A two-dimensional mapping with a strange attractor." Communications in Mathematical Physics 50.1 (1976): 69-77

[32] Larry Bradley, Chaos and fractals, 2010

[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] Jafari, A., Hussain, I., Nazarimehr, F., Golpayegani, S. M. R. H., & Jafari, S. (2021). A simple guide for plotting a proper bifurcation diagram. International Journal of Bifurcation and Chaos, 31(01), 2150011. https://doi.org/10.1142/S0218127421500115

[35] 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

[36] 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