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

UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU

FACULTE DE GENIE ELECTRIQUE ET INFORMATIQUE

DEPARTEMENT : ELECTRONIQUE

Mémoire de fin d'études

En vue de l'obtention du diplôme Master académique
Brevet / STARTUP

Domaine : **Sciences et Technologie**

Filière : **Génie Electrique**

Spécialité : **Electronique des Systèmes Embarqués**

Thème

Conception Et Réalisation D'un Système De Cryptage De Données Pour La Transmission Drone/Télécommande

Présenté par :

MELBOUCI SALIHA
MELLAL AMEL

Dirigé par :

Mr. ZIRMI RACHID

Co-encadrer par :

Mme. MEGHERBI OUERDIA

Promotion : 2023/2024

Remerciements

Remerciements

Nous tenons tout d'abord à exprimer notre profonde gratitude envers Dieu, qui nous a accordé la force, la persévérance et la clarté d'esprit nécessaires pour mener à bien cette recherche.

Nous souhaitons également adresser nos sincères remerciements à notre encadreur, Monsieur ZIRMI, ainsi qu'à notre co-encadreuse, Madame MEGHERBI, pour leur disponibilité, leur suivi constant et leurs précieux conseils tout au long de ce travail. Un grand merci à Monsieur GANA, dont l'expertise, la disponibilité et les encouragements ont joué un rôle crucial dans la réussite de ce projet.

Nous remercions également les membres du jury qui nous font l'honneur de juger notre travail, ainsi que les membres de l'incubateur pour les formations qu'ils nous ont dispensées, nous permettant ainsi de mener à bien notre startup.

Enfin, nos remerciements s'adressent à toutes les personnes qui, de près ou de loin, ont contribué à cette recherche et à l'enrichissement de nos connaissances. Votre soutien et votre implication ont été inestimables, et nous vous en sommes profondément reconnaissants.

Dédicaces

Dédicace

Je dédie ce travail :

À mes chers parents, pour tout le soutien et l'amour que vous m'avez donnés, me permettant d'accomplir ce parcours. Aucune parole ne pourra jamais traduire toute la reconnaissance que je ressens pour vous.

À ma sœur, mon frère, et à tous mes proches. Votre amour, vos encouragements constants, et votre présence bienveillante ont été des sources inestimables de motivation. Vous avez contribué, chacun à votre manière, à la réussite de cet accomplissement.

À mes amis fidèles, qui m'ont accompagné tout au long de cette aventure, je vous exprime toute ma gratitude pour la force et l'inspiration que vous m'avez apportées.

Un remerciement spécial à mon binôme, Amel, avec qui j'ai partagé ce parcours académique pour la réalisation de notre mémoire de fin d'études, et avec qui j'ai tissé des liens d'amitié sincères.

Saliha

Dédicace

Je remercie Allah de m'avoir accordé le don de l'écriture et de la réflexion, la force de persévérer dans mes projets, et la patience d'atteindre mes objectifs.

Je dédie ce travail à mes parents bien-aimés, à qui je dois tout. Leur amour inconditionnel, leur soutien indéfectible et leurs sacrifices m'ont permis de devenir la personne que je suis aujourd'hui. Qu'Allah les protège et les récompense généreusement.

À ma sœur, mon frère, mes neveux, ainsi qu'à toute ma famille et mes proches, qui me souhaitent toujours la réussite.

À mes chers amis et chères amies, qui m'encouragent sans relâche, tant dans les moments de doute que dans ceux de bonheur. Merci à vous.

Un remerciement tout particulier à Saliha, mon binôme, pour sa précieuse collaboration et son amitié. Ensemble, nous avons surmonté tous les défis.

Amel

Table des matières

Chapitre 2 Généralités sur les systèmes chaotiques

Chapitre 3 Généralités sur le Cryptage

Chapitre 4 Réalisation

Liste des figures

Liste des figures

Liste des figures

Liste des tableaux

Liste des tableaux

Listes d’abréviations

Abréviations :

UAV (Unmanned Aerial Vehicle) : Véhicule aérien autonome (drone)

ESC (Electronic Speed Controller) : Régulateur de vitesse électronique

PDB (Power Distribution Board) : Carte de distribution d'énergie

LiPo (Lithium Polymer) : Type de batterie utilisée

FPV (First Person View) : Vol en immersion

LoRa : Long Range (communication sans fil longue portée)

GPS : Global Positioning System

Wi-Fi : Wireless Fidelity

MHz : Mégahertz

GHz : Gigahertz

mAh : Milliampère-heure (capacité de batterie)

ARM : Advanced RISC Machine (type de processeur)

IDE : Integrated Development Environment (environnement de développement intégré, utilisé ici pour Arduino)

PWM : Pulse Width Modulation (modulation de largeur d'impulsion)

Introduction

Introduction générale

Ces dernières années, le domaine de la robotique aérienne a connu un essor considérable, devenant l'une des branches les plus dynamiques des systèmes embarqués. Les véhicules aériens autonomes (UAVs), ou drones, suscitent un intérêt croissant tant pour les applications professionnelles que pour les loisirs. Grâce à des avancées technologiques dans les domaines de l'électronique, de la miniaturisation et des systèmes embarqués, ces dispositifs offrent désormais de nombreuses possibilités dans des secteurs aussi divers que la cartographie, le militaire, l'agriculture de précision ou encore la modélisation 3D [56]. Cependant, avec l'essor des drones et la multiplication des échanges de données sensibles, la sécurisation des transmissions est devenue une priorité absolue. En effet, les informations transmises par les drones, qu'elles soient de nature civile ou militaire, sont de plus en plus vulnérables aux attaques extérieures, d'où la nécessité d'adopter des méthodes de cryptage robustes pour garantir la confidentialité et l'intégrité des communications.

La cryptographie, science millénaire de la protection des messages, a évolué au fil du temps pour répondre aux défis des nouveaux modes de communication. Parmi les récentes avancées dans ce domaine, l'utilisation des systèmes chaotiques s'est révélée être une approche prometteuse pour le cryptage des données. Découvert dans les années 1960 par le météorologue Edward Lorenz [57], le chaos se distingue par sa sensibilité aux conditions initiales et son comportement imprévisible à long terme, malgré sa nature déterministe. Ces propriétés font des systèmes chaotiques des candidats idéaux pour masquer les informations de manière sûre et efficace. Plus récemment, la cryptographie chaotique, qui consiste à utiliser des signaux chaotiques pour camoufler des données, a émergé comme une alternative viable aux méthodes de chiffrement classiques.

C'est dans ce cadre que s'inscrit notre projet de mémoire startup, visant à innover dans le domaine de la sécurisation des communications par drone. L'objectif de ce projet est de concevoir et de développer un système de cryptage basé sur un modèle de chaos. Cet oscillateur chaotique, spécialement adapté pour répondre aux exigences de la transmission sécurisée, génère des signaux complexes et imprévisibles, garantissant un haut niveau de sécurité pour les données échangées via drone. Ce système ambitionne non seulement de protéger efficacement les informations contre toute tentative d'intrusion ou d'espionnage, mais aussi de maintenir un débit de communication compatible avec les contraintes des systèmes embarqués.

Ce mémoire est structuré en quatre parties. Le premier chapitre présente une introduction générale aux drones, leurs applications et les défis liés à leur utilisation. Le deuxième chapitre est consacré aux systèmes chaotiques et à leurs propriétés, en mettant l'accent sur l'intérêt du chaos dans les systèmes de communication sécurisée. Le troisième chapitre aborde les principes de la cryptographie, avec un focus sur les méthodes de chiffrement chaotiques. Enfin, le quatrième chapitre détaille la conception et la mise en œuvre de notre système de cryptage basé sur l'oscillateur chaotique.

CHAPITRE 1

Etat de l'art sur le drone

Introduction

Dans ce chapitre, nous allons examiner l'évolution des drones, depuis leur apparition jusqu'à leur intégration dans divers secteurs d'activité. Nous commencerons par un aperçu historique suivi de la définition d'un drone. Ensuite, nous détaillerons l'architecture d'un drone, en décrivant les composants clés tels que le châssis, le système de propulsion, les moteurs, et les systèmes de communication. Une classification des drones sera ensuite présentée, basée sur des critères d'altitude, de taille et de mode de propulsion. Nous explorerons également les différents domaines d'utilisation des drones, qu'il s'agisse du secteur militaire, de la livraison, de l'agriculture ou encore de la photographie. Pour terminer, nous aborderons les dernières avancées ainsi que les défis opérationnels auxquels fait face cette technologie en constante évolution.

1.1 Histoire de drone

L'origine du drone remonte à la fin du XIXe siècle, avec les premiers ballons captifs utilisés à des fins d'observation. Toutefois, c'est pendant la Première Guerre mondiale, entre 1914 et 1918, que les États-Unis ont manifesté un intérêt marqué pour le développement de ces dispositifs. Ce n'est que lors de la Seconde Guerre mondiale, lorsque les aviations d'observation des différents camps ont subi d'importantes pertes, que l'idée de créer des engins d'observation non habités a émergé.

Pendant la Guerre Froide, et plus précisément durant la guerre du Viet Nam et celle du Kippour, le véritable essor des drones a eu lieu. C'est à cette époque que leur utilisation s'est largement développée, notamment au sein des armées. Les Américains ont utilisé des drones Firebee pendant la guerre du Vietnam pour localiser les rampes de lancement des missiles solair soviétiques «SAM-2» : 3500 missions furent recensées. Plus tard, en 1991, lors de la guerre du Golfe, ils ont fait appel au drone (Pioneer) pour la surveillance jour/nuit, l'acquisition des objectifs, et les réglages de l'artillerie. Dans ce même conflit, les Britanniques et les Français commencèrent à servir des drones [1].

Pendant la guerre du Kippour en 1973, les Israéliens ont également fait un usage intensif des drones [2], réussissant à saturer les défenses aériennes égyptiennes le long du canal de Suez en déployant un grand nombre de drones bon marché.

Pendant la guerre froide, les Américains ont été motivés par la nécessité d'envoyer des drones près des sites d'essais nucléaires, inaccessibles aux humains, renforçant ainsi l'intérêt stratégique des drones pour les missions dangereuses ou sensibles.

La fin du XXe siècle a été marquée par l'introduction du "Predator", un drone américain, pour des missions de reconnaissance, développant ainsi de nouvelles capacités de surveillance et de renseignement.

Les années 2000 ont vu l'émergence du "Global Hawk" comme un support essentiel lors d'opérations militaires. Disposant d'une grande autonomie et d'une forte capacité d'observation, ce drone a joué un rôle clé dans de nombreux conflits contemporains.

1.2 Définition d'un drone

Un UAV, ou drone, est un véhicule aérien sans pilote qui peut voler de manière autonome ou être contrôlé à distance. Utilisant la force aérodynamique pour maintenir son vol, il peut être réutilisable ou récupérable et transporte une charge utile, pouvant être létale ou non. Ces appareils sont polyvalents et peuvent être employés dans diverses applications, de la livraison de colis aux opérations militaires.

« Le nom de drone vient d'un mot anglais signifiant faux-bourdon donné comme surnom par l'artillerie anglaise dans les années 1930 à un avion cible utilisé pour l'entraînement ayant un vol lent et bruyant ressemblent à celui du bourdon. Maintenant il désigne un aéronef sans pilote à bord généralement télécommandé du sol, il peut être programmé pour voler de façon autonome ou via un smart-phone ou une tablette, etc. » [3]

1.3 Architecture et composants d'un drone

1.3.1 Un châssis

C'est la structure de base du drone, qui peut être fabriquée à partir de différents matériaux tels que la fibre de carbone, le plastique, l'aluminium, ou d'autres matériaux résistants. Le châssis peut être conçu pour accueillir 3, 4, 6 ou 8 bras pour la fixation des moteurs. Il peut être recouvert d'une coque en plastique pour des raisons esthétiques ou rester sans revêtement pour réduire le poids de l'appareil.

1.3.2 Un système de propulsion

Ce système permet au drone de se déplacer dans les airs. Il est composé de moteurs, d'hélices et de contrôleurs de vitesse électroniques (ESC). Les drones de loisir sont généralement alimentés par des batteries électriques. Le temps de vol et la charge maximale supportée par le drone dépendent des spécifications de ces composants.

1.3.3 Un contrôleur de vol

Les cartes de contrôle de vol, surnommées le cerveau des drones, sont essentielles à leur navigation. Elles interprètent les signaux des capteurs et récepteurs pour guider le drone selon les données qu'elles reçoivent, telles que la position, la vitesse ou la direction. Les capteurs (gyroscope, accéléromètre, GPS, etc.) jouent un rôle central, en permettant au contrôleur de stabiliser et d'orienter l'appareil en vol. Différents types de contrôleurs existent, allant des modèles simples à base de microprocesseur, aux plus avancés avec processeur ARM, tout-enun ou encore open source, qui offrent une grande flexibilité.

En plus des trois principaux composants mentionnés ci-dessus, les drones peuvent contenir d'autres composants complémentaires tels que :

1.3.4 Les moteurs

Les moteurs de drones sont des moteurs électriques brushless spécialement conçus pour fournir la puissance nécessaire à la propulsion des drones. Alimentés par des batteries LiPo, ces moteurs fonctionnent à des régimes élevés pour maintenir le drone en vol. Ils sont caractérisés par le diamètre de leur cage tournante et par le nombre de tours/volt ou KV. Un moteur ayant un KV de 1000 tr/V fonctionnera à 12000 tours/min s'il est alimenté en 12V.

Figure 1.1: Moteur brushless

1.3.5. Les hélices

Les hélices d'un drone, fabriquées en plastique ou en matériaux composites, sont essentielles à sa propulsion et stabilité. Leur diamètre et leur pas, mesurés en pouces (par exemple 9x4, 5), déterminent leur performance. Un drone quadrirotor utilise deux hélices à sens horaire et deux à sens anti-horaire pour équilibrer les forces de traction et assurer un vol stable.

Figure 1.2: Hélices du drone

1.3.6 La batterie

Les batteries utilisées dans les drones multirotors sont principalement des batteries au lithium polymère (LiPo), appréciées pour leur rapport poids/puissance élevé. Ces batteries fournissent généralement une tension de 3,7V par cellule (1S), et les configurations courantes sont de 3 ou 4 cellules (3S ou 4S). Leur capacité, exprimée en mAh, influence directement l'autonomie du drone, une batterie de 3000mAh offrant une meilleure autonomie qu'une batterie de 2200mAh. Il est crucial d'utiliser un chargeur spécifique et de respecter strictement les règles de sécurité, car les batteries LiPo peuvent être dangereuses en cas de manipulation incorrecte.

Figure 1.3: Batterie

1.3.7 Système de communication

Les drones nécessitent différents systèmes de communication pour permettre leur contrôle et leur pilotage. La radio-commande est un élément essentiel pour contrôler un drone. Elle se compose d'un émetteur pour le pilote et d'un récepteur intégré dans l'appareil. Les radios modernes utilisent généralement la technologie 2,4 GHz, offrant une meilleure fiabilité et une

plus grande portée que les radios FM en 41 MHz. Une radio-commande idéale devrait avoir six voies pour piloter le drone avec précision et activer des fonctions supplémentaires. Il existe deux modes de configuration des manettes, le Mode 1 et le Mode 2, qui offrent des dispositions différentes pour les commandes de gaz et de direction.

Figure 1.4: Radio commande

Autres systèmes de communication pour les drones :

Système	Description
Smartphone ou tablette	Contrôle du drone via une application dédiée et une connexion sans fil (Wi-Fi ou Bluetooth). Offre une interface intuitive avec des fonctionnalités avancées comme le suivi automatique et le partage de vidéos.
Lunettes FPV (First Person View)	Permet une expérience de pilotage immersive en donnant au pilote une vue en temps réel de ce que voit la caméra du drone.
Commandes vocales	Le pilote contrôle le drone en utilisant des instructions vocales, offrant une alternative pratique à la radio-commande.
Interface cerveauordinateur	Utilise les signaux électriques générés par l'activité cérébrale du pilote pour contrôler le drone, offrant une approche innovante et immersive.

Tableau 1.1: système de communication

1.3.8 La camera

La présence d'une caméra sur un drone peut servir à enregistrer des vidéos du vol pour une visualisation ultérieure ou à pratiquer le vol en immersion (FPV).

1.3.9 Carte de distribution d'énergie

La carte de distribution d'énergie (PDB) est un circuit imprimé essentiel pour la gestion des connexions électriques dans un drone. Elle répartit efficacement l'énergie de la batterie vers les différents composants comme les moteurs, contrôleurs de vol, caméras et éclairages. Bien que non systématique sur tous les drones, la PDB permet une organisation propre et sécurisée

des connexions, assurant un fonctionnement équilibré et fiable de l'ensemble des systèmes embarqués.

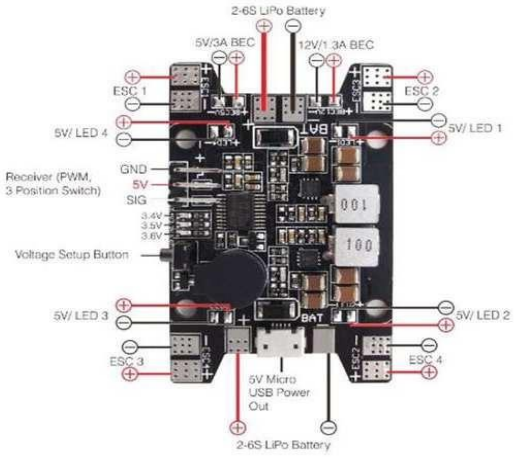

Figure 1.5: carte de distribution d'énergie

1.3.10 Régulateur de vitesse électronique

Les contrôleurs électroniques de vitesse (ESC) représentent une composante essentielle du fonctionnement des drones, car ils régulent la vitesse et la direction des moteurs en transformant les signaux électriques de la carte de contrôle de vol en mouvements physiques des hélices. Grâce à des microcontrôleurs et des logiciels sophistiqués, les ESC permettent un contrôle précis et réactif, contribuant directement à la stabilité et à la maniabilité du drone en vol. Chaque moteur est associé à son propre ESC, bien que des versions ESC 4 en 1 existent pour simplifier l'installation. Lors de problèmes de puissance, l'ESC est souvent le premier élément à vérifier pour identifier d'éventuelles pannes.

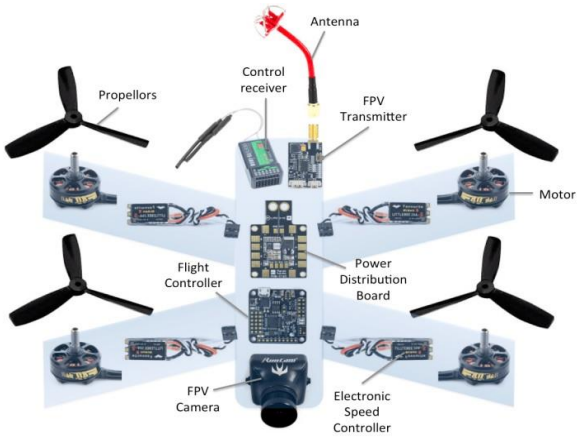

Figure 1.6: Bronchement d'un régulateur de vitesse sur un drone

1.4 Classification des drones

Dans le domaine des drones, une classification variée est possible selon plusieurs critères, notamment la taille, l'altitude et le mode de propulsion.

1.4.1 Classification selon l'altitude et la taille

- **HALE (High Altitude Long Endurance)** : Ces drones, de grande taille, peuvent atteindre les dimensions d'un avion civil. Ils sont conçus pour des vols de longue durée, pouvant aller jusqu'à 48 heures, et collectent des informations sur de vastes zones.

Figure 1.7: Drone type HALE

- **MALE (Medium Altitude Long Endurance)** : Ces drones volent à moyenne altitude, entre 5000 et 12000 mètres, et sont capables de parcourir jusqu'à 1000 km à des vitesses relativement faibles. Ils ont une masse pouvant atteindre 3,5 tonnes et une envergure généralement comprise entre 10 et 20 mètres.

Figure 1.8: Drone type MALE

- **Micro-drone** : Ces drones de petite taille, variant du centimètre à quelques dizaines de centimètres, sont propulsés électriquement et sont adaptés aux vols en intérieur. Ils sont généralement utilisés pour des charges légères.

Figure 1.9: Drone type micro-drone

- **Mini-drone** : Ils ont légèrement plus d'envergure que les micro-drones. La taille d'un mini drone varie entre 50 cm et 2 m. Les mini-drones sont très souvent utilisés dans les missions d'enregistrements et de prise de vues aériennes. Ils sont aussi utilisés dans l'audiovisuel et dans la cinématographie [4]

Figure 1.10: Drone type mini-drone

1.4.2 Classification selon le mode de propulsion

Les drones peuvent également être classés en fonction de leur mode de propulsion :

- Drones à ailes battantes : Inspirés par les oiseaux ou les insectes, ces drones imitent le mouvement des ailes pour se déplacer.
- Drones à voilure fixe : Ces drones utilisent des ailes fixes, similaires à celles des avions ou des dirigeables, pour le vol.
- Drones à voilure tournante : Cette catégorie comprend les drones mono-rotors, birotors, tri-rotors et multi-rotors.

- Drones mono-rotors : Ils sont équipés d'un rotor principal, parfois avec un rotor de queue pour contrôler la direction.

Figure 1.11: Drone type mono-rotors

- Drones birotors : Composés de deux rotors coaxiaux contrarotatifs, ils peuvent utiliser des configurations variées pour le contrôle de position.

Figure 1.12: Drone type birotors

- Drones tri-rotors : Dotés de deux rotors à l'avant et un à l'arrière pour le réglage du roulis, ils offrent des performances de vol différentes des quadrirotors.

Figure 1.13: Drone type tri-rotors

- Multi-rotors : Avec plusieurs rotors, ces drones peuvent supporter des charges plus lourdes en raison de leur capacité de portance accrue.

Figure 1.14: Drone type multi-rotors

1.5 Domaine d’utilisation

1.5.1 Militaire

Les drones ont d'abord été développés pour des usages militaires, notamment durant la Seconde Guerre mondiale. Leur utilisation s'est intensifiée au Vietnam et lors de conflits comme la guerre du Golfe et le Kosovo. Ils remplissent des missions de surveillance, de soutien au combat et de combat direct, équipés de systèmes sophistiqués comme des caméras thermiques et des armes. « L'un des drones les plus utilisés à des fins militaires aujourd'hui est le MQ-9 Reaper, qui mesure 36 pieds de long et a une portée de vol de 1 852 km à une altitude de 50 000 pieds. » [5]

1.5.2 Livraison

Les drones sont de plus en plus utilisés pour les livraisons, offrant une solution efficace pour les envois urgents et dans des zones difficiles d'accès. Bien que leur capacité de charge soit encore limitée, ils promettent d'améliorer la rapidité et l'efficacité des services logistiques. « L’introduction de la livraison par drone Amazon Prime Air durant l’été 2020 a été précédée par l’entreprise d’e-commerce JD.com basée en Chine, qui avait commencé à utiliser des drones pour servir ses clients dans les zones difficiles d’accès du pays dès 2016. Approuvé par la FAA en 2019, le service Flight Forward d’UPS a été le tout premier service de drone fonctionnant comme une ligne commerciale. Les services de livraison commerciale par drone sont également disponibles en Australie et en Europe. En plus d’être utilisés pour livrer des paquets aux clients, les drones sont utilisés dans les entrepôts dans le cadre du déploiement généralisé de robots autonomes pour aider à scanner les stocks, en particulier dans les zones difficiles d’accès, sans l’aide de lasers ou de repères. [6] »

Figure 1.15: Drone de livraison

1.5.3 Photographie et vidéographie

Les drones ont révolutionné l'industrie des tournages vidéo en offrant des prises de vue aériennes spectaculaires et des images de haute qualité autrefois difficiles à obtenir. Ils sont désormais essentiels pour capturer des plans uniques dans des publicités, des films, des événements, et bien plus encore, ouvrant ainsi de nouvelles perspectives créatives.

Recherche et sauvetage

Dans les opérations de recherche, de sauvetage, et les situations d'urgence, les drones sont devenus des outils indispensables. Leur capacité à accéder à des zones difficiles, à localiser rapidement les personnes en danger grâce à des caméras thermiques et des capteurs avancés, ainsi qu'à permettre une intervention rapide, en fait des alliés précieux pour sauver des vies et minimiser les risques pour les équipes de secours.

1.5.4 Agriculture

L'utilisation croissante des drones révolutionne le domaine de l'agriculture en offrant aux agriculteurs des outils précis et polyvalents pour surveiller les cultures, cartographier les terres, pulvériser efficacement les produits agricoles et optimiser les pratiques de gestion des ressources.

Figure 1.16: Drone d'agriculture

1.6 Avancées récente dans le domaine des drones

Les avancées technologiques dans le domaine des drones ont franchi des étapes impressionnantes, avec des innovations marquantes qui redéfinissent les capacités et les applications de ces appareils volants [7]. Mais ce n'est pas tout : les drones intègrent désormais

des systèmes de détection d'obstacles omnidirectionnels avec une portée maximale de 200 mètres, rendant le vol autonome plus sûr et plus fiable que jamais.

1.7 Les défis opérationnels

L'adoption des drones dans les domaines civil et militaire est freinée par plusieurs défis opérationnels et techniques.

1.7.1 Difficultés opérationnelles

L'intégration des drones dans l'espace aérien nécessite des normes strictes, assurant fiabilité en vol, détection d'obstacles et gestion des urgences. Sur le plan juridique, l'utilisation des drones est encadrée par des législations spécifiques qui varient d'un pays à l'autre, régissant leur enregistrement et l'obtention de licences.

Les drones, bien qu'ayant une capacité de vol à haute altitude, soulèvent des questions de souveraineté aérienne et sont vulnérables aux menaces. La sécurité des communications entre le drone et le sol est primordiale pour éviter les interférences.

1.7.2 Difficultés techniques

La fiabilité des transmissions, la discrétion des drones pour des usages militaires, et la motorisation doivent répondre à des exigences élevées. La maintenance, la gestion des pannes en vol, et l'entraînement des opérateurs sont des aspects clés à optimiser pour garantir des performances durables et sécurisées. Entraînement et maintien des compétences des opérateurs : Si la simulation intensive est possible, l'expérience montre que l'entraînement réel sur le terrain est indispensable pour valider l'état opérationnel et l'efficacité des systèmes.

Conclusion

Ce chapitre a établi une base de compréhension essentielle des drones, de leurs composants ainsi que de leurs diverses applications civiles et militaires. Cette exploration préliminaire permet d'appréhender les défis techniques et réglementaires inhérents à leur intégration dans les secteurs civil et commercial. Le chapitre suivant introduira les systèmes chaotiques, en approfondissant leur rôle dans la cryptographie pour sécuriser les communications entre drones et dispositifs de commande.

CHAPITRE 2

Généralités sur les systèmes chaotiques

Introduction

Dans ce chapitre, nous abordons les systèmes chaotiques, en retraçant leur histoire, depuis les premières découvertes de Poincaré et Lorenz, jusqu'à leur application en cryptographie. Nous définirons ensuite les systèmes chaotiques et mettrons en lumière leurs principaux avantages pour la sécurité des communications. En particulier, nous explorerons des concepts clés tels que l'aspect aléatoire, la sensibilité aux conditions initiales, et les attracteurs étranges, avant d'illustrer ces notions par des exemples concrets comme les systèmes de Lorenz et de Hénon modifié. Cette analyse théorique nous permettra de mieux comprendre l'utilisation des systèmes chaotiques dans le cryptage des données, notamment pour les transmissions sécurisées entre drones et télécommandes.

2.1 Histoire des systèmes chaotiques

L'histoire des systèmes chaotiques constitue un domaine d'étude significatif qui s'étend sur plusieurs siècles. Ce champ de recherche est étroitement lié à l'évolution des mathématiques, de la physique et de diverses disciplines scientifiques. Cela comprend l'étude de systèmes très sensibles aux conditions initiales, un phénomène souvent appelé « effet papillon ». Ce concept suggère que de petits changements dans l'état initial d'un système peuvent conduire à des résultats radicalement différents, rendant impossibles les prévisions à long terme pour certains systèmes.

Les racines de la théorie du chaos remontent à la fin du 19ème et au début du 20ème siècle [8]. Le mathématicien français Henri Poincaré est considéré comme l'un des premiers à avoir ouvert la voie à la théorie du chaos. En étudiant le problème des trois corps en mécanique céleste, il découvrit des orbites non périodiques qui ne convergeaient pas simplement vers un point fixe, indiquant ainsi un comportement chaotique dans des systèmes déterministes. Poincaré avait noté cet effet et l'a mentionné dans ses écrits en 1908 : « *Une cause très petite qui nous échappe détermine un effet considérable que nous ne pouvons pas ne pas voir, et alors nous disons que cet effet est dû au hasard. Il peut arriver que de petites différences dans les conditions initiales en engendrent de très grandes dans les phénomènes finaux. Une petite erreur sur les premières produirait une erreur énorme sur les derniers la prédiction devient impossible* et nous avons le phénomène fortuit » [9].

Au début des années 1960, Edward Lorenz, mathématicien et météorologue américain, à découvert que le temps présente un phénomène non linéaire connu sous le nom de dépendance

sensible aux conditions initiales [10]. Il a démontré qu'un simple ensemble de trois équations non linéaires couplées de premier ordre pouvait entraîner des trajectoires complètement chaotiques. Sa découverte a révélé que de petites variations dans les conditions initiales peuvent produire des résultats totalement différents, illustrant ainsi le concept du chaos déterministe. Grâce à cette avancée, la théorie moderne du chaos a trouvé ses fondements en montrant que même les systèmes régis par des lois précises peuvent avoir un comportement imprévisible en fonction des conditions initiales.

L'exploration de la théorie du chaos s'est intensifiée durant les années 1970 et 1980 grâce à des contributions majeures de scientifiques tels que Mitchell Feigenbaum, qui découvrit les constantes universelles liées au chaos en étudiant le phénomène de doublement de période. En 1975, James Yorke et T.Y. Li introduisirent le terme "chaos" dans un contexte mathématique, donnant un nom officiel à ce comportement complexe. Leurs recherches, ainsi que celles d'autres experts, ont enrichi notre compréhension des dynamiques chaotiques dans divers systèmes, des conditions météorologiques aux marchés financiers.

Depuis lors, la théorie du chaos s'est étendue à de nombreux domaines, comme la météorologie, l'ingénierie, l'économie, la biologie et la philosophie. Elle a transformé notre compréhension du monde naturel, mettant en lumière la complexité et l'interconnexion de systèmes autrefois considérés comme déterministes et prévisibles.

Le tableau ci-dessous présente les étapes marquantes du développement de la théorie du chaos :

1890	Henri Poincaré a remporté le premier prix du roi Oscar II, étant le plus proche à résoudre le problème des n-corps en astronomie. Il a découvert que lorsque trois corps célestes interagissent, leurs orbites peuvent devenir instables et imprévisibles. C'est à partir de cette découverte que la notion de chaos a émergé.
1963	Edward Lorenz a découvert qu'un simple système composé de trois équations non linéaires peut générer des trajectoires totalement chaotiques. Il a ainsi démontré l'un des premiers exemples de chaos déterministe.
1975	Tien-Yien Li et James A. Yorke ont été les premiers à utiliser le terme « chaos ».
1978	Mitchell Feigenbaum a découvert une constante universelle liée au chaos.

1990	Edward Ott, James A. Yorke et Celso Grebogi ont introduit le concept de contrôle du chaos. Pecora et Carroll ont travaillé sur la synchronisation des systèmes chaotiques.

Tableau 2.2: Historique de la théorie du chaos

2.2 Système chaotique

Dans cette section, nous procéderons à une définition des systèmes chaotiques en nous appuyant sur deux concepts fondamentaux : les systèmes dynamiques et les systèmes déterministes. Cette analyse nous permettra ensuite d'explorer les avantages potentiels que le chaos peut offrir dans divers contextes.

2.2.1 Définition

Les systèmes chaotiques sont des systèmes dynamiques déterministes dans lesquels de très petits changements dans les conditions initiales peuvent entraîner des écarts exponentiels dans l'évolution future du système. Cette sensibilité aux conditions initiales rend leur prédiction à long terme extrêmement difficile, voire impossible.

Paradoxalement, cette imprévisibilité intrinsèque des systèmes chaotiques est ce qui en fait des candidats intéressants pour des applications en cryptographie et transmission sécurisée de données. La synchronisation de deux systèmes chaotiques identiques, mais initiés avec des conditions légèrement différentes peut permettre de générer des séquences de données pseudoaléatoires utilisées pour le chiffrement.

Ainsi, les propriétés des systèmes dynamiques chaotiques, telles que la sensibilité aux conditions initiales et l'apparition d'attracteurs étranges, offrent de nouvelles possibilités pour résoudre des problèmes de sécurité de l'information, en complément des méthodes de cryptographie classiques.

2.2.1.1 Système dynamique

Un système dynamique est un modèle mathématique qui décrit l'évolution d'un phénomène en fonction du temps ou d'une autre variable. Il se caractérise par un ensemble d'équations, telles que les équations différentielles ou aux dérivées partielles, qui déterminent la trajectoire d'un objet ou d'un processus dans le temps. Ces systèmes sont composés de deux types de variables : dynamiques, qui changent avec le temps, et statiques, qui restent fixes. Leur

évolution peut être continue ou discrète, et suit un principe de causalité, où les événements passés ou présents déterminent l'évolution future du système, avec une condition initiale donnée conduisant à un seul état futur possible. Ces concepts s'appliquent à divers domaines tels que la physique, la chimie et la biologie.

2.2.1.2 Système déterministe

Un système est déterministe si, en connaissant son état à un instant donné, ainsi que les conditions initiales et les règles qui le régissent, on peut prédire avec précision son état futur. Cela signifie que, si les mêmes conditions se répètent, le système donnera toujours les mêmes résultats. Le déterminisme est donc opposé aux phénomènes aléatoires, où il est impossible de prédire avec certitude ce qui se passera.

Dans un système chaotique, même si l'évolution semble imprévisible et irrégulière, elle suit toujours des lois déterministes. Les mêmes causes produisent les mêmes effets. Cependant, une petite différence dans les conditions de départ peut provoquer des résultats très différents, ce qui rend difficile la prévision à long terme. Ainsi, même si le système est déterministe, il devient imprévisible en pratique à cause de cette sensibilité aux conditions initiales.

2.2.2 Avantages du chaos

En première approche, les systèmes chaotiques sont des systèmes dynamiques qui évoluent dans une région bornée, qui possèdent une infinité de trajectoires non périodiques denses [11]. Ce qui les rend particulièrement intéressants, c'est leur grande sensibilité aux conditions initiales : deux points de départ très proches peuvent entraîner des trajectoires qui divergent rapidement. Cette propriété permet de générer une infinité de signaux chaotiques à partir du même système en modifiant légèrement les conditions de départ. Ces signaux peuvent être utilisés pour créer des séries de nombres pseudo-aléatoires, très utiles dans des domaines comme la cryptographie ou les protocoles de communication tels que TCP/IP [12].

Une autre application des signaux chaotiques est de remplacer les séquences conventionnelles dans les systèmes de communication à spectre étalé. En raison de leur caractère imprévisible, ces signaux possèdent des propriétés spécifiques comme une faible corrélation croisée et des spectres de puissance proches du bruit blanc, ce qui les rend difficiles à intercepter. De plus, contrairement aux signaux sinusoïdaux classiques, qui concentrent leur puissance dans une bande étroite et peuvent causer des problèmes de synchronisation et d'interférence, les signaux chaotiques sont dispersés sur une large bande, ce qui réduit la densité

spectrale de puissance et diminue les risques d'interception. Ainsi, en utilisant des signaux chaotiques pour crypter les informations, on génère des signaux étalés sur une bande plus large, avec une densité de puissance inférieure à celle des solutions usuelles [13].

2.3 Classe des systèmes chaotiques

Les systèmes chaotiques se classent en deux grandes catégories : les systèmes chaotiques à temps continu et les systèmes chaotiques à temps discret.

➢ Systèmes chaotiques à temps continu

Ces systèmes sont décrits par des équations différentielles ordinaires qui modélisent l'évolution continue des variables d'état dans le temps. Les exemples les plus connus de systèmes chaotiques continus incluent :

- Le système de Lorenz : Un système tridimensionnel décrit par un ensemble d'équations différentielles, célèbre pour son attracteur en forme d'ailes de papillon.
- Le système de Rössler : Un autre système tridimensionnel, également décrit par des équations différentielles, caractérisé par ses trajectoires qui définissent un attracteur étrange aux propriétés fractales.

➢ Systèmes chaotiques à temps discret

Ces systèmes sont modélisés par des équations aux différences finies, qui définissent l'évolution du système à des intervalles de temps discrets. Parmi les systèmes chaotiques discrets, on retrouve :

- Le système de Hénon : Un système bidimensionnel introduit par Michel Hénon, caractérisé par des comportements chaotiques, intermittents ou périodiques selon les valeurs des paramètres.
- Le système Hénon-Heiles (ou Hénon modifié) : Un système tridimensionnel qui présente un comportement chaotique sous certaines conditions initiales et paramètres spécifiques.

2.4 Caractéristiques des systèmes chaotiques

Les systèmes chaotiques, se caractérisent par des comportements imprévisibles et complexes. Ces comportements peuvent être observés dans divers phénomènes physiques tels

que l'atmosphère terrestre, un robinet qui goutte ou encore un pendule soumis à des forces magnétiques [14]. Chacun de ces systèmes illustre la nature dynamique et non linéaire du chaos, qui se manifeste à travers des mouvements apparemment désordonnés mais pourtant régis par des lois déterministes. Plusieurs définitions du chaos ont été formulées, mettant en lumière différents aspects de ce concept. Cependant, elles convergent toutes vers certains points communs. Les caractéristiques suivantes permettent de mieux saisir les éléments clés qui définissent un système chaotique.

2.4.1 Aspect aléatoire

Les systèmes chaotiques présentent un comportement qui semble aléatoire et imprévisible à première vue. Cet aspect aléatoire résulte du fait qu'il est difficile, voire impossible, de donner une description exacte et mathématique de l'évolution temporelle du système. Cependant, cette imprévisibilité apparente ne doit pas être confondue avec le hasard pur. En réalité, le comportement chaotique est gouverné par des équations non-linéaires déterministes, telles que les équations de Newton lorsqu'elles régissent l'évolution de systèmes complexes comme celui de trois corps en interaction [15]. Bien que le système soit non périodique, ce qui signifie qu'il ne répète pas son comportement de manière régulière, il reste strictement déterministe. Ainsi, l'aspect aléatoire des systèmes chaotiques n'est qu'une manifestation de la complexité inhérente à ces systèmes, où des trajectoires très proches peuvent diverger rapidement, rendant toute prédiction à long terme extrêmement difficile. Les figures ci-dessous illustrent les aspects aléatoires de divers signaux issus de systèmes chaotiques continus et discrets [15].

Aspect aléatoire de l'état x du système de Lorenz :

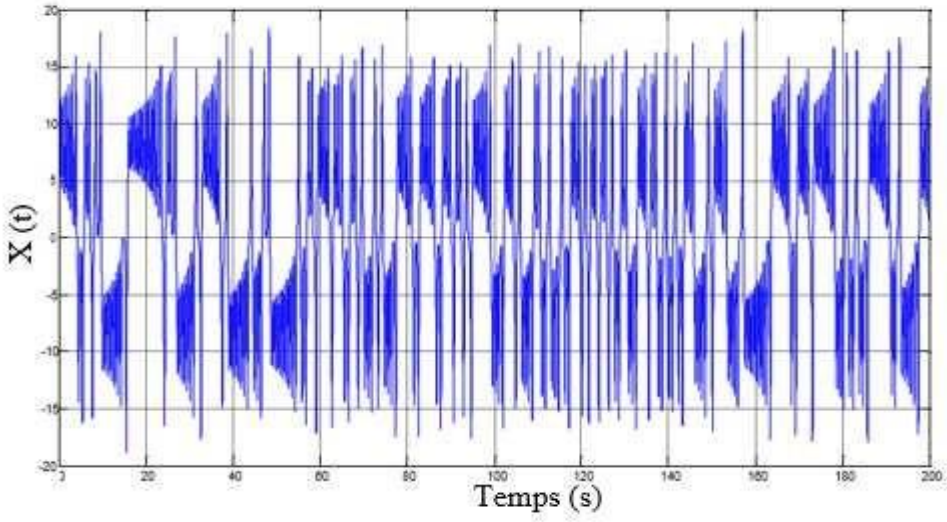

Figure 2.17: Aspect aléatoire de l'état x du système de Lorenz.

Aspect aléatoire de l'état x du système de Rössler :

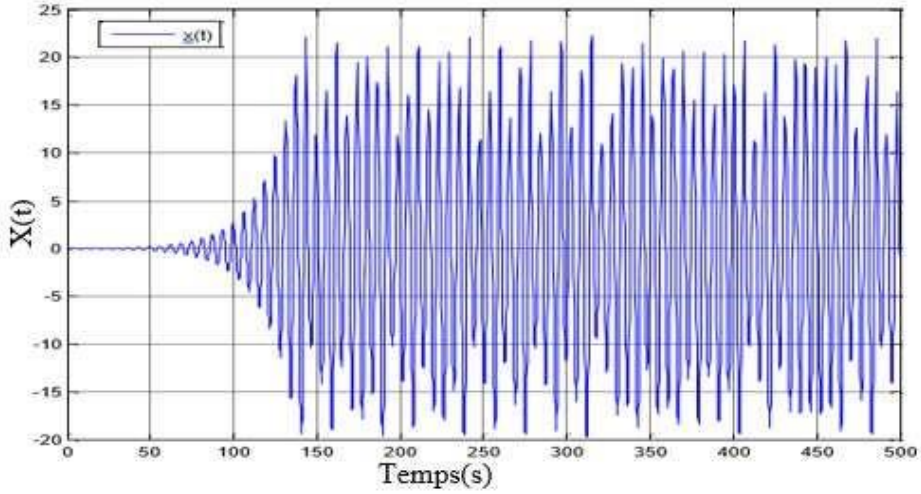

Figure 2.18: Aspect aléatoire de l'état x du système de Rössler.

Aspect aléatoire de l'état x du système de Hénon :

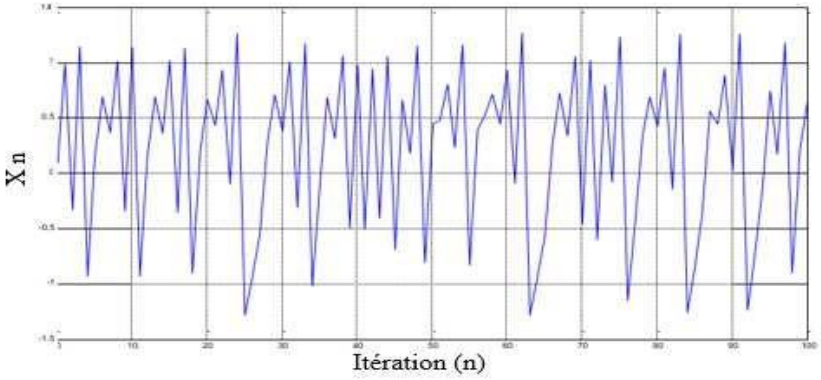

Figure 2.19: Aspect aléatoire de l'état x du système de Hénon.

Aspect aléatoire de l'état x du système de Hénon-Heiles :

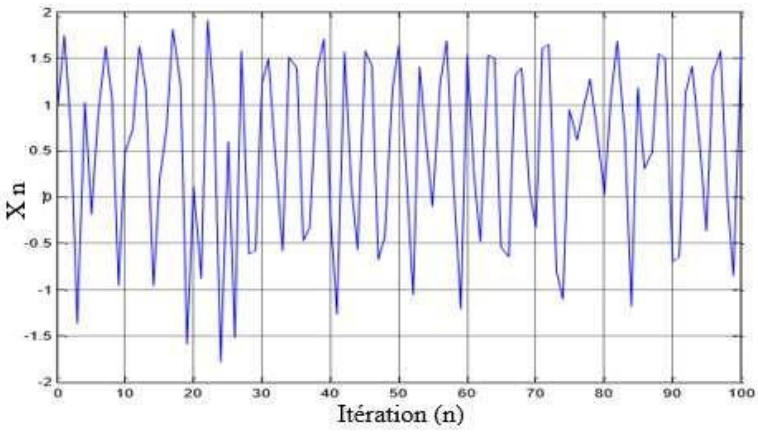

Figure 2.20: Aspect aléatoire de l'état x du système de Hénon modifié

2.4.2 Sensibilité aux conditions initiales

L'une des propriétés fondamentales des systèmes chaotiques est leur sensibilité extrême aux conditions initiales. Cela signifie que de petites variations dans l'état de départ peuvent entraîner des évolutions radicalement différentes au fil du temps. Ce phénomène a été mis en évidence par Edward Lorenz lorsqu'il étudiait les prévisions météorologiques. Il découvrit que même un léger changement dans les chiffres de départ de son modèle météorologique pouvait aboutir à des résultats complètement différents. Pour illustrer cette sensibilité, on peut se référer à l'« effet papillon », qui suggère qu'un battement d'ailes de papillon pourrait théoriquement provoquer une tornade à des milliers de kilomètres de distance. Cette illustration métaphorique démontre que même une modification infime, comme un battement d'ailes, pourrait entraîner des conditions météorologiques très différentes, telles qu'une tempête ou un calme plat [16]. Cela souligne un principe clé du chaos : de légères différences initiales peuvent provoquer des écarts considérables dans l'évolution du système. Les figures ci-dessous illustrent les sensibilités aux conditions initiales des différents systèmes chaotiques continus et discrets [15].

Sensibilité aux conditions initiales du système chaotique de Lorenz

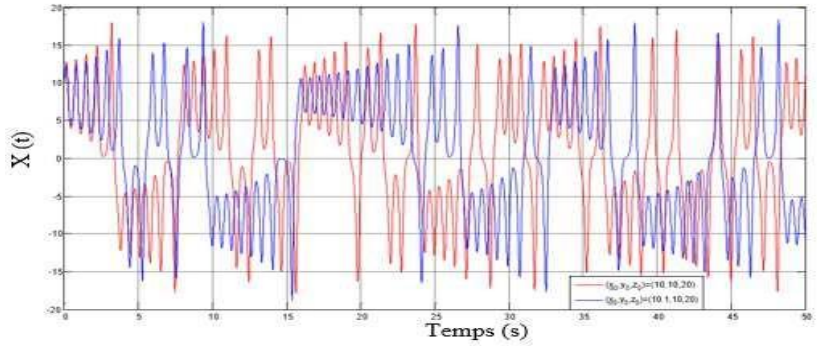

Figure 2.21: Sensibilité aux conditions initiales de l'état x du Système de Lorenz.

Sensibilité aux conditions initiales du système de Hénon modifié

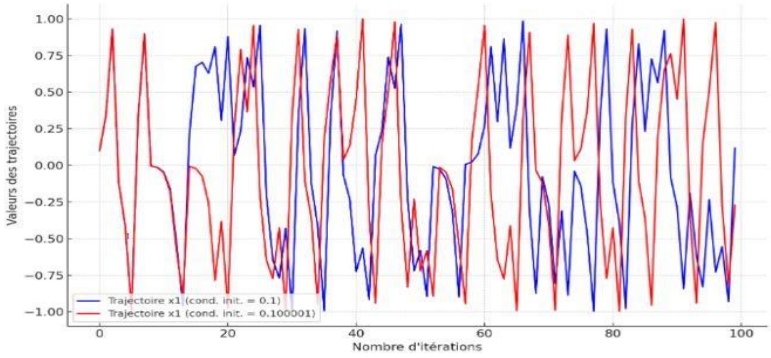

Figure 2.22: Sensibilité aux conditions initiales de l'état x Système de Hénon modifié.

2.4.3 L'Attracteur étrange

Dans un système dynamique, l'espace des phases représente tous les états possibles du système. Un attracteur est une région de cet espace où convergent les trajectoires, quelles que soient les conditions initiales. Il reflète l'état stable vers lequel évolue un système à long terme.

Dans les systèmes non chaotiques, on rencontre des attracteurs réguliers, tels que des points fixes (où le système atteint un état d'équilibre stable) ou des cycles limites (où le système suit une trajectoire périodique). Dans ces cas, les trajectoires évoluent de manière prévisible et restent proches les unes des autres, garantissant une stabilité à long terme.

Cependant, dans les systèmes chaotiques, les trajectoires sont beaucoup plus complexes et imprévisibles. Ici, on observe des attracteurs étranges, caractérisés par une structure fractale. Ces attracteurs étranges présentent des trajectoires irrégulières, qui s'étirent et se replient sans se croiser, mais restent confinées dans une région finie de l'espace des phases. Ils sont qualifiés d'étranges en raison de leur géométrie complexe : deux trajectoires proches peuvent diverger rapidement, même si elles restent attachées à la même région.

L'attracteur étrange est défini par :

- Bassin d'attraction : l'ensemble des points de départ qui mènent les trajectoires vers l'attracteur.
- Dimension fractale : contrairement aux attracteurs réguliers qui ont une dimension entière (comme un point ou un cercle), les attracteurs étranges ont une dimension non entière, reflétant leur structure infiniment complexe.

Un exemple célèbre est l'attracteur de Lorenz, représenté sous forme de papillon, qui symbolise la dynamique chaotique imprévisible mais contenue dans un espace défini.

- Attracteur de Lorenz

L'attracteur de Lorenz, issu d'un modèle simplifié de l'atmosphère, constitue un exemple emblématique du comportement chaotique. Ce modèle démontre que, bien que les trajectoires de systèmes initialement presque identiques semblent évoluer de manière imprévisible, elles convergent finalement vers une structure complexe, en l'occurrence une forme évoquant un papillon. Cet attracteur étrange illustre la complexité inhérente aux systèmes chaotiques, où un ordre sous-jacent émerge malgré l'apparente désorganisation des trajectoires. [17].

La figure ci-dessous représente l'attracteur de Lorenz [18] :

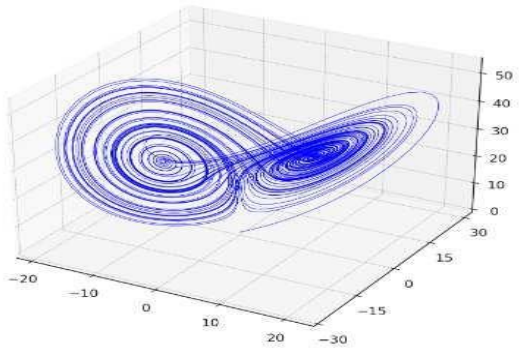

Figure 2.23 : Attracteur de Lorenz

2.4.4 Exposant de Lyapunov

L'exposant de Lyapunov, introduit par le mathématicien Alexander Lyapunov, est un indicateur clé pour mesurer la sensibilité aux conditions initiales dans un système dynamique. Il mesure la vitesse à laquelle de petites différences dans les conditions initiales s'amplifient au fil du temps, déterminant ainsi le taux de divergence ou de convergence des trajectoires dans l'espace des phases.

Pour qu'un système à n états soit qualifié de chaotique, au moins un exposant de Lyapunov doit être positif, indiquant une divergence exponentielle des trajectoires et un comportement chaotique. Si deux exposants ou plus sont positifs, le système est dit hyperchaotique, caractérisé par une divergence encore plus rapide. À l'inverse, si aucun exposant n'est positif, le système n'est pas chaotique. Le plus grand exposant est particulièrement important pour évaluer le degré de chaos.

Un système dynamique possède autant d'exposants de Lyapunov qu'il a de dimensions dans son espace des phases, chaque exposant correspondant à une direction dans cet espace :

- Un exposant positif signale une divergence exponentielle des trajectoires proches, caractéristique du chaos et de l'imprévisibilité à long terme.
- Un exposant négatif indique une convergence des trajectoires, traduisant une stabilité.
- Un exposant nul indique que les trajectoires restent parallèles, sans divergence ni convergence.

2.5 Bifurcation et route vers le chaos

Une bifurcation est un phénomène en dynamique des systèmes où un changement progressif dans un paramètre conduit à une modification qualitative du comportement du système, comme le passage d'un état stable à un état chaotique ou périodique. Le paramètre de bifurcation joue un rôle clé dans l'émergence du chaos au sein des systèmes dynamiques non linéaires. À travers les diagrammes de bifurcation, on peut observer comment le comportement d'un système évolue à mesure que ce paramètre change. Lorsque ce dernier franchit un seuil critique, les bifurcations deviennent de plus en plus rapprochées, ce qui conduit à l'apparition d'un comportement imprévisible, souvent décrit comme chaotique. Un exemple classique est la cascade de bifurcations de Feigenbaum, qui illustre comment un système périodique évolue progressivement vers un comportement chaotique. Chaque bifurcation introduit une nouvelle complexité, jusqu'à atteindre un régime chaotique. « Mitchell Feigenbaum a redécouvert une route vers le chaos qui avait été étudiée dans les années 1960 par Myrberg. Aujourd'hui, cette route est appelée « cascade de doublements de période » pour décrire la transition entre un comportement périodique et un comportement chaotique. » [19]

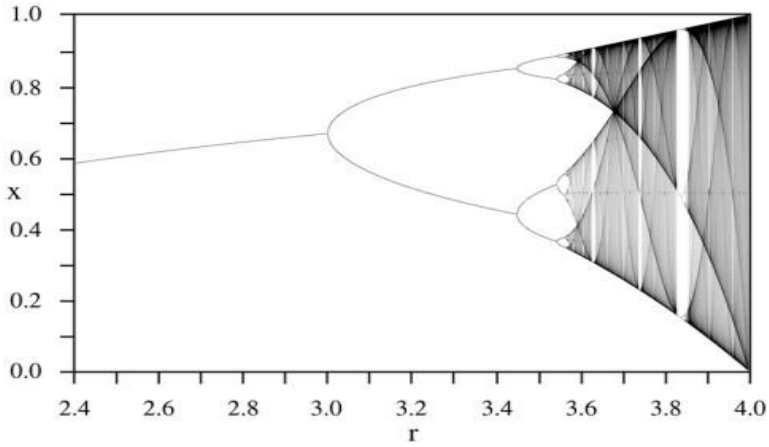

Figure 2.24 : Bifurcation vers le chaos par doublement de période.

On distingue généralement trois scénarios théoriques d'évolution vers le chaos, qui permettent de classer certains phénomènes expérimentaux comme étant chaotiques déterministes.

Le premier scénario est celui du doublement de période. Lorsqu'on augmente un paramètre dans un système initialement périodique, on observe un doublement progressif du nombre de période : elle passe de 2 à 4, puis à 8, 16, et ainsi de suite. À partir d'une certaine valeur du paramètre, ces doublements de périodes se rapprochent de plus en plus, jusqu'à

atteindre un point où la fréquence devient théoriquement infinie. C'est à ce point précis que le chaos apparaît, rendant les prédictions impossibles au-delà de ce seuil critique. À partir de la **Figure 2.24** nous pouvons constater les caractéristiques suivantes [20] :

- Pour $0< r < 3$, le système converge vers un point fixe attractif, où les valeurs de $_n$ se stabilisent.
- Pour $3 < r < 3{,}57$, le système présente un attracteur périodique. Cela se traduit par des cycles qui se divisent, donnant lieu à des bifurcations.
- Au-delà de $r = 3{,}57$, l'attracteur devient chaotique. L'image montre alors une complexité croissante avec des trajectoires qui semblent aléatoires, marquant le passage vers un régime chaotique.

Le deuxième scénario est celui de l'intermittence. Ici, le système alterne entre des phases régulières et des épisodes de chaos. Prenons l'exemple d'un flux de circulation qui reste stable pendant un certain temps, avant qu'un changement brusque ne provoque des embouteillages imprévisibles. Dans un système physique, cela pourrait se traduire par des oscillations régulières soudainement perturbées par des phases chaotiques. À mesure que le paramètre continue de s'éloigner de la valeur critique, les épisodes de chaos deviennent plus fréquents et de plus longue durée, jusqu'à éventuellement dominer complètement le comportement du système. [21]

Le troisième scénario est celui de la quasi-périodicité. Dans ce cas, une nouvelle période, indépendante de la première, apparaît dans le système. Si le rapport entre ces deux périodes est irrationnel, leur superposition crée une évolution vers un comportement chaotique. Imaginez une roue qui tourne avec deux rythmes différents et non synchronisés ; cette désynchronisation finit par créer un mouvement imprévisible, proche du chaos. C'est un phénomène que l'on peut observer dans certains systèmes mécaniques complexes ou dans les interactions entre différents cycles naturels, comme les marées et les saisons. [22]

Ces trois scénarios, qu'ils soient étudiés théoriquement ou observés dans des expériences, fournissent un cadre de référence pour comprendre les mécanismes qui mènent à l'apparition du chaos dans des systèmes dynamiques.

2.6 Exemples des systèmes chaotiques

Les systèmes chaotiques sont caractérisés par leur sensibilité aux conditions initiales, leur imprévisibilité à long terme, et leur dynamique complexe. Pour illustrer ces concepts, deux

modèles chaotiques bien connus sont étudiés dans cette section : le système de Lorenz et le système de Hénon modifié. Ces systèmes représentent des exemples clés de la théorie du chaos et ont des applications dans de nombreux domaines.

2.6.1 Le système de Lorenz

Dans cette partie, nous aborderons les équations de Lorenz, leur sensibilité aux conditions initiales, l'attracteur de Lorenz, ainsi que leurs applications concrètes.

2.6.1.1 Définition et présentation des équations de Lorenz

Le système de Lorenz, découvert en 1963 par le météorologue Edward N. Lorenz, a radicalement changé notre compréhension des systèmes dynamiques en introduisant le concept de chaos déterministe. À l'origine, Lorenz cherchait à simuler les mouvements atmosphériques avec un modèle simple, mais il a rapidement constaté qu'un minuscule changement dans les conditions initiales pouvait entraîner des divergences considérables dans l'évolution du système [23]. Ce qui distingue le système de Lorenz, c'est son applicabilité bien au-delà de la météorologie. Il s'est révélé pertinent dans des domaines variés tels que la physique, l'ingénierie, la biologie et la finance. Sa capacité à illustrer des comportements imprévisibles dans des systèmes régis par des lois précises en fait un modèle essentiel pour ceux qui cherchent à comprendre la complexité du monde qui nous entoure.

Le système de Lorenz est basé sur un ensemble de trois équations différentielles non linéaires interconnectées. Ces équations modélisent les mouvements d'un fluide soumis à un gradient de température (comme l'air dans l'atmosphère), où les variables x , y et z représentent respectivement la vitesse du fluide, la différence de température entre le haut et le bas du fluide, et la distorsion verticale du fluide [24].

Les équations de Lorenz sont les suivantes :

$$\frac{dx}{dy} = \sigma(y - x)$$

$$\frac{dy}{dt} = x(\rho - z) - y \qquad \textbf{2.1}$$

$$\frac{dz}{dt} = xy - \beta z$$

Où :

- σ (Sigma) est le nombre de Prandtl, mesurant la viscosité relative à la conductivité thermique.
- ρ (Rho) est le nombre de Rayleigh, qui décrit la différence de température.
- β (Beta) est un paramètre lié à la géométrie du système.

2.6.1.2 Sensibilité aux conditions initiales et l'effet papillon

L'un des aspects marquants du système de Lorenz réside dans sa sensibilité aux conditions initiales. De minuscules différences dans les valeurs de départ peuvent entraîner des trajectoires complètement différentes à long terme. Lorenz a fait cette découverte par hasard, lorsqu'il a recalculé une prévision météorologique en modifiant légèrement une valeur initiale, ce qui a conduit à des résultats radicalement différents. Ce comportement est bien illustré dans la **figure 2.21**, qui montre la sensibilité aux conditions initiales dans le cadre du système de Lorenz.

Ce phénomène, désormais connu sous le nom d'« effet papillon », en référence à l'idée qu'un simple battement d'ailes de papillon à un endroit du monde pourrait, en théorie, provoquer une tempête à l'autre bout du globe, illustre parfaitement l'imprévisibilité des systèmes chaotiques, bien qu'ils soient régis par des lois déterministes [25].

2.6.1.3 L'attracteur De Lorenz

L'attracteur de Lorenz est un système dynamique non linéaire en temps continu tridimensionnel. La **figure 2.23** illustre cet attracteur à partir des conditions initiales $x_0 = y_0 = z_0 = 0.01$, avec un pas de simulation de 0.01. À travers l'analyse de cet attracteur, on observe que la trajectoire présente deux comportements distincts. D'une part, elle semble régulière, formant des boucles similaires à des trajectoires périodiques dans certaines régions de l'espace d'état. D'autre part, elle révèle un comportement aléatoire, où le nombre de boucles dans une région avant de passer brusquement à une autre est imprévisible, tout comme les moments de ces transitions [14].

L'attracteur de Lorenz, en tant que structure fractale, illustre la complexité des systèmes chaotiques. Contrairement à une trajectoire fixe ou périodique, celle-ci ne se répète jamais exactement, mais reste confinée dans une zone limitée. Cela met en lumière la capacité des trajectoires à évoluer de manière imprévisible tout en demeurant à l'intérieur d'une région

définie de l'espace des phases. La visualisation de cet attracteur permet de mieux comprendre cette dynamique complexe.

2.6.1.4 Applications concrètes du système de Lorenz

Le système de Lorenz a des applications variées, notamment dans [28] :

- La météorologie : L'effet papillon montre pourquoi il est impossible de prévoir le temps avec précision sur le long terme. De très petites erreurs dans les conditions initiales peuvent se multiplier et rendre les prévisions incertaines.
- Les circuits électroniques : Les systèmes chaotiques comme celui de Lorenz sont utilisés dans des oscillateurs chaotiques pour générer des signaux pseudoaléatoires, notamment en cryptographie et dans les communications sécurisées.
- La biologie : Les principes du chaos aident à comprendre des systèmes biologiques complexes, comme la dynamique des populations animales, et à expliquer certains comportements imprévisibles.

2.6.2 Système de Hénon Modifié

Dans cette partie, nous explorerons le système de Hénon modifié, sa sensibilité aux conditions initiales, son attracteur étrange, ainsi que le diagramme de bifurcation et les applications concrètes de ce système.

2.6.2.1 Définition et Présentation du Système de Hénon Modifié

Le système de Hénon modifié est une adaptation du modèle original développé par Michel Hénon en 1976, qui visait à représenter un système dynamique chaotique de manière simplifiée. Ce modèle discret en deux dimensions est largement utilisé pour étudier les phénomènes chaotiques, notamment dans le cadre de la théorie du chaos et de la dynamique non linéaire.

Dans sa version modifiée, certains paramètres ou termes supplémentaires ont été introduits pour altérer son comportement d'origine, permettant ainsi d'explorer des régimes dynamiques différents. Par exemple, en ajustant ces paramètres, il est possible de passer d'un comportement chaotique à des comportements plus stables ou quasi-périodiques, selon l'objectif de l'étude. Cela permet aux chercheurs de mieux comprendre la transition entre l'ordre et le chaos dans des systèmes complexes.

Cette flexibilité rend le système de Hénon modifié particulièrement intéressant pour l'étude de phénomènes complexes dans des domaines tels que la météorologie, l'astrophysique, ou encore l'économie, où des comportements dynamiques imprévisibles peuvent émerger à partir de règles simples. En conservant les propriétés non linéaires du modèle original, tout en ajoutant la possibilité d'introduire de nouvelles variables, cette version modifiée élargit considérablement les horizons de la recherche sur les systèmes dynamiques.

Le système de Hénon modifié est décrit par les équations suivantes [27] :

$$\begin{cases} x_1(k+1) = a - x_2^2(k) - bx_3(k) \\ x_2(k+1) = x_1(k) \\ x_3(k+1) = x_2(k) \end{cases} \quad \textbf{2.2}$$

Tel que :

x_1, x_2, x_3 représentent les états du système à chaque instant k, où k est l'indice temporel discret correspondant à chaque étape de l'évolution du système, et a et b sont les paramètres du système qui contrôlent le comportement dynamique.

2.6.2.2 Sensibilité aux conditions initiales du système de Hénon modifié

Le système de Hénon modifié est particulièrement connu pour sa sensibilité aux conditions initiales, une propriété caractéristique des systèmes chaotiques. En termes simples, cela signifie que des variations infimes dans les conditions de départ peuvent entraîner des différences radicales dans les trajectoires à long terme.

Cette sensibilité est bien illustrée par la **figure 2.22**, qui montre comment deux trajectoires, initialement très proches, divergent rapidement au fil du temps. Même si les différences entre les conditions initiales sont minimes, leurs évolutions respectives finissent par suivre des chemins totalement distincts, démontrant à quel point le système est imprévisible à long terme.

2.6.2.3 L'Attracteur étrange du système de Hénon modifié

L'attracteur d'un système de Hénon modifié révèle la dynamique complexe du système dans l'espace des phases. La structure observée, fractale et tridimensionnelle, est typique des systèmes chaotiques montre comment les trajectoires se regroupent en zones de densité

variable, reflétant la sensibilité du système aux conditions initiales et sa nature non linéaire. En dépit de l'imprévisibilité apparente à court terme, l'attractrice capture l'évolution asymptotique des trajectoires, donnant un aperçu du comportement à long terme du système. Cette dynamique est illustrée dans la **figure 2.25** [28], qui met en évidence ces regroupements de trajectoires dans l'espace des phases.

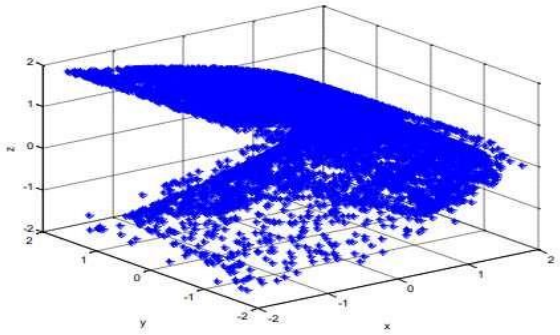

Figure 2.25: Attracteur étrange de Hénon modifié

2.6.2.4 Diagramme de bifurcation pour le système de Hénon modifié

Le système de Hénon modifié et ses variantes montrent, à travers leur diagramme de bifurcation, l'évolution du comportement dynamique en fonction du paramètre a.

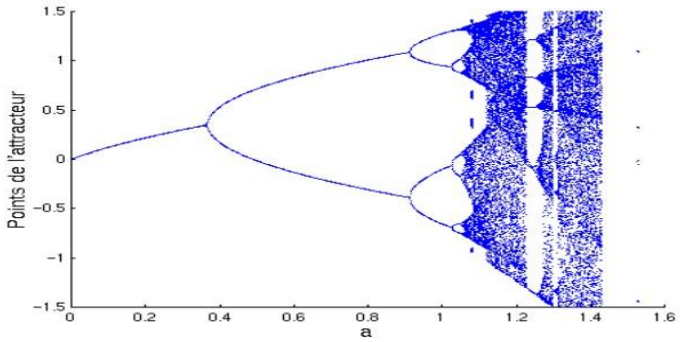

Figure 2.26 : Diagramme de bifurcation pour le système de Hénon modifié

Pour des valeurs de « a » comprises entre 0 et 0.8, le système converge vers une valeur unique, correspondant à un cycle limite de période 1. Autrement dit, quel que soit l'état initial, le système finit par osciller autour d'un point stable.

Entre 0.8 et 1.1, un dédoublement de période se produit, et le système commence à osciller entre deux valeurs distinctes, marquant une première bifurcation qui divise la solution stable en deux points.

Dans l'intervalle 1.1 à 1.3, le système montre des bifurcations successives, avec des oscillations de périodes de plus en plus complexes. La période s'allonge, et le nombre de points d'oscillation croît rapidement, rendant les trajectoires du système plus compliquées.

Lorsque « a » dépasse 1.3 et jusqu'à environ 1.4, le système entre dans une phase chaotique. À ce stade, les oscillations deviennent imprévisibles et très sensibles aux conditions initiales, un trait distinctif des systèmes chaotiques.

Le diagramme de bifurcation du système de Hénon modifié permet d'observer ces transitions. À mesure que « a » augmente, les branches du diagramme se multiplient, illustrant le passage d'un comportement régulier à des oscillations complexes, puis au chaos. Ce diagramme détaille ainsi la progression du système, passant d'un état stable à des oscillations de périodes multiples, pour finalement entrer dans un régime chaotique caractérisé par des comportements désordonnés et imprévisibles. [28].

2.6.2.5 Applications concrètes du système Hénon modifié

Le système de Hénon modifié et ses variantes ont des applications concrètes dans plusieurs domaines, notamment en raison de ses propriétés chaotiques. Voici quelques exemples d'applications [29] :

- Génération de nombres pseudo-aléatoires pour la cryptographie : Le système chaotique de Hénon modifié est utilisé pour concevoir des générateurs de nombres pseudoaléatoires. Ces générateurs sont essentiels dans les systèmes de cryptographie modernes pour assurer la sécurité des communications. Grâce à la sensibilité aux conditions initiales du système chaotique, il devient difficile pour un attaquant de prédire ou reproduire la séquence de nombres, ce qui renforce la sécurité cryptographique.
- Compression et cryptage d'images : Les systèmes chaotiques, y compris celui de Hénon modifié, sont exploités dans des algorithmes de cryptage et de compression d'images. L'idée est d'utiliser les propriétés chaotiques pour transformer les données d'une image de manière réversible et sécurisée, rendant plus difficile l'accès aux informations visuelles non autorisées. Ces techniques sont notamment utilisées dans les systèmes de communication sécurisés et les applications militaires.

- Modélisation de la dynamique des systèmes biologiques : Le système de Hénon modifié peut être appliqué à la modélisation de la dynamique dans des systèmes biologiques complexes, tels que la croissance des populations ou la propagation d'épidémies. Sa capacité à représenter des comportements dynamiques complexes et non linéaires le rend utile pour simuler des interactions dans des environnements biologiques où des facteurs chaotiques influencent les résultats.

Conclusion

Ce chapitre a mis en lumière la manière dont les systèmes chaotiques, par leur imprévisibilité et leur sensibilité aux conditions initiales, constituent un cadre idéal pour les applications en cryptographie. Les concepts abordés, tels que les exposants de Lyapunov et les attracteurs étranges, illustrent la capacité de ces systèmes à générer des séquences aléatoires, essentielles pour le cryptage. En outre, des exemples concrets comme les systèmes de Lorenz et de Hénon modifié montrent l'efficacité de ces modèles dans le domaine de la sécurité des communications. Ces bases théoriques serviront d'introduction au chapitre suivant, où nous examinerons plus en détail l'utilisation de la cryptographie pour sécuriser les échanges de données.

CHAPITRE 3

Généralités sur le cryptage

Introduction

Le cryptage est essentiel pour protéger les informations dans un contexte de cyberattaques croissantes. Dans ce chapitre, nous explorons les fondements de la cryptologie, en distinguant la cryptographie (protection des données) de la cryptanalyse (décryptage). Nous présentons ensuite les objectifs de la cryptographie : confidentialité, intégrité, authentification et non répudiation, garantissant la sécurité des échanges d'informations. Enfin, nous détaillons les méthodes de cryptage classiques, modernes et chaotiques et abordons la synchronisation des systèmes chaotiques, en en examinant le principe, les modes, les types et les méthodes.

3.1 Notions sur le cryptage

3.1.1. Définition de la cryptologie

La cryptologie est la science qui étudie les moyens de protéger la confidentialité et la (science). « Cryptologie » signifie littéralement science du secret et a pour objet de cacher les informations d'un message [30]. La cryptologie se divise principalement en deux domaines : la cryptographie et la cryptanalyse.

Bien que ses origines remontent à l'Antiquité, avec des exemples historiques tels que le code de César ou le code Atbash, la cryptologie n'est véritablement devenue une science étudiée à part entière qu'à partir des années 1970. Elle est donc considérée comme une science relativement émergente. Aujourd'hui, la cryptologie joue un rôle essentiel dans la protection des données sensibles, que ce soit dans un contexte militaire, gouvernemental ou commercial.

3.1.2 Définition de la cryptographie

La cryptographie est l'une des principales branches de la cryptologie, la science du secret. Elle a pour but de protéger la confidentialité, l'authenticité et l'intégrité des informations en les chiffrant à l'aide de techniques mathématiques et informatiques. Larousse donne la définition suivante : « Ensemble des techniques de chiffrement qui assurent l'inviolabilité de textes et, en informatique, de données. » [31]

L'objectif de la cryptographie est de rendre les messages incompréhensibles pour toute personne non autorisée, de sorte que seul le destinataire légitime puisse les déchiffrer et en prendre connaissance.

3.1.3 Définition de la cryptanalyse

Alors que la cryptographie vise à protéger les informations en les chiffrant, la cryptanalyse s'attache à décoder et analyser les messages chiffrés pour en extraire le contenu original. La cryptanalyse, ou l'attaque sur un chiffrement, englobe les méthodes utilisées pour attaquer un crypto-système. Elle est essentielle pour évaluer la sécurité des techniques de chiffrement employées en cryptographie. Son objectif principal est de trouver un algorithme permettant de déchiffrer les messages, souvent en essayant de reconstituer la clé secrète de déchiffrement. Selon Larousse, c'est « l'ensemble des techniques mises en œuvre pour tenter de déchiffrer un message codé dont on ne connaît pas la clé. » [32]

3.2 Objectifs de la cryptographie

Lorsque l'on parle de "sécuriser un échange", on met en lumière trois services essentiels :

la confidentialité, l'intégrité et l'authentification [33].

- **La confidentialité :** La confidentialité des informations échangées assure que seules les personnes autorisées y ont accès. Cela nécessite le cryptage des données pour qu'elles ne soient compréhensibles que par les destinataires légitimes, tout en permettant au récepteur de vérifier leur origine et d'empêcher toute usurpation d'identité.
- **L'intégrité :** Garantit que le message n'a pas été altéré lors de sa transmission. Les fonctions de hachage sont utilisées pour vérifier cela, permettant au récepteur de s'assurer que le message reçu est identique à celui envoyé par l'émetteur, empêchant ainsi toute substitution frauduleuse par une tierce personne.
- **L'authentification :** Assure que l'émetteur d'un message est bien identifié, évitant ainsi toute usurpation d'identité. Cela permet au récepteur de vérifier que la communication provient de la source prévue et non d'un tiers malveillant. Pour ce faire, diverses techniques telles que les signatures numériques et les certificats sont utilisées pour valider l'identité des parties impliquées.
- **La non-répudiation :** La non-répudiation de l'information est la garantie qu'aucun des correspondants ne pourra nier la transaction. [34]

3.3 Les méthodes de cryptographie

3.3.1 Cryptographie classique

La cryptographie n'est pas uniquement une technique moderne ni un produit de l'ère informatique. Depuis toujours, les hommes ont ressenti le besoin de dissimuler des informations confidentielles. Bien sûr, la cryptographie a beaucoup évolué depuis ses débuts. Au fil des siècles, de nombreux systèmes de chiffrement ont été inventés, devenant de plus en plus sophistiqués, et l'ère informatique a largement contribué à cette évolution. Cependant, les premiers algorithmes étaient loin d'être aussi complexes et ingénieux que ceux d'aujourd'hui. La cryptographie classique, qui décrit la période avant les ordinateurs, reposait sur des méthodes comme la substitution et la transposition. Ces techniques consistaient à remplacer des caractères par d'autres et à les permuter dans des ordres différents, tout en gardant secrètes les procédures de chiffrement et de déchiffrement. Sans cette confidentialité des méthodes, le système devenait complètement inefficace, puisque n'importe qui pouvait alors déchiffrer le message codé.

3.3.1.1 Système de césar

Le chiffrement de César est une méthode de cryptographie par décalage alphabétique, inventée par l'empereur romain Jules César au 1er siècle avant J.C. Son principe consiste à décaler les lettres de l'alphabet d'un nombre fixe de positions, par exemple pour un décalage de 3, A devient D, B devient E, et ainsi de suite [35]. Ce système simple et facile à mettre en œuvre a été utilisé par l'armée romaine pour sécuriser les communications pendant les batailles.

Bien que très basique, le chiffre de César a été largement employé dans l'Antiquité et même réutilisé à des périodes plus récentes, comme pendant la guerre de Sécession et par l'armée russe en 1915 [36]. Cependant, sa simplicité facilite également sa cryptanalyse. Il existe seulement 26 façons possibles de chiffrer un message, correspondant au nombre de lettres de l'alphabet, ce qui rend ce système vulnérable aux attaques par force brute.

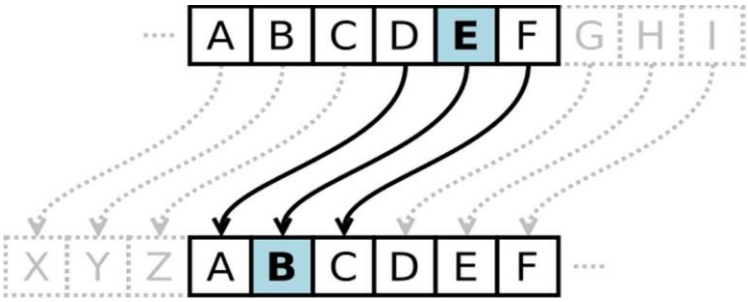

Figure 3.23: Chiffrement par substitution

De plus, le chiffre de César ne masque pas les fréquences d'apparition des lettres, ce qui permet aux techniques de cryptanalyse fréquentielle d'identifier facilement les lettres les plus courantes et de casser le code. Une version moderne de ce système, connue sous le nom de ROT13, décale les lettres de 13 positions et est utilisée sur certains forums Internet pour empêcher la lecture involontaire de textes. Le ROT13 n'a pas pour but de sécuriser les communications mais de les rendre temporairement illisibles.

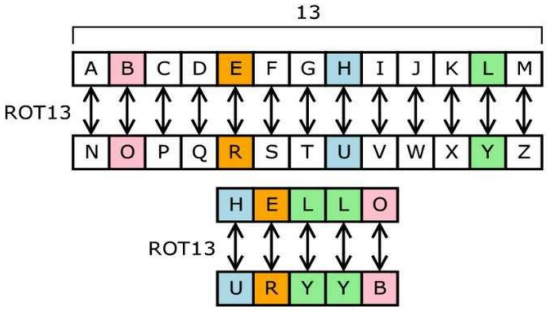

Figure 3.24: Un exemple du ROT13

Le chiffrement de César est l'un des systèmes de cryptographie les plus anciens et les plus simples, basé sur la substitution mono-alphabétique. Malgré son utilisation historique, il présente de nombreuses faiblesses qui le rendent inadapté aux besoins de sécurité modernes.

3.3.1.2 Système de Vigenère

Le chiffre de Vigenère, créé par le diplomate français Blaise de Vigenère en 1586, est un système de chiffrement polyalphabétique qui représente une amélioration significative par rapport au chiffre de César. Contrairement à ce dernier, où le décalage est constant pour toutes les lettres, le chiffre de Vigenère utilise un décalage variable qui change de lettre en lettre. Pour ce faire, il se base sur une table appelée carré de Vigenère, composée de 26 lignes et 26 colonnes, chacune représentant une substitution différente.

L'utilisation du chiffre de Vigenère implique l'utilisation d'une clé qui se répète sur la longueur du message à chiffrer. À chaque lettre du message, un décalage spécifique est appliqué en fonction de la lettre correspondante dans la clé. Ce processus rend le message beaucoup plus difficile à déchiffrer que le simple chiffre de César, car il offre une plus grande sécurité grâce à l'utilisation de multiples alphabets de substitution.

Pour chiffrer un message, on place la clé au-dessus du texte à chiffrer, lettre par lettre, et on trouve la lettre chiffrée en croisant la ligne correspondant à la lettre de la clé avec la

colonne correspondant à la lettre du texte. Ce processus est répété pour chaque lettre du message jusqu'à ce que tout le texte soit chiffré.

La principale force du chiffre de Vigenère réside dans sa capacité à offrir des méthodes de codage et de décodage simples à appliquer. De plus, il permet de coder la même lettre de différentes manières, ce qui rend plus difficile toute tentative de cryptanalyse fréquentielle. Cependant, si la longueur du message à chiffrer dépasse considérablement celle de la clé, il devient possible de repérer la longueur de la clé dans le message, ce qui peut faciliter la cryptanalyse. Ainsi, il est recommandé d'utiliser une clé se rapprochant autant que possible de la longueur du message pour garantir la sécurité du chiffrement et rendre le message indéchiffrable.

La figure ci-dessous illustre Grille de chiffrement du code de Vigenère [37] :

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 3.25: Grille de chiffrement du code de Vigenère

3.3.1.3 Système de Playfair

Le code de Playfair est une méthode de chiffrement par substitution polygraphique, inventée en 1854 par Sir Charles Wheatstone et popularisée par le baron Lyon Playfair [38]. Contrairement aux systèmes de chiffrement traditionnels qui chiffrent des caractères individuels, le code de Playfair chiffre des paires de lettres, appelées digrammes, ce qui complique l'analyse de fréquence utilisée pour le décryptage.

Pour utiliser le code de Playfair, on crée une grille de 5x5 lettres à partir d'une clé, en incluant toutes les lettres de l'alphabet à l'exception d'une (souvent 'J', qui est fusionnée avec 'I'). Le texte à chiffrer est préparé en remplaçant 'J'par 'I', en ajoutant une lettre convenue (souvent 'X' ou 'Y') entre les lettres identiques, et en ajoutant une lettre à la fin si le nombre de lettres est impair.

Dans le chiffrement de Playfair, chaque paire de caractères $m1m2$ message est chiffrée selon les trois règles suivantes, basées sur la position de $m1m2$ dans la matrice :

- **Même ligne** : Si les deux lettres sont sur la même ligne de la grille, chaque lettre est remplacée par celle immédiatement à sa droite, en circulant de la fin au début de la ligne si nécessaire.
- **Même colonne** : Si les deux lettres sont sur la même colonne de la grille, chaque lettre est remplacée par celle immédiatement en dessous, en circulant du bas vers le haut de la colonne si nécessaire.
- **Rectangle** : Si les lettres forment un rectangle, chaque lettre est remplacée par la lettre se trouvant sur la même ligne mais dans la colonne de l'autre lettre de la paire.

Le code de Playfair a été utilisé à des fins tactiques pendant la Première Guerre mondiale et par les forces britanniques lors de la deuxième guerre des Boers, ainsi que par les Australiens pendant la Seconde Guerre mondiale, en raison de sa rapidité d'utilisation et de l'absence de nécessité d'équipement particulier. Cependant, il peut être déchiffré par analyse des digrammes les plus fréquents du texte chiffré, ce qui en limite la sécurité.

3.3.2 Cryptographie moderne

Avec le développement des ordinateurs, les techniques de cryptographie ont considérablement évolué, rendant obsolètes les méthodes de cryptage manuel. Les procédés de substitution et de transposition restent toutefois d'actualité, mais sont désormais appliqués à des séquences de bits puisque les ordinateurs manipulent des données numériques. Cela a rendu les techniques de chiffrement modernes beaucoup plus sûres, certaines étant même considérées comme pratiquement incassables, nécessitant des millions d'années pour être déchiffrées par les meilleurs supercalculateurs actuels.

Une différence majeure dans la cryptographie moderne est que les algorithmes ne sont plus secrets ; ils sont connus de tous. La sécurité repose uniquement sur les clés utilisées. La cryptographie moderne se divise en deux branches principales :

- Cryptographie à clé secrète (ou symétrique)
- Cryptographie à clé publique (ou asymétrique)

Les méthodes modernes, bien que plus complexes, reposent sur la même philosophie que les anciennes méthodes. Cependant, elles manipulent directement des bits au lieu des caractères

alphabétiques. Ce changement de taille de données - de 26 lettres de l'alphabet à deux éléments binaires - permet des combinaisons plus robustes de substitutions et de transpositions. Les règles de ces systèmes, connues de tous selon le principe de Kerckhoffs, reposent sur le concept des clés.

Aujourd'hui, la cryptographie moderne est une discipline scientifique essentielle pour sécuriser les communications, authentifier les utilisateurs et protéger l'intégrité des données, notamment dans le cloud computing. Elle continue d'évoluer pour répondre aux défis de sécurité dans le monde numérique, s'appuyant sur des techniques mathématiques avancées. En résumé, la cryptographie moderne est une science dynamique et en perpétuelle évolution, indispensable pour garantir la sécurité dans l'ère numérique.

3.3.2.1 Cryptographie symétrique

Le cryptage symétrique, également connu sous le nom de cryptage à clé secrète ou cryptage à clé privée, est la forme de chiffrement la plus ancienne et la plus répandue [39]. Il repose sur l'utilisation d'une seule clé partagée entre les deux parties communicantes. Cette clé unique sert à la fois à chiffrer le message en texte clair et à déchiffrer le message chiffré.

Les algorithmes de chiffrement symétrique les plus connus incluent Kerberos et le Data Encryption Standard (DES). Ces algorithmes reposent sur des opérations mathématiques de permutation et de substitution pour transformer le texte d'origine en un texte chiffré illisible sans la clé.

Le cryptage symétrique est largement utilisé dans de nombreuses applications informatiques, telles que le chiffrement de fichiers, de partitions, ou de communications en ligne sécurisées. Il est particulièrement apprécié pour sa rapidité et sa simplicité d'implémentation sur divers matériels, ce qui le rend adapté à une utilisation sur des réseaux Internet filaires et mobiles.

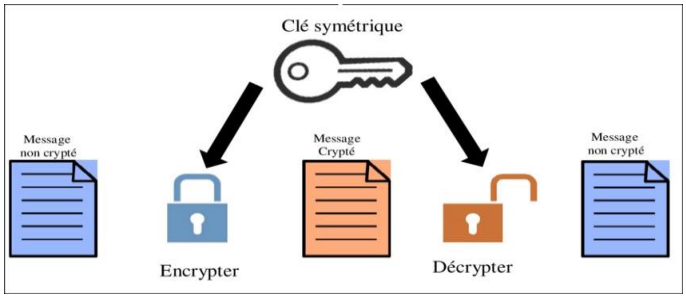

Figure 3.26: Cryptage symétrique

Cependant, un défi majeur du cryptage symétrique réside dans la gestion de la clé secrète. Étant donné que la même clé est utilisée pour chiffrer et déchiffrer les données, les parties doivent se mettre d'accord sur cette clé et la partager de manière sécurisée. La transmission sécurisée de cette clé est cruciale, car la sécurité de l'algorithme dépend entièrement de la clé. Si la clé est compromise, le message peut être facilement déchiffré par un tiers non autorisé.

De plus, la gestion des clés devient rapidement impraticable à grande échelle. Pour n participants à la communication, il faudrait n (n-1)/2 clés secrètes différentes, ce qui complique la gestion et le stockage sécurisé de ces clés. Pour résoudre ce problème, la cryptographie asymétrique est souvent utilisée en complément pour sécuriser l'échange initial de clés.

Il existe deux principales catégories de chiffrement symétrique : le chiffrement par blocs et le chiffrement de flux. Le chiffrement par blocs divise le texte en blocs de taille fixe et applique le chiffrement à chaque bloc individuellement. En revanche, le chiffrement de flux chiffre les données en continu, bit par bit ou caractère par caractère.

3.3.2.2 Cryptographie asymétrique

Le cryptage asymétrique, également appelé cryptage à clé publique, se distingue du cryptage symétrique par l'utilisation de deux clés différentes : une clé publique, partagée avec tous les correspondants, et une clé privée, connue uniquement du destinataire. La clé publique est utilisée pour chiffrer les messages, tandis que la clé privée permet de les déchiffrer.

Contrairement au cryptage symétrique, qui nécessite un échange préalable de la clé secrète, le cryptage asymétrique permet de s'affranchir de cette contrainte [40][4l], rendant ainsi les communications plus pratiques entre des parties qui ne se connaissent pas. Cette méthode a été présentée pour la première fois en 1976 par Whitfield Diffie et Martin Hellman [42], et le premier cryptosystème à clé publique, RSA, a été développé en 1978 par Ronald Rivest, Adi Shamir et Leonard Adleman [43].

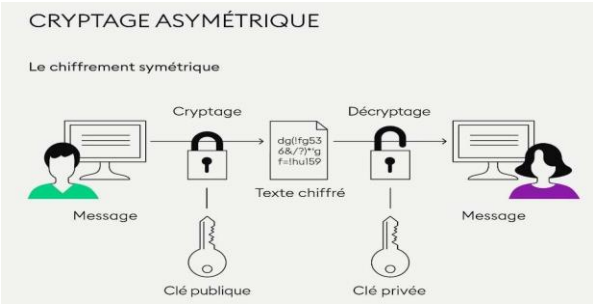

Figure 3.27: Cryptage asymétrique

La cryptographie asymétrique repose sur des problèmes mathématiques complexes, comme la factorisation de grands nombres entiers ou les équations de logarithme discret. Un chiffrement asymétrique est défini par trois algorithmes : un pour la génération des clés, un pour le chiffrement et un pour le déchiffrement. Ces algorithmes assurent la confidentialité, l'authentification, l'intégrité et l'échange sécurisé de clés secrètes. RSA, DSA et Diffie-Hellman sont quelques-uns des principaux algorithmes asymétriques utilisés.

Malgré ses avantages, le cryptage asymétrique est généralement plus lent que le cryptage symétrique. Ainsi, ils sont souvent combinés : le cryptage asymétrique sécurise l'échange de la clé secrète, ensuite utilisée pour le cryptage symétrique des données. Cette méthode combine la rapidité du cryptage symétrique avec la sécurité du cryptage asymétrique pour l'échange des clés. Le cryptage asymétrique est essentiel pour des applications comme la signature électronique et l'authentification, assurant la confidentialité et l'authenticité des messages en utilisant des paires de clés publique et privée.

3.4 Cryptographie chaotique

La cryptographie chaotique émerge comme un domaine innovant dans le paysage de la sécurité de l'information, exploitant les propriétés uniques des systèmes chaotiques pour protéger des données sensibles.

3.4.1 Principe

Le chiffrement d'un message par chaos repose sur une méthode innovante qui consiste à superposer un signal chaotique à l'information initiale. Cette approche assure une sécurité accrue en rendant le message illisible pour quiconque n'ayant pas accès aux caractéristiques du générateur de chaos utilisé.

Lorsque l'émetteur souhaite transmettre un message, il génère un signal chaotique à l'aide d'un système dynamique non linéaire. Ce signal est ensuite ajouté à l'information à chiffrer, créant ainsi un message noyé dans le chaos. Ce processus de superposition rend le contenu original pratiquement indéchiffrable pour un observateur non autorisé.

Une fois le message transmis, le récepteur, qui connaît les paramètres et les caractéristiques du générateur de chaos, peut procéder à l'extraction de l'information. Il lui suffit de soustraire le signal chaotique du message reçu pour retrouver l'information initiale. Ce mécanisme de chiffrement et de déchiffrement, basé sur les propriétés complexes des systèmes

chaotiques, offre une sécurité renforcée, car toute tentative de décryptage sans accès au générateur de chaos aboutit à des résultats incompréhensibles.

Ainsi, le principe du cryptage par chaos illustre comment les propriétés des systèmes chaotiques peuvent être exploitées pour sécuriser efficacement les communications, rendant la tâche des attaquants d'autant plus difficile.

3.4.2 Similarités entre le système chaotiques et système cryptographique

Caractéristique	Système chaotique	Système cryptographique
Complexité et sensibilité	Très sensible aux conditions initiales	Très sensible aux clés de chiffrement
Imprévisibilité	Génère des séquences de données aléatoires	Utilise des clés pour produire des messages chiffrés imprévisibles
Dépendance à la clé	Dépendance aux paramètres du système chaotique pour reproduire le comportement	Dépendance à la clé de chiffrement pour la sécurité du message
Non-linéarité	Basé sur des équations non linéaires, rendant le système imprévisible.	Utilise des transformations non linéaires pour renforcer la sécurité.

Tableau 3.3: Similarités entre le système chaotique et système cryptographique

La transmission sécurisée basée sur la théorie du chaos s'appuie sur des signaux chaotiques, qui présentent une sensibilité extrême aux conditions initiales. Cette caractéristique implique qu'une petite variation dans les paramètres initiaux peut engendrer des résultats très différents, ce qui rend la synchronisation des systèmes particulièrement essentielle.

3.5 La synchronisation

La synchronisation est un mécanisme clé permettant la coordination entre plusieurs processus ou systèmes. Nous aborderons ici sa définition, ses principes, les différents types de régimes ainsi que les méthodes employées pour la mettre en œuvre.

3.5.1 Définition de la synchronisation

(De Larousse) Synchronisation est un mot grec composé en deux parties : Syn signifie ensemble, et Chrono signifie temps. C’est l’action de mettre en phase pour créer une simultanéité entre plusieurs opérations, en fonction du temps. [44]

La synchronisation a été découverte par le chercheur hollandais Christian Huygens, un jour de 1665 alors qu'il était alité [45]. En observant deux pendules accrochés au mur, Huygens remarque un phénomène fascinant : l'un oscille vers la gauche pendant que l'autre oscille vers la droite, se synchronisant de manière étonnante. Peu importe leur position de départ, ces pendules finissent toujours par se caler en opposition de phase, avec l'un allant vers la droite et l'autre vers la gauche. Huygens conclut que ces horloges à balancier ajustent rapidement leur mouvement pour adopter une même phase et une même fréquence, même en présence de perturbations.

3.5.2 Principe de synchronisation des systèmes chaotiques

La synchronisation des systèmes chaotiques est un phénomène fascinant qui a captivé les chercheurs depuis l'observation initiale de Christian Huygens. La synchronisation des oscillateurs non linéaires, comme les systèmes chaotiques, se manifeste lorsque deux ou plusieurs systèmes dynamiques adoptent un comportement identique en fonction du temps. Ce phénomène peut se produire sous différentes formes, telles que l'auto-synchronisation, où les interactions internes entre les systèmes suffisent à aligner leurs mouvements, ou la synchronisation commandée, qui nécessite une intervention externe pour forcer l'harmonisation des systèmes dynamiques [46].

Un exemple courant est la configuration maître-esclave, où un système dynamique (esclave) ajuste son rythme et sa trajectoire pour suivre un autre système (maître). Dans le cadre des systèmes chaotiques, ce processus est particulièrement pertinent. En dépit de leur comportement imprévisible et instable en raison d'exposants de Lyapunov positifs, il est possible de synchroniser deux systèmes chaotiques, comme l'ont démontré Pecora et Carroll dans leur définition de la synchronisation identique. Le but est de faire correspondre les signaux chaotiques de ces systèmes via un couplage ou un forçage, afin qu'ils génèrent des comportements synchrones.

Dans les communications, la synchronisation chaotique permet de transmettre une information d'un émetteur à un récepteur. Le système chaotique du récepteur tente alors d'adapter son comportement à celui de l'émetteur, assurant ainsi une évolution commune des deux systèmes, malgré la nature complexe et imprévisible de leurs dynamiques.

3.5.3 Mode de synchronisation

La synchronisation des systèmes chaotiques peut être classée en deux types, selon la façon dont les systèmes sont couplés : la synchronisation unidirectionnelle et la synchronisation bidirectionnelle.

3.5.3.1 Synchronisation unidirectionnelle

Dans le cas d'une synchronisation unidirectionnelle, le couplage entre deux systèmes identiques a et b est réalisé à l'aide d'un élément fonctionnant dans un seul sens, par exemple l'utilisation d'un circuit électrique suiveur [14].

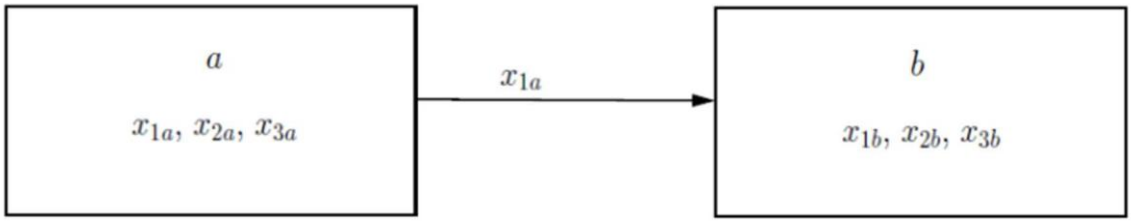

Figure 3.28: Couplage unidirectionnel

3.5.3.2 Synchronisation bidirectionnelle

Dans le cas d'une synchronisation bidirectionnelle, le couplage entre deux systèmes identiques a et b est réalisé à l'aide d'un élément permettant l'échange d'énergie dans les deux sens, par exemple l'utilisation d'une simple résistance [14].

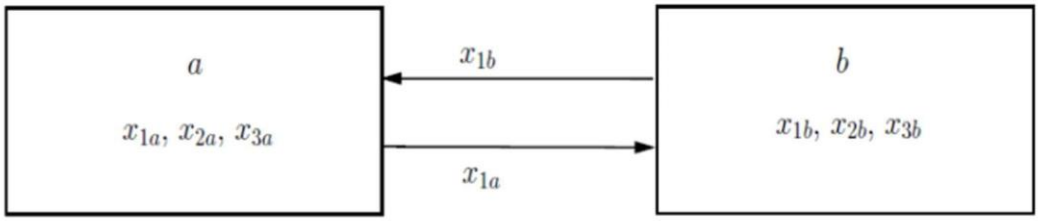

Figure 3.29: Couplage bidirectionnel

3.5.4 Type de synchronisation

3.5.4.1 Synchronisation projective

La synchronisation projective est une forme particulière de synchronisation dans laquelle les variables d'état de deux systèmes chaotiques partiellement linéaires se synchronisent jusqu'à un facteur d'échelle constant. Ce phénomène a été étudié pour la première fois par Mainieri et Rehacek dans le cadre de systèmes chaotiques identiques, où la synchronisation se produit lorsque les réponses des systèmes suivent une constante de proportionnalité nommée facteur d'échelle α_i.

Xu et al. Ont également proposé plusieurs méthodes de contrôle basées sur la théorie de la stabilité de Lyapunov afin de moduler ce facteur d'échelle et d'assurer que les systèmes

atteignent la synchronisation projective sous certaines conditions. Une synchronisation projective se produit lorsque les trajectoires du système esclave deviennent une constante multiple des trajectoires du système maître, conformément à l'équation suivante : [58] [59]

$$\exists \alpha_i \neq 0 \lim_{t \to +\infty} \left|\left| y_i(t) - \alpha_i x_i(t) \right|\right| = 0;\ \forall \big(x(0), y(0)\big), i = 1,2, \dots, n$$

3.5.4.2 Synchronisation généralisé

La synchronisation généralisée constitue une extension des différents types de synchronisation, notamment la synchronisation complète, l'anti-synchronisation et la synchronisation projective. Elle se distingue par sa capacité à établir une relation fonctionnelle entre deux systèmes dynamiques, même lorsque ceux-ci possèdent des dimensions différentes et suivent des modèles divergents. Ce type de synchronisation est particulièrement utile dans l'étude des systèmes chaotiques couplés de manière unidirectionnelle.

Introduite par Rulkov et al. En 1995 pour des systèmes chaotiques, la synchronisation généralisée permet de relier un système maître à un système esclave en définissant une fonction qui gouverne la dynamique de leurs états respectifs. Cela se manifeste par l'alignement asymptotique des trajectoires du système esclave en fonction de celles du système maître, comme décrit par l'équation suivante :

$$\begin{cases} \dot{x}(t) = f(x(t)) \\ \dot{y}(t) = g\big(y(t)\big) + u \end{cases} \quad \textbf{3.1}$$

Ou $x(t) \in \mathbb{R}^n, y(t) \in \mathbb{R}^m$, sont les états de système maitre et le système esclave respectivement, $f: \mathbb{R}^n, g: \mathbb{R}^m, u(t) = (u_i(t))_{i=1}^n \in \mathbb{R}^n$ est un contrôleur à déterminer [58].

3.5.4.3 Synchronisation retardé

Les chercheurs ont découvert que deux systèmes dynamiques chaotiques, même s'ils ne sont pas identiques, peuvent présenter un phénomène de synchronisation où leurs variables dynamiques se synchronisent, mais avec un décalage temporel. Ce type de synchronisation est appelé synchronisation retardée (ou anticipée) lorsque l'état du système chaotique esclave convergent vers l'état décalé dans le temps, du système chaotique maître [22].

$$\lim_{t \to +\infty} \|x'(t) - x(t - \tau)\| = 0$$

Où $x(t)$ est l'état du système maitre, $x'(t)$ est l'état du système esclave et τ est un retard positif. [T]

3.5.5 Méthodes de synchronisation

Il existe plusieurs techniques de synchronisation, notamment :

3.5.5.1 Synchronisation par boucle fermé

La synchronisation des systèmes chaotiques par boucle fermée repose sur une approche de contre-réaction pour corriger les variations paramétriques qui peuvent affecter la synchronisation en boucle ouverte. Cette méthode consiste à appliquer une correction au système en fonction de l'erreur entre le signal émis par le premier système (émetteur) et celui régénéré par le second (récepteur). L'erreur, utilisée en contre-réaction, ajuste le comportement du récepteur pour assurer la synchronisation.

Mathématiquement, si l'émetteur est décrit par :

$$\begin{cases} x = f(x) \\ y = h(x) \end{cases} \quad \textbf{3.2}$$

Le récepteur se présente comme :

$$\begin{cases} \hat{x} = f(\hat{x}) + g(y - \hat{y}) \\ \hat{y} = h(\hat{x}) \end{cases} \quad \textbf{3.3}$$

Où g est une fonction de l'erreur y et $\hat{y}$. Cette fonction est choisie de manière à garantir que le récepteur suive correctement le signal de l'émetteur, assurant ainsi la synchronisation. Ce type de récepteur peut être interprété comme un observateur, qui ajuste dynamiquement son comportement en fonction de l'erreur entre les deux systèmes.

3.5.5.2 Synchronisation à l'aide d'observateur

La synchronisation peut également être réalisée en employant un observateur. L'observateur est une méthode typique afin d'estimer les états inconnus d'un système dynamique qui ne peuvent pas être mesurés directement : soit inaccessible, soit pas économique [47].

La synchronisation par observateur consiste à créer un système esclave qui agit comme un observateur du système maître, permettant ainsi aux deux systèmes d'évoluer de manière identique.

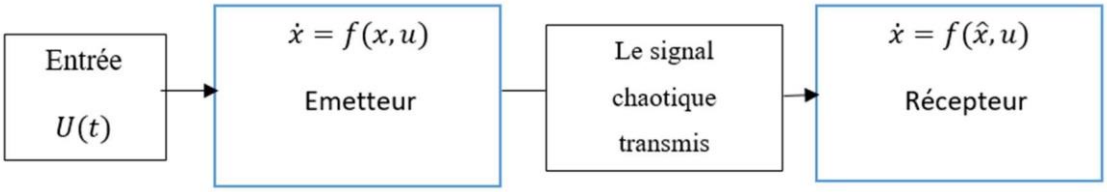

Figure 3.30: Synchronisation à l'aide d'observateur

L'image illustre le principe de synchronisation utilisant un observateur.

- $x(t)$ Représente l'état du système émetteur, dont la dynamique est régie par

  l'équation $\dot{x} = f(x,u)$, ou $u(t)$ est le signal d'entrée appliqué.

- $\hat{x}(t)$ désigne l'état du système récepteur, qui évolue selon $\dot{\hat{x}} = f(\hat{x},u)$.
- Pour que l'émetteur et le récepteur se synchronisent, il est nécessaire que le système $\dot{\hat{x}} = f(\hat{x},u)$ agisse comme un observateur convergent pour le système

  $\dot{x} = f(x,u)$.

Cela signifie que le récepteur ajuste son comportement en fonction du signal chaotique transmis par l'émetteur, cherchant à suivre $x(t)$ de manière efficace. Un retard positif τ peut également être introduit pour compenser les délais dans la transmission du signal.

A. Observateur

Un observateur est un système dynamique qui, à partir de l'entrée $u(t)$ du système et de la sortie $y(t)$ mesurée, fournit un état estimé $\hat{x}(t)$ qui doit tendre vers l'état réel $x(t)$ [46]. Il permet ainsi de reconstituer les états internes du système à partir des informations disponibles, même lorsque certaines de ces variables ne sont pas directement mesurables. En combinant cette estimation avec les données mesurées, l'observateur joue un rôle crucial dans l'amélioration du contrôle et de la synchronisation des systèmes dynamiques.

B. Observateur mode glissant

Un observateur à mode glissant est un type d'observateur où le correcteur fait appel à une fonction signe discontinue. Son principe consiste à contraindre les erreurs d'estimation d'un système non linéaire à converger vers une surface spécifique appelée surface de

glissement, notée $\boldsymbol{S}$. Cette surface est définie comme l'ensemble des états $x \in \mathbb{R}^n$ pour lesquels $S(x) = 0$.

Dans le cadre de ces observateurs, l'erreur d'observation, définie par $e(t) = x(t) - \hat{x}(t)$, où $x(t)$ est l'état réel et $\hat{x}(t)$ l'état estimé, tend à diminuer au fil du temps. À partir de leurs valeurs initiales, ces erreurs convergent vers les valeurs d'équilibre en imposant l'évolution des dynamiques du système sur la surface de glissement.

Sur cette surface, la différence entre la sortie du système réel et celle de l'observateur $\epsilon(t) = y(t) - \hat{y}(t)$ devient nulle, ce qui signifie que le système observé et le système réel sont parfaitement synchronisés. Les dynamiques sur cette surface sont stabilisées de manière à minimiser ou éliminer toute erreur restante d'observation, permettant ainsi une estimation précise des états du système.

C. Observateur impulsif

Prenons comme point de départ le système suivant [61] :

$$\begin{cases} \dot{x}_1(t) = f_1(x_1, x_2, t) \\ \dot{x}_2(t) = f_2(x_1, x_2, t) \\ y(tk) = x_1(t_k) \end{cases} \quad \textbf{3.4}$$

Dans ce système, $x_1(t) \in \mathbb{R}^n$ et $x_2(t) \in \mathbb{R}^{n-p}$ sont les variables d'état, tandis que $y(t_k) \in \mathbb{R}^n$ est le vecteur de sortie. L'idée est de concevoir un observateur capable de suivre cette dynamique, en s'ajustant à certains moments clés t_k, grâce à des impulsions qui transmettent l'état du système pour corriger les écarts.

L'observateur est conçu pour suivre de près l'évolution du système original, tout en appliquant des corrections discrètes pour éviter une redondance excessive du signal.

Mathématiquement, cela se traduit par le modèle suivant :

$$\begin{cases} \dot{\hat{x}}_1(t) = f_1(\hat{x}_1, \hat{x}_2, t) \\ \dot{\hat{x}}_2(t) = f_2(\hat{x}_1, \hat{x}_2, t) \\ \hat{x}_1(tk) = x_1(t_k) \end{cases} \quad \textbf{3.5}$$

Ainsi, à chaque instant discret t_k, l'observateur synchronise l'une de ses variables, $\hat{x}_1$, avec l'état réel x_1 , ce qui garantit que l'observateur reste aligné sur la trajectoire du système.

Quant à l'erreur d'observation, elle est définie comme la différence entre le comportement du système réel et celui estimé par l'observateur. Cette erreur est décrite par le système suivant :

$$\begin{cases} \dot{e}_1(t) = f_1(x_1, x_2, t) - f_1(\hat{x}_1, \hat{x}_2, t) \\ \dot{e}_2(t) = f_2(x_1, x_2, t) - f_2(\hat{x}_1, \hat{x}_2, t) \\ e_1(t_k) = 0 \end{cases} \quad \textbf{3.6}$$

L'observateur corrige donc ses états à ces instants précis D pour ramener l'erreur à zéro sur la première composante, ce qui permet de stabiliser le système en suivant fidèlement sa dynamique originale.

Un observateur impulsif est approprié pour les schémas de synchronisations impulsives chaotiques lorsque la sortie est discrète. En utilisant la sortie d'un système (émetteur) à des instants de temps discrets, l'observateur permet de reconstruire tous les états [14].

3.6 Méthodes de cryptage à base de la synchronisation

La plupart des méthodes de cryptage chaotique reposent sur une architecture maîtreesclave, où un système émetteur (maître) génère un signal chiffré qui est ensuite transmis à un système récepteur (esclave), dont le rôle est de se synchroniser avec le maître pour restaurer le signal d'information. Ces techniques de synchronisation permettent d'assurer une transmission sécurisée des données. Parmi les méthodes classiques de communication basées sur le chaos, on retrouve notamment :

3.6.1 Cryptage par addition (masquage chaotique)

Le cryptage par addition est une technique pionnière dans le domaine de la cryptographie, utilisant la synchronisation du chaos. Cette méthode est la première chronologiquement à utiliser la synchronisation du chaos. Elle est liée aux travaux de (Wu et Chua, 1993) et de (Cuomo et al.) [48]. Fondamentalement, cette méthode consiste à combiner un signal chaotique avec un message utile et à transmettre le résultat à travers un canal public. La récupération du message original se fait par synchronisation chaotique au niveau du récepteur, où le message est retrouvé par soustraction.

Cette approche présente plusieurs avantages significatifs. D'abord, elle offre un cryptage relativement simple et peut être appliquée à des messages continus ou discrets. De plus, elle dissimule efficacement le message, ce qui dissuade les tentatives de décryptage par des tiers.

Cependant, pour garantir la synchronisation, l'amplitude du message doit être nettement plus faible que celle du signal chaotique émis. En présence de bruit dans le canal de transmission, détecter l'information devient difficile et exige que l'amplitude du message soit supérieure à celle du bruit.

Malgré ses avantages, cette méthode présente des inconvénients, l'information agissant comme une perturbation, la synchronisation n'est jamais parfaite, même lorsque l'amplitude du message est faible [49]. De plus, l'utilisation de cette méthode peut être inefficace en termes d'énergie transmise par rapport à la qualité de l'information fournie.

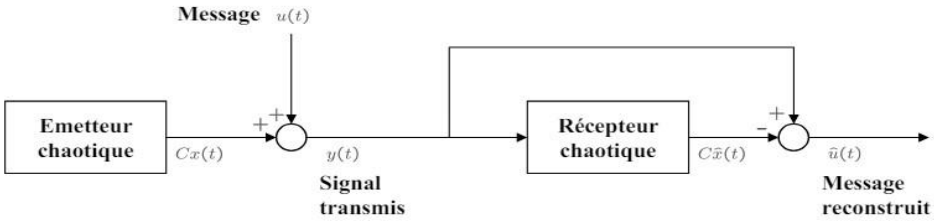

Figure 3.31: Cryptage par addition

3.6.2 Cryptage par inclusion

Le cryptage par inclusion est une technique où le message à transmettre est directement injecté dans la dynamique de l'émetteur, sans nécessiter une modulation de paramètre. Le rôle principal du récepteur est de synchroniser son comportement avec celui de l'émetteur, afin de restaurer le message original. La restauration de l'information repose sur deux approches :

- **L'utilisation d'observateurs à entrées inconnues [14]**

La figure ci-dessous présente un problème classique d'estimation d'état non linéaire avec des entrées inconnues : il s'agit de reconstruire l'état $x(t)$ du système émetteur ainsi que l'entrée inconnue $u(t)$.

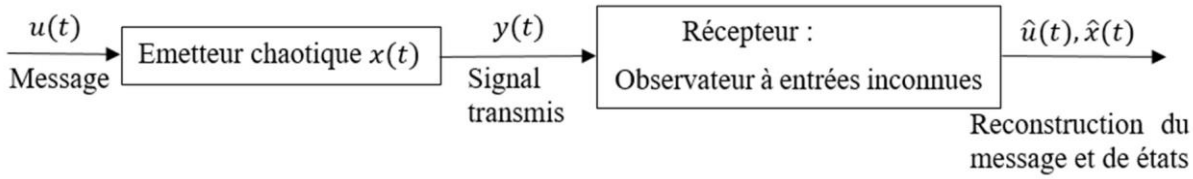

Figure 3.32: Observateur à entrées inconnues

• L'inversion du système émetteur [14]

Le récepteur est conçu en inversant le modèle de l'émetteur, La figure ci-dessous présente le principe général de cette approche.

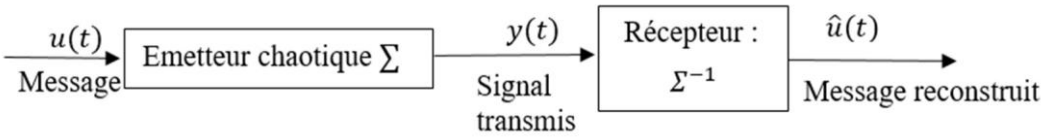

Figure 3.33: Principe du cryptage par inversion

L'un des principaux défis de cette méthode est d'assurer l'observabilité, ainsi que la capacité à inverser les dynamiques du système pour reconstruire à la fois les états internes et le message transmis à partir des signaux de sortie et de leurs dérivées.

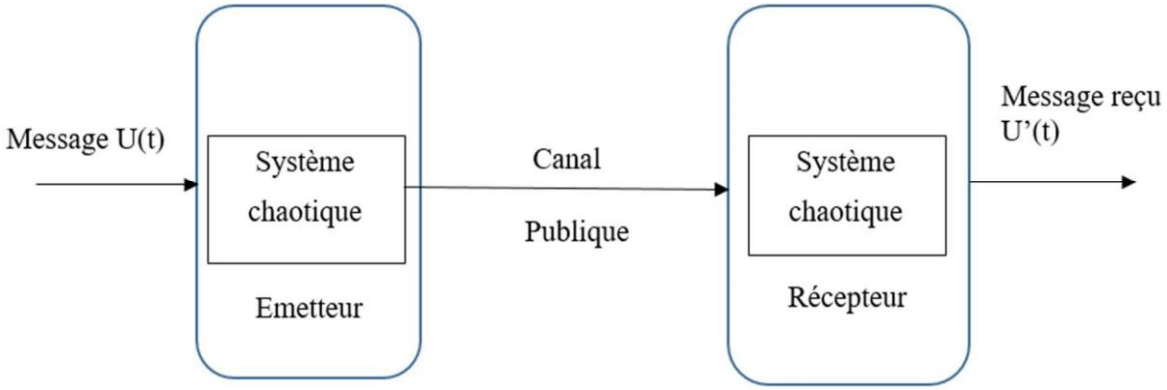

Figure 3.34: Cryptage par inclusion

3.6.3 Cryptage par modulation paramétrique

Un contrôleur adaptatif est chargé de maintenir la synchronisation entre l'émetteur et le récepteur. Il ajuste en temps réel le récepteur pour suivre les variations du paramètre modulé, assurant ainsi la cohérence du signal chaotique transmis. Le schéma correspondant à ce processus est illustré dans la figure associée.

Au niveau de l'émetteur, la modulation du ou des paramètres entraîne une modification continue de la trajectoire de l'attracteur chaotique. De ce fait, le signal transmis est beaucoup plus complexe qu'un signal chaotique ordinaire, ce qui renforce la sécurité. Cependant, la manière d'injecter le message et la fonction de démodulation des paramètres doivent être conçues de façon à ne pas altérer le caractère chaotique du signal. Ce dernier doit rester suffisamment imprévisible pour empêcher toute tentative d'interception non autorisée.

Cette technique exploite pleinement les propriétés des systèmes chaotiques, offrant un niveau de sécurité élevé et une efficacité sans équivalent dans les systèmes de communication traditionnels.

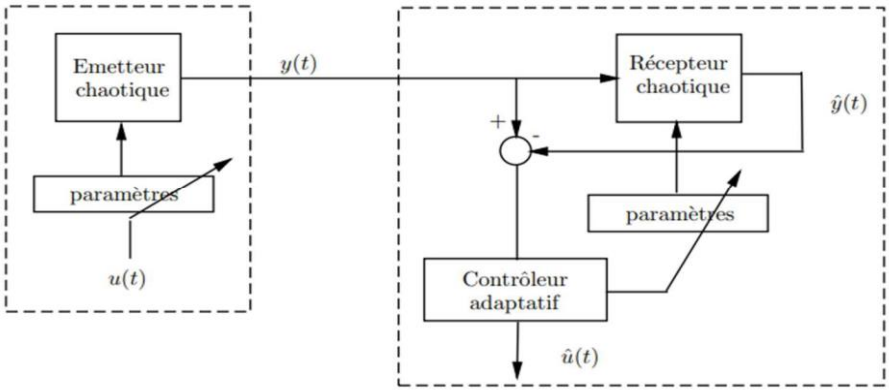

Figure 3.35: Cryptage par modulation paramétrique

3.6.4 Cryptage mixte

Le **cryptage mixte** est une méthode qui combine la cryptographie traditionnelle avec la dynamique d'un système chaotique pour renforcer la sécurité des communications. Dans ce processus, le message à protéger, noté $u(t)$, est d'abord crypté à l'aide d'une clé chaotique, $c(t)$, générée par l'émetteur. Ce message crypté est ensuite injecté dans la dynamique du système chaotique, rendant la structure du signal plus complexe et difficile à décoder pour des tiers.

Une fois ce signal modifié, un signal supplémentaire, noté $y(t)$, qui dépend des variables d'état du système émetteur, est transmis au récepteur. Ce dernier, grâce à la synchronisation avec l'émetteur, parvient à reconstruire la clé chaotique $c(t)$. Cette clé permet alors de décoder le message crypté, assurant ainsi une communication sécurisée. [60]

Le cryptage mixte utilise donc la complexité inhérente des systèmes chaotiques pour rendre le cryptage plus robuste face à des tentatives d'interception ou de décryptage non autorisées.

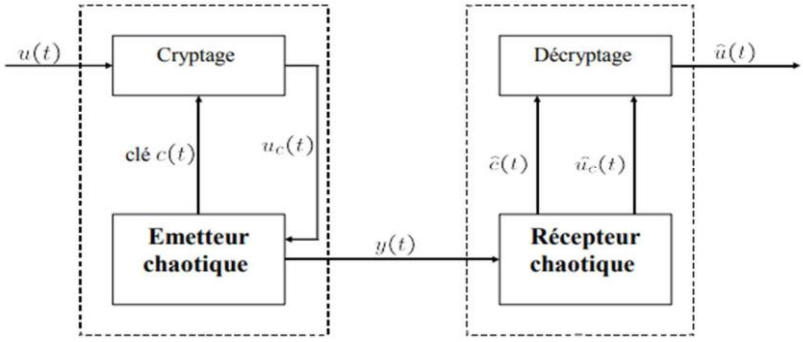

Figure 3.36: Cryptage mixte.

Conclusion

Ce chapitre met en avant l'évolution des techniques de cryptage pour répondre aux menaces de sécurité grandissantes. En particulier, les méthodes chaotiques renforcent la complexité du décryptage non autorisé en ajoutant un signal chaotique à l'information originale, selon divers schémas de chiffrement. Il souligne également l'importance du principe de synchronisation, qui s'avère essentiel pour sécuriser efficacement la transmission des données.

CHAPITRE 4

Réalisation

Introduction

Ce chapitre présente l'implémentation et la validation de notre système de cryptage et de transmission de données, dans un environnement de test initial et sécurisé. Il s'agit ici d'une première phase de simulation avant un déploiement réel sur un drone. À travers l'utilisation de composants variés, tels que la carte Arduino Uno, le module LoRa et un joystick, ce dispositif évalue la robustesse du cryptage et la qualité de la transmission des commandes.

PARTIE MATERIELLE

Afin de valider l'efficacité de notre système de cryptage et de transmission des données dans un environnement sécurisé, nous avons conçu une phase de test initiale. Cette configuration utilise un joystick pour simuler les commandes d'une radiocommande et une matrice de LEDs pour représenter les réponses du drone. Les commandes générées par le joystick sont cryptées, transmises via le protocole LoRa, puis les LEDs réagissent en fonction des données décryptées, simulant ainsi le comportement du drone.

Ce banc de test nous permet de valider la robustesse du cryptage et de la transmission des données avant de passer à des expérimentations en conditions réelles avec un drone. Une fois cette étape terminée, l'intégration finale pourra être confirmée, garantissant ainsi la confidentialité et l'intégrité des communications.

4.1 Composants utilisés

Dans ce projet, nous avons initialement utilisé une carte ESP32 pour exploiter ses capacités WiFi et tester la communication sans fil. Afin d'explorer différentes configurations et de diversifier nos essais, nous avons également utilisé une carte Arduino, notamment pour intégrer et tester les commandes du joystick. Après avoir validé la communication via WiFi, nous avons opté pour une communication longue portée en adoptant la technologie LoRa, qui s'est avérée mieux adaptée à nos besoins en termes de portée et de stabilité de la transmission.

4.1.1 Carte ESP32

4.1.1.1 Définition

L'ESP32 est une série de microcontrôleurs système sur puce (SoC) à faible consommation d'énergie développée par Espressif Systems. Successeur de l'ESP8266, il est basé sur l'architecture Xtensa LX6 et se distingue par son intégration native du Wi-Fi (802.11 b/g/n) et

du Bluetooth (jusqu'aux versions 5.0 et 5.1), le tout à un coût abordable. L'ESP32 est souvent utilisé dans les **a**pplications embarquées, ce qui le rend idéal pour les projets nécessitant à la fois une connectivité sans fil et une faible consommation d'énergie. Destiné principalement aux applications de l'Internet des Objets (IoT), l'ESP32 est disponible sous forme de puce (comme le très populaire ESP32-WROOM-32), mais il existe également plusieurs variantes (comme l'ESP32-S2 et l'ESP32-C3) adaptées à différentes applications.

Le développement de logiciels pour l'ESP32 se fait principalement avec l'ESP-IDF, un framework open-source en C utilisant FreeRTOS, un système d'exploitation temps réel, et offrant un riche écosystème de bibliothèques. L'ESP32 est également compatible avec Arduino et MicroPython, facilitant son intégration dans divers projets.

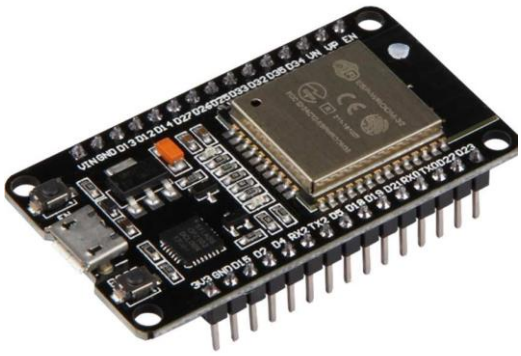

Figure 4.37: ESP32-WROOM-32

4.1.1.2 Architecture d'une carte ESP32

L'architecture de l'ESP32 est conçue pour offrir polyvalence et performance dans les environnements embarqués et IoT. Voici ses composants principaux :

- **Processeur :** L'ESP32 intègre généralement deux cœurs Xtensa LX6 cadencés jusqu'à 240 MHz, permettant l'exécution parallèle de tâches pour maximiser les performances tout en minimisant la consommation d'énergie. Certaines variantes, comme l'ESP32C3, utilisent également un cœur RISC-V, offrant des options supplémentaires selon les besoins du projet.
- **Connectivité sans fil :** L'ESP32 prend en charge nativement le Wi-Fi 802.11 b/g/n et le Bluetooth (Classic et Low Energy), permettant une connectivité simultanée à plusieurs réseaux, essentielle pour les applications IoT.
- **Mémoire :** Le microcontrôleur dispose de 520 Ko de SRAM pour l'exécution des programmes et est généralement couplé à une mémoire flash externe (jusqu'à 4 Mo),

utilisée pour stocker le firmware et les données. Cette mémoire **flash externe** peut être soit intégrée au module, soit ajoutée séparément selon la carte de développement utilisée.

- **Gestion de l'alimentation :** Grâce à plusieurs modes de veille, dont le "Deep Sleep" à très faible consommation (quelques microampères), l'ESP32 est optimisé pour les applications alimentées par batterie, prolongeant ainsi leur autonomie.
- **Périphériques et interfaces :** L'ESP32 offre un large éventail de GPIO, ainsi que des convertisseurs analogique-numérique (ADC) et numérique-analogique (DAC). Il prend également en charge des interfaces standards telles qu'UART, SPI, I2C, PWM, et inclut des capteurs comme un capteur de température et un capteur à effet Hall.
- **Sécurité :** Le microcontrôleur intègre des accélérateurs matériels pour les algorithmes de cryptographie (AES, SHA-2, RSA, ECC), garantissant des communications sécurisées, un atout important pour les applications IoT sensibles.
- **Coprocesseur ULP (Ultra Low Power) :** Ce coprocesseur permet l'exécution de tâches simples à très faible consommation d'énergie, comme la surveillance de capteurs, sans réveiller les cœurs principaux, optimisant ainsi encore plus la gestion de l'énergie.

4.1.2 Carte arduino

La carte Arduino est une plateforme de prototypage électronique open-source conçue pour rendre la programmation des microcontrôleurs plus accessible. Créée en 2005 par Massimo Banzi et David Cuartielles à l'école de design Interaction Design Institute Ivrea en

Italie, Arduino visait à offrir une solution abordable pour des projets robotiques et interactifs [50]. L'écosystème Arduino comprend des cartes matérielles et un environnement de développement (IDE) permettant de programmer des microcontrôleurs, tels que l'ATmega328 ou des architectures ARM pour des modèles plus puissants comme l'Arduino Due. Initialement conçu pour les débutants, Arduino est désormais utilisé aussi bien par des novices que des experts dans des domaines variés, tels que l'Internet des Objets (IoT), la robotique, l'enseignement et les arts numériques.

Au fil des ans, de nombreux modèles de cartes Arduino ont été développés pour répondre à différentes applications. La première carte Arduino, la Diecimila, est sortie en 2007, marquant le début de l'évolution de cette plateforme. Parmi les autres modèles notables, on trouve [51] :

- **LilyPad** (2007) : conçue pour l'intégration dans les vêtements et les tissus.
- **Nano** (2008) : destinée aux applications miniatures et discrètes.
- **Mini** (2008) : une autre version compacte pour les petits projets.
- **Duemilanove** (2008) : initialement équipée d'un ATmega168, remplacé ensuite par l'ATmega328.
- **Mega** (2009) : dotée d'une plus grande capacité pour les projets nécessitant davantage de broches et de mémoire.
- **Uno** (2010) : la plus populaire et utilisée pour les projets de base et intermédiaires.
- **Leonardo** (2012) : utilisant un microcontrôleur avec une interface USB intégrée.
- **Esplora** (2012) : intègre des capteurs et actionneurs pour des projets interactifs.
- **Yún** (2013) : combinant Arduino et une plateforme Linux pour l'Internet des Objets (IoT).
- **Portenta** (2020) : conçue pour des applications IoT, IA et industrielles avec des capacités de traitement avancées.

Pour notre projet, nous avons choisi d'utiliser une carte Arduino Uno, en raison de sa popularité et de sa facilité d'utilisation.

4.1.3 Carte Arduino UNO

Lancée en 2010, l'Arduino Uno est l'une des cartes les plus emblématiques de la gamme Arduino. Ce microcontrôleur programmable permet de gérer différents éléments mécaniques comme des systèmes, des éclairages ou des moteurs. Polyvalente, elle facilite grandement la création de systèmes automatisés.

Caractéristiques de l'Arduino Uno [52] :

Catégorie	Valeur
Microcontrôleur	ATmega328
Fréquence d'horloge	16 MHz
Tension de service	5 V
Tension d'entrée (recommandée)	7–12 V
Tension d'entrée (limites)	6–20 V
Ports numériques	14 entrées et sorties (6 sorties commutables en MLI)

Ports analogiques	6 entrées analogiques
Courant maxi. par broche d'E/S (c.c.)	40 mA
Courant maxi. par broche 3,3 V	50 mA
Mémoire	32 Ko Flash, 2 Ko SRAM, 1 Ko EEPROM
Chargeur d'amorçage	0,5 Ko (en mémoire Flash)
Interface	USB
Dimensions	6,86 cm × 5,3 cm

Tableau 4.4: Caractéristique d'une carte arduino UNO

4.1.3.1 Architecture de la carte

L'architecture de la carte Arduino Uno est conçue pour être simple, intuitive et efficace, adaptée à une large gamme de projets électroniques. Voici un aperçu détaillé de ses principaux composants et fonctionnalités :

- **Microcontrôleur ATmega328 :** Au cœur de la carte, le microcontrôleur ATmega328 exécute les instructions programmées, contrôle les entrées/sorties et assure le bon fonctionnement de l'ensemble du système.
- **Entrées et sorties numériques (Pins 0 à 13) :** - Les pins 2 à 13 permettent de lire et d'écrire des états logiques (haut ou bas) pour contrôler des dispositifs externes comme des LEDs, des moteurs, ou des relais.

- Certaines de ces broches (3, 5, 6, 9) sont capables de générer un signal PWM (modulation de largeur d'impulsion), permettant de contrôler des moteurs ou la luminosité des LEDs.

- Les pins 0 et 1 sont dédiées à la communication série, avec le pin 0 (RX) pour la réception et le pin 1 (TX) pour l'émission des données. Ces pins sont également utilisés lors de la connexion via USB.

- **Pins réservés :**

- La carte utilise certains pins pour des fonctions spécifiques :
- SPI (liaison série) est disponible sur les pins 10, 11, 12, 13, pour communiquer avec des périphériques tels que des capteurs, des mémoires ou d'autres microcontrôleurs.
- Le pin 4 est réservé pour le contrôle d'une carte SD, utile pour stocker des données externes.

- **Entrées analogiques (A0 à A5) :**

- L'Arduino Uno possède 6 broches analogiques, numérotées d'A0 à A5, qui permettent de lire des signaux analogiques (valeurs continues) provenant de capteurs, comme des potentiomètres ou des capteurs de température.
- Ces broches utilisent un convertisseur analogique-numérique (ADC) avec une résolution de 4,0883 mV, ce qui permet de convertir les signaux analogiques en valeurs numériques que le microcontrôleur peut traiter.

- **Alimentation :** La carte peut être alimentée de différentes manières :

- Par le port USB qui fournit directement 5V.
- Par une alimentation externe (de 7V à 12V) via le port d'alimentation externe. La carte possède un régulateur de tension intégré, qui abaisse la tension pour fonctionner à 5V.

- **Connecteur ICSP :** L'interface ICSP (In-Circuit Serial Programming) permet de reprogrammer ou de flasher le microcontrôleur à l'aide d'un programmateur externe. Elle est également utilisée pour recharger le firmware ou réinitialiser la carte.
- **Bouton Reset :** Le bouton Reset permet de redémarrer le programme en cours sans avoir besoin de déconnecter la carte de son alimentation. Cela est utile pour tester rapidement des modifications de programme.
- **Sorties d'alimentation :** Plusieurs broches fournissent des tensions de 3.3V, 5V et GND pour alimenter des capteurs, des modules et d'autres composants externes connectés à la carte.
- **Communication et visualisation :** Pour la communication série, la carte utilise les Pins 0 et 1 pour la réception (RX) et l'envoi (TX) des données, respectivement. Ces communications peuvent également transiter via le port USB lorsque la carte est connectée à un ordinateur.
- **Trois LEDs sont présentes :** - Une LED connectée à la broche 13, souvent utilisée pour tester des programmes ou pour indiquer que la carte est sous tension.

- Deux autres LEDs visualisent l'activité sur les pins série : une pour la transmission (TX) et l'autre pour la réception (RX).

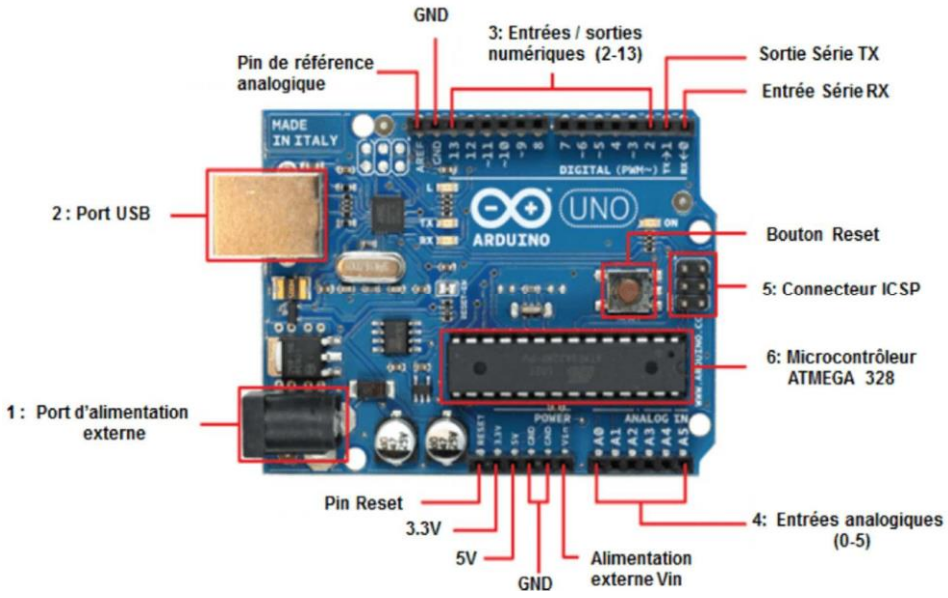

Figure 4.38 : Composants d'une carte arduino UNO

4.1.3.2 Avantages et inconvénients

• Avantages

- L'Arduino Uno est relativement peu coûteux par rapport à d'autres cartes microcontrôleurs, ce qui le rend accessible pour les amateurs et les professionnels.
- Une documentation complète est disponible, offrant des exemples de code, des schémas et des projets, ce qui aide à la compréhension et à l'utilisation.
- L'Uno peut être utilisé avec une grande variété de capteurs et de modules, permettant de l'adapter à de nombreux projets, allant des simples clignotants LED aux applications robotiques et IoT complexes.
- Bien que principalement programmé en C/C++, l'Arduino Uno est compatible avec d'autres langages via des bibliothèques, offrant ainsi une plus grande flexibilité pour les développeurs.
- L'Arduino Uno est compatible avec de nombreux shields et modules, permettant une extension facile des fonctionnalités, y compris les écrans, capteurs, moteurs, etc.
- Avec un bon nombre de broches d'entrée/sortie numériques et analogiques, l'Arduino Uno permet de connecter une variété de capteurs et d'actionneurs.

• Inconvénient

- Mémoire limitée à 32 Ko, ce qui peut poser problème pour les projets nécessitant beaucoup de code.

- Absence de connectivité sans fil intégrée (Wi-Fi, Bluetooth), nécessitant des modules externes pour ces fonctionnalités.
- Tension d'entrée fixe, limitant l'utilisation dans certaines applications spécifiques.
- Performances limitées avec un processeur à 16 MHz, rendant la carte peu adaptée pour des applications nécessitant un traitement en temps réel ou de haute performance.

  Pas de prise en charge native du multitâche, rendant complexe l'exécution de plusieurs tâches simultanées.

4.1.4 Module LoRa

Le LoRa (Long Range) est une technologie sans fil destinée aux applications nécessitant des communications longue portée et à faible consommation d'énergie, principalement dans l'IoT (Internet des Objets) et les réseaux M2M (Machine-to-Machine). Basée sur la modulation chirp à spectre étalé, elle permet des transmissions efficaces sur de grandes distances tout en minimisant la consommation énergétique. LoRa fonctionne sur des bandes de fréquences spécifiques selon les régions (915 MHz aux États-Unis, 868 MHz en Europe, 433 MHz en Asie).

Développée par la société française Cycleo et acquise par Semtech en 2012, cette technologie est aujourd'hui normalisée par la LoRa Alliance. Le module RA-01, utilisé dans notre projet, conçu par Ai-Thinker avec la puce SX1278 de Semtech, fonctionne sur la bande ISM à 433 MHz. Il est idéal pour les communications longue portée à faible consommation d'énergie, largement employé dans des applications IoT comme les systèmes de surveillance à distance.

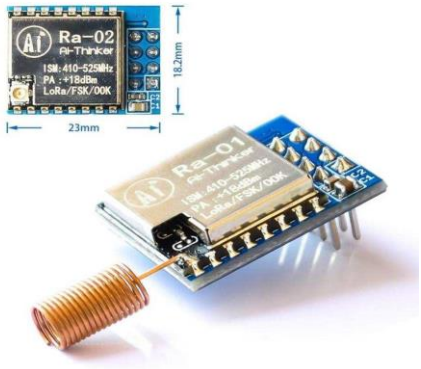

Figure 4.39: Module LoRa

- **Les caractéristiques techniques essentielles de la technologie LoRa sont résumées dans le tableau ci-dessous [52] :**

Caractéristique	Détails
Fréquence	433 MHz (plage de 420 à 450 MHz)
Puissance de sortie RF	+20 dBm (10 mW)
Taux de transfert de données	Jusqu'à 300 kbps
Modes de modulation	LoRa, FSK, GFSK, MSK, GMSK, OOK
Courant de fonctionnement	< 10,8 mA en réception, < 120 mA en transmission
Température de fonctionnement	-40 à +85 °C

Tableau 4.5: Caractéristique du module LORA

4.1.4.1 La couche physique de LoRa

La couche physique de LoRa repose sur la modulation chirp à spectre étalé, qui permet d'augmenter la portée du signal tout en réduisant les interférences.

La fréquence d'un signal LoRa évolue de manière linéaire, soit en augmentant (upchirp), soit en diminuant (downchirp). L'information est transmise par des variations de fréquence, ce qui rapproche LoRa de la modulation par déplacement de fréquence multiple (MFSK - Multiple Frequency-Shift Keying). Grâce à l'étalement du spectre, cette technique permet une transmission très résistante aux interférences tout en étant économe en énergie. Ce type de modulation est couramment utilisé dans les radars et s'étend généralement sur une bande passante de 125 kHz à 500 kHz [53].

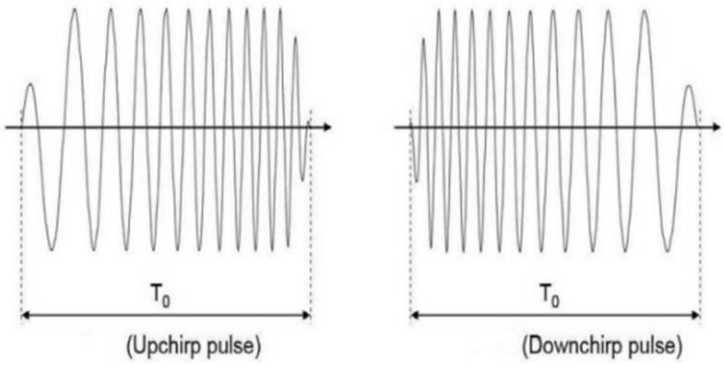

Figure 4.40: Variation de fréquence effectuée par LoRa

4.1.4.2 La couche de liaison LoRaWAN

Pour assurer l'interopérabilité entre différents fabricants, la LoRa Alliance a spécifié un standard appelé LoRaWAN [54]. Ce standard décrit en détail le protocole de communication utilisé et définit une architecture réseau standardisée. LoRaWAN permet de gérer le contrôle d'accès au réseau et de faciliter les échanges entre les appareils connectés et une ou plusieurs passerelles.

LoRaWAN adopte une topologie en étoile, où une passerelle relaie de manière transparente les messages entre le terminal (comme un capteur IoT) et le serveur de réseau. Cette architecture permet d'assurer une communication fiable, comme illustré dans le schéma de la **Figure 4.5**.

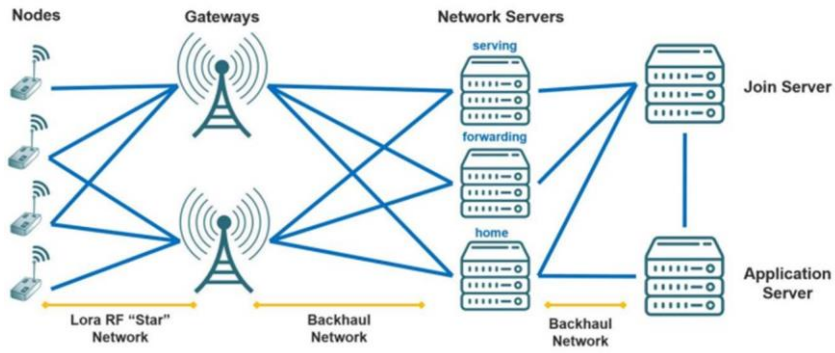

Figure 4.41: Architecture d'un réseau LoRa

4.1.4.3 Avantages et inconvénients

- **Avantage :**
  - Portée jusqu'à 5 km en zone urbaine, 15 km en zone rurale, voire plus avec une ligne de mire dégagée.
  - Un petit nombre de passerelles couvre de larges zones.
  - Gestion de milliers de nœuds par passerelle grâce à différents canaux et facteurs de propagation.
  - Faible consommation d'énergie permettant des années d'autonomie avec des petits paquets de données.
  - Excellente résistance aux interférences grâce à la modulation chirp à spectre étalé.
- **Inconvénients :**
  - Débit de données bien inférieur au WiFi et aux réseaux 4G/5G.

- Capacité des nœuds limitée par la couverture des passerelles.
- Risque d'interférences sur les bandes sans licence.
- Faible prise en charge des transferts de données volumineux, tels que les vidéos ou fichiers lourds.

4.1.5 Joystick

Le module joystick KY-023 est un dispositif à deux axes XY conçu pour contrôler les mouvements sur les axes X et Y dans divers projets électroniques. Compatible avec des plateformes populaires comme Arduino, Raspberry Pi et ESP32, ce module est équipé de cinq broches mâles. Il utilise un potentiomètre biaxial pour la détection de mouvement et intègre un interrupteur qui s'active lorsqu'il est enfoncé. Le KY-023 est largement utilisé dans une variété d'applications, allant des véhicules télécommandés aux systèmes d'éclairage à LED.

Figure 4.42: joystick KY-023

Ci-dessous, les principales caractéristiques techniques du module joystick KY-023 :

Caractéristique	Valeur
Tension de fonctionnement	5 V
Valeur du potentiomètre interne	10 kΩ
Câbles d'interface	Broches de 2,54 mm
Dimensions	1,57 po x 1,02 po x 1,26 po (4,0 cm x 2,6 cm x 3,2 cm)
Température de fonctionnement	0 à 70 °C

Figure 4.43: Caractéristique du joystick

4.1.6 Résistances et leds

- **Résistances :** Les résistances sont des composants électroniques passifs qui limitent le courant électrique dans un circuit. Elles sont utilisées pour protéger les autres composants, ajuster les niveaux de signal ou diviser la tension. Les valeurs de résistance sont exprimées en ohms (Ω), et elles sont disponibles dans une variété de tailles et de types.

- **Leds :** Une diode électroluminescente (DEL ou LED) est un composant optoélectronique capable d'émettre de la lumière lorsqu'il est parcouru par un courant électrique. Une LED ne laisse passer le courant électrique que dans un seul sens (le sens passant). Lorsqu'elle est traversée par un courant, la LED oppose une tension fixe : 1,9 V pour une LED rouge, 3,2 V pour les LEDs blanches ou autres couleurs.

4.2 Bronchement et montage de la réalisation

4.2.1 Bronchement de l'arduino et du module LoRa

Pour établir la connexion entre l'Arduino Uno et le module LoRa, nous utilisons le protocole SPI (Serial Peripheral Interface), qui permet une communication rapide entre le microcontrôleur (Arduino) et le module LoRa. Voici la correspondance des pins pour l'émetteur et le récepteur :

Fonction	Emetteur	Récepteur
MOSI	Pin 11	Pin 11
MISO	Pin 12	Pin 12
SCK	Pin 13	Pin 13
SS	Pin 10	Pin 8
RST	Pin 9	Pin 7
DIO0	Pin 2	Pin 2

Tableau 4.6: Pins utilisé pour le bronchement de la carte arduino et le module LoRa

Voici le circuit de connexion entre l'Arduino Uno et le module LoRa :

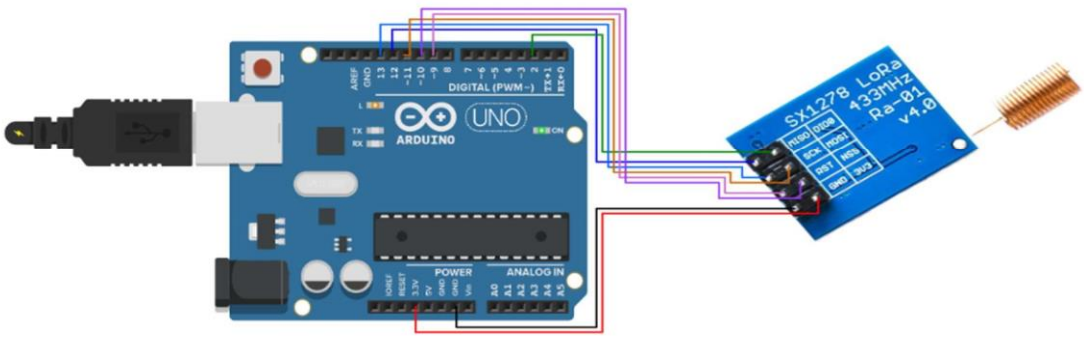

Figure 4.44: Schéma de connexion entre l'Arduino Uno et le module LoRa réalisé sur EasyEDA

4.2.2 Bronchement du joystick à l'arduino

Le joystick dispose de deux axes (X et Y) qui correspondent à des potentiomètres analogiques et d'un bouton intégré. Chaque axe envoie un signal de tension variable qui peut être lu par les broches analogiques de l'Arduino.

Voici les connexions réalisées entre le joystick et l'Arduino Uno :

- **Axe X (X-axis)** : connecté à la broche analogique A0 de l'Arduino (xPin = A0).
- **Axe Y (Y-axis)** : connecté à la broche analogique A1 de l'Arduino (yPin = A1).

Le montage ci-dessous illustre les connexions entre le joystick et l'Arduino :

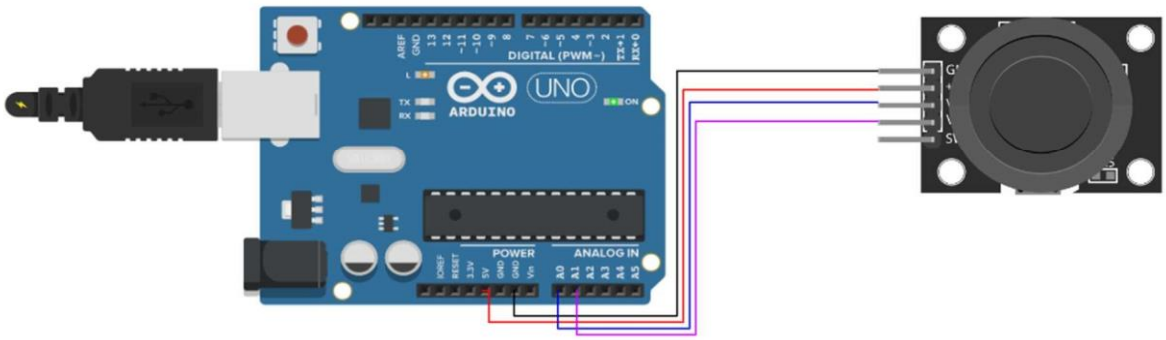

Figure 4.45: Schéma de connexion entre l'Arduino Uno et le joystick réalisé sur EasyEDA

4.2.3 Montage de la réalisation

• Émetteur

Notre émetteur est conçu autour de trois composants clés : un joystick, une carte Arduino Uno et un module LoRa RA-01. Décrivons le rôle de chacun dans la chaîne de transmission :

- **Joystick :** Notre joystick sert d'interface de contrôle. Ses mouvements sur les axes X et Y sont traduits en valeurs analogiques, représentant les commandes à transmettre.
- **Arduino Uno :** L'Arduino Uno est le cœur de notre émetteur. Il reçoit les valeurs analogiques du joystick, les traites, et les cryptes grâce à notre système de cryptage, assurant ainsi la sécurité de la transmission.
- **Module LoRa RA-01 :** Notre module LoRa RA-01 assure la transmission sans fil des données cryptées. Il reçoit les données de l'Arduino et les transmet sur 433 MHz, nous permettant une communication longue portée et basse consommation. La modulation LoRa assure robustesse et portée étendue.

L’image ci-dessous montre le montage final de l’émetteur, avec le joystick relié à l’Arduino, et le module LoRa connecté pour la transmission des données cryptées :

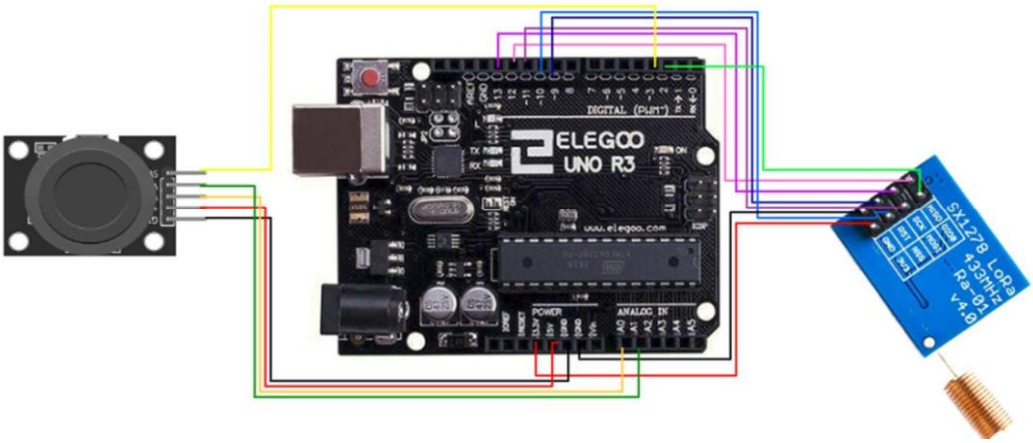

Figure 4.46: Schéma du circuit de l'emetteur réalisé sur EasyEDA

• Récepteur

Notre récepteur se compose d'un module LoRa RA-01, d'une carte Arduino Uno, de LEDs et de résistances. Chaque composant joue un rôle précis :

- **Module LoRa RA-01 :** Il réceptionne les données transmises par l'émetteur sur 433 MHz, capturant ainsi les signaux radio contenant les informations cryptées.
- **Arduino Uno :** L'Arduino Uno gère la logique du récepteur. Il reçoit les données du module LoRa, les décrypte à l'aide de notre système de décryptage correspondant à celui de l'émetteur, et les interprète comme des instructions. Par exemple, si le joystick de l'émetteur est poussé vers le haut, les données décryptées indiqueront à l'Arduino d'allumer la LED correspondante au mouvement "haut".
- **LEDs :** Les LEDs visualisent les commandes reçues. Suivant les données décryptées par l'Arduino, la LED correspondant à la direction du joystick (haut, bas, gauche, droite, etc.) s'allumera. Ainsi, si le joystick est déplacé vers le bas, la LED "bas" du récepteur s'allumera.
- **Résistances :** Connectées en série avec les LEDs, les résistances limitent le courant et protègent les LEDs contre les surintensités, assurant leur bon fonctionnement.

L'image ci-dessous illustre le montage final du récepteur, avec le module LoRa connecté à l'Arduino, lequel contrôle l'allumage des LEDs en fonction des données décryptées :

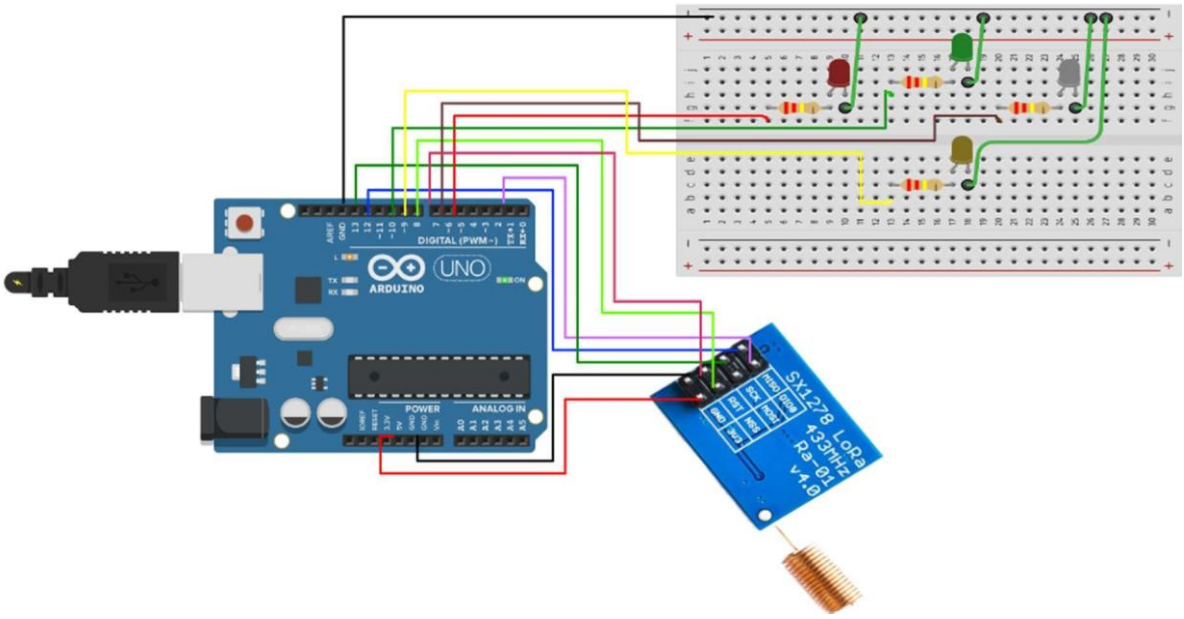

Figure 4.47: Schéma du circuit du récepteur réalisé sur EasyEDA

PARTIE LOGICIELLE

4.3 Présentation de l'IDE Arduino

4.3.1 Définition de l'IDE

L'IDE Arduino (Integrated Development Environment) est un environnement de développement intégré open-source, conçu pour permettre la programmation de microcontrôleurs comme les Arduino, ESP32, et autres cartes compatibles. Cet outil simplifie considérablement la création de projets électroniques embarqués, notamment grâce à son interface intuitive, adaptée aux débutants comme aux utilisateurs plus expérimentés.

4.3.2 Fonctionnalités et Caractéristiques Principales

L'IDE Arduino repose sur le langage de programmation Arduino, qui est basé sur le C/C++. Ce logiciel fournit aux utilisateurs un ensemble d'outils essentiels pour la programmation de microcontrôleurs :

- **Éditeur de code :** L'IDE inclut un éditeur de texte qui permet de rédiger des programmes, appelés "sketches". Ces sketches contrôlent les composants matériels reliés à la carte, tels que des capteurs ou des moteurs.
- **Vérification et compilation :** Une fois le code écrit, l'utilisateur peut vérifier sa syntaxe en cliquant sur le bouton "Vérifier". Ensuite, l'IDE compile le code pour le rendre

compréhensible par le microcontrôleur, transformant les instructions en un format binaire.

- **Téléversement :** Après la compilation, l'utilisateur peut transférer (téléverser) le programme sur la carte Arduino ou ESP32 via un câble USB. Ce processus permet au microcontrôleur d'exécuter les instructions du programme.
- **Gestion des bibliothèques :** L'IDE intègre un gestionnaire de bibliothèques qui simplifie l'ajout de fonctionnalités externes. Par exemple, les utilisateurs peuvent importer des bibliothèques pour gérer la communication sans fil, contrôler des capteurs, ou intégrer des affichages graphiques.

L'une des grandes forces de l'IDE Arduino est sa compatibilité multi-plateforme. Le logiciel fonctionne de manière identique sur Windows, Mac et Linux, garantissant une expérience fluide et cohérente quelle que soit la plateforme utilisée. La version actuelle (2.3.3) maintient une interface graphique familière tout en bénéficiant des dernières corrections de bugs et améliorations [55].

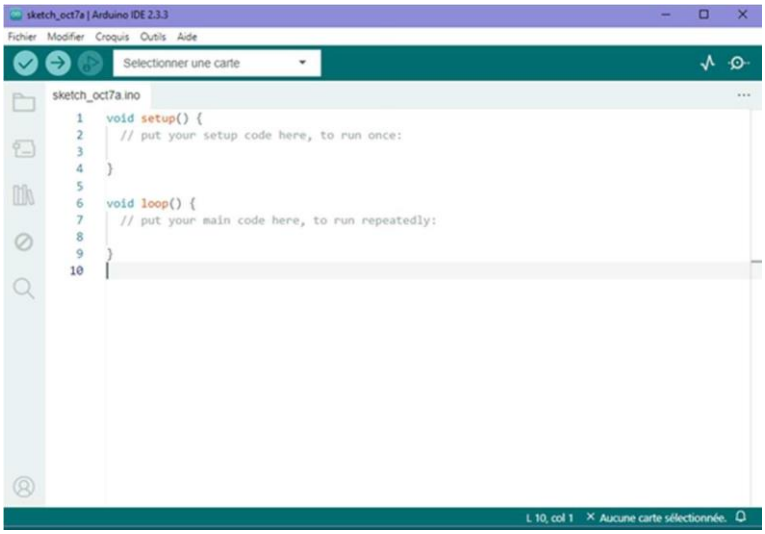

Figure 4.48: L'écran principal de l'IDE Arduino au démarrage

4.4 Installation de l'ESP32 dans l'IDE Arduino

L'intégration de l'ESP32 dans l'IDE Arduino nécessite plusieurs étapes clés. D'abord, l'URL spécifique au gestionnaire de cartes ESP32 doit être ajoutée dans les préférences de l'IDE Arduino, sous la section dédiée aux "URL de gestionnaire de cartes supplémentaires" (https://dl.espressif.com/dl/package_esp32_index.json). Ensuite, après l'ajout de cette URL, il est possible d'installer le package ESP32 en accédant au "Gestionnaire de cartes" via le menu

Outils. En recherchant "ESP32", le package correspondant peut être localisé et installé. Une fois cette installation effectuée, la carte ESP32 devient sélectionnable dans le menu des cartes disponibles, permettant ainsi de la programmer de manière similaire à une carte Arduino classique.

4.5 Bibliothèques Utilisées

4.5.1 Bibliothèque LoRa

La bibliothèque LoRa permet d'implémenter la technologie LoRa (Long Range), un protocole de communication sans fil longue portée et à faible consommation d'énergie. Elle est particulièrement adaptée aux projets nécessitant une couverture étendue avec une faible utilisation de puissance.

- **Fonctionnalité :** Elle facilite l'envoi et la réception de données entre dispositifs compatibles avec LoRa, offrant une solution idéale pour des communications sans fil à faible consommation.
- **Installation :** La bibliothèque LoRa peut être installée directement dans l'IDE Arduino en accédant à Croquis > Inclure une bibliothèque > Gérer les bibliothèques, puis en recherchant "LoRa". Une fois installée, elle est prête à être utilisée dans vos projets.

4.5.2 Bibliothèque SPI

La bibliothèque SPI (Serial Peripheral Interface) est utilisée pour permettre une communication rapide entre une carte microcontrôleur (comme l'Arduino Uno) et divers périphériques externes, tels que des capteurs ou des modules LoRa. Le protocole SPI est un protocole de communication série qui assure une transmission de données rapide et fiable entre le microcontrôleur et les dispositifs connectés.

- **Fonctionnalité :** Cette bibliothèque est essentielle pour interfacer la carte avec des composants matériels externes nécessitant une communication rapide, y compris les modules de transmission LoRa.
- **Installation :** Tout comme la bibliothèque LoRa, la bibliothèque SPI doit être installée manuellement via l'IDE Arduino. Pour ce faire, allez dans Croquis > Inclure une bibliothèque > Gérer les bibliothèques, puis recherchez "SPI" pour l'installer.

Grâce à la bibliothèque SPI, il devient facile de gérer les échanges de données à haute vitesse entre la carte et les périphériques connectés, garantissant une communication fluide et efficace.

4.6 Perspective futurs

Pour notre projet de communication sécurisée, nous avons utilisé les cartes ESP32 et Arduino Uno, mais leurs limitations suggèrent des améliorations possibles. L'intégration de plateformes avancées comme le STM32 et l'Arduino Portenta permettrait d'accroître les performances et la sécurité de notre système. Ces microcontrôleurs, avec leurs capacités de calcul et de connectivité optimisées, seraient des atouts pour renforcer la robustesse et l'efficacité de notre solution.

4.6.1 Carte STM32

Le STM32 est un microcontrôleur puissant basé sur l'architecture ARM Cortex, offrant une large gamme de périphériques intégrés tels que les interfaces SPI, I2C, USART, ainsi que des convertisseurs ADC et DAC. Cette diversité en fait un choix idéal pour gérer des connexions avec divers capteurs et modules, tout en renforçant la sécurité des communications grâce à des algorithmes de cryptage avancés.

Un des atouts majeurs du STM32 est son écosystème de développement robuste, soutenu par STMicroelectronics. L'environnement de développement intégré STM32CubeIDE, associé à la bibliothèque STM32CubeMX, simplifie considérablement la configuration des périphériques et de l'horloge. Ces outils, combinés à la bibliothèque STM32CubeHAL, facilitent l'initialisation et la gestion des périphériques, rendant le processus de développement plus efficace. De plus, le recours à des environnements tiers comme Keil ou IAR Embedded Workbench permet d'accéder à des fonctionnalités avancées pour le développement et le débogage des applications. Les outils tels que ST-Link assurent un débogage et une programmation efficaces des microcontrôleurs STM32, garantissant ainsi une mise au point optimale du code.

Les capacités de calcul en virgule flottante et de traitement du signal numérique (DSP), disponibles dans certaines variantes comme celles basées sur les Cortex-M4 et M7, permettent d'accélérer le traitement en temps réel, essentiel pour les applications nécessitant des opérations de cryptage avancées. En outre, certaines versions du STM32 intègrent des options de sécurité matérielles, telles que le cryptage, la protection contre la

copie et la génération de nombres aléatoires (RNG), renforçant ainsi la protection des données.

La flexibilité de connectivité du STM32, prenant en charge des protocoles tels que UART, SPI, I2C et CAN, s'avère précieuse pour notre système, en permettant une communication adaptable aux besoins en distance et en débit, tout en optimisant la consommation énergétique. Grâce à ses modes de gestion d'énergie, comme la veille, l'arrêt et la veille prolongée, le STM32 peut garantir une transmission sécurisée et économique des données, ce qui est particulièrement avantageux dans des applications embarquées telles que les drones, où une autonomie prolongée est essentielle.

4.6.2 Carte Portenta

Le Portenta H7 est une carte microcontrôleur avancée qui se démarque par ses caractéristiques clés. Dotée d'un processeur dual-core STM32H747, elle intègre un cœur Cortex M7 fonctionnant à 480 MHz et un cœur Cortex M4 à 240 MHz. Cette architecture permet l'exécution simultanée de tâches en parallèle, offrant ainsi une grande flexibilité pour divers projets.

En matière de connectivité, le Portenta H7 est équipé d'un module sans fil qui gère à la fois le WiFi et le Bluetooth. Le WiFi peut fonctionner en mode point d'accès ou station, avec des débits allant jusqu'à 65 Mbps, ce qui est idéal pour les applications IoT.

La carte est également compatible avec l'Arduino IoT Cloud, facilitant la connexion et le contrôle des dispositifs à distance. Grâce à son GPU Chrom-ART et à son encodeur/décodeur JPEG intégré, elle permet de créer des interfaces utilisateur riches et de gérer des applications graphiques.

Le Portenta H7 prend en charge l'exécution de modèles de machine learning via TensorFlowLite, ce qui le rend adapté aux applications de vision par ordinateur et d'intelligence artificielle. De plus, il propose une variété d'interfaces d'E/S, y compris UART, SPI, I2C, et Ethernet, accessible via des connecteurs à haute densité.

Pour l'alimentation, le Portenta H7 utilise un connecteur USB-C, qui peut non seulement alimenter la carte, mais aussi servir de hub USB ou connecter un moniteur via DisplayPort. Cela lui confère une grande polyvalence dans la conception de projets.

Conclusion

En conclusion, cette phase initiale de développement et de test de notre système de cryptage et de transmission de données a démontré sa robustesse et son efficacité dans un environnement simulé. Les choix techniques et les configurations expérimentées se sont révélés bien adaptés aux exigences de portée, de sécurité et de consommation énergétique. Ces résultats prometteurs posent les bases d'une future intégration sur un drone, avec des perspectives d'optimisation via des cartes plus performantes, telles que l'Arduino Portenta ou la STM32, pour renforcer encore les capacités et la fiabilité de notre dispositif.

Conclusion

Conclusion générale

Ce travail explore la conception et la réalisation d'un système de cryptage de données pour la transmission entre un drone et sa télécommande, en mettant en lumière l'utilisation d'une approche chaotique pour renforcer la sécurité des communications. À travers une analyse théorique approfondie et une validation expérimentale, il démontre que l'oscillateur chaotique pour ce projet, offre une solution efficace pour garantir la confidentialité et l'intégrité des données échangées.

L'évolution rapide des drones et leur intégration dans des secteurs aussi divers que l'agriculture, la surveillance ou la cartographie soulignent l'importance de sécuriser les transmissions entre ces appareils et leurs contrôleurs. Le recours aux systèmes chaotiques pour le cryptage, grâce à leurs propriétés uniques comme la sensibilité aux conditions initiales et le comportement imprévisible, s'avère particulièrement pertinent dans ce contexte. Un prototype expérimental, basé sur des cartes Arduino Uno et des modules LoRa, a été mis en œuvre pour simuler les communications, mais cette expérimentation reste provisoire avant d'être testée sur un drone réel. Elle a néanmoins confirmé la capacité du système à sécuriser et synchroniser les données dans un environnement de communication sans fil.

Les résultats obtenus démontrent clairement le potentiel des systèmes chaotiques pour améliorer la sécurité des communications embarquées, en particulier pour les drones. Cependant, des optimisations sont nécessaires, notamment avec l'intégration de plateformes matérielles plus performantes, afin d'améliorer la vitesse et la capacité de traitement parallèle. Les applications de cette méthode s'étendent également à d'autres dispositifs connectés, notamment dans l'Internet des objets (IoT), où la sécurisation des données est un enjeu crucial.

Ce projet prouve la faisabilité et l'efficacité d'un cryptage chaotique pour les communications drone-télécommande, tout en ouvrant la voie à des améliorations futures.

Bibliographie

[1] mieux-connaitre-les-drones (onera.fr)

[2] https://tpedrone.home.blog/la-naissance-du-drone/

[3] https://www.drone-malin.com/pages/en-savoir-plus/les-drones/c-est-quoi-un-drone.html

[4] https://htpratique.com/types-drones/.

[5] https://builtin.com/drones.

[6] https://www.drone-actu.fr/drone/innovations-technologiques-domaine-drones

[7] https://www.drone-actu.fr/drone/innovations-technologiques-domaine-drones

[8] Théorie du chaos – Wikipédia.

[9] Chaos et hasard - Les Echos

[10] Britannica, Les éditeurs de l'encyclopédie. « Théorie du chaos ». Encyclopédie Britannica, 1er juin 2024, https://www.britannica.com/science/chaos-theory.

[11] K. T. Alligood, T. D. Sauer and A. J. Yorke, Chaos: An introduction to dynamical systems, Springer-Verlag, New York, 1996.

[12] F. Beritelli, E. D. Cola and L. Fortuna, Multilayer chaotic encryption for secure communications in pachet switching networks, IEEE Transactions on communication, vol. 30, no. 4, pp. 1575–1582, 2000.

[13] W. Liu and G. Chen, A New Chaotic System and its generation, International Journal of Bifurcation and Chaos, vol. 13, no. 1, pp. 261–267, 2003.

[14] H. HAMICHE, Thèse De Doctorat « Inversion à Gauche des Systèmes Dynamiques Hybrides Chaotiques. Application à la Transmission Sécurisée de Données », Tizi Ouzou, 2011.

[15] K. HANNOUN, Mémoire de Fin d'Etudes de master académique « Etude, Simulation et implémentation d'un émetteur hyper chaotique sur carte Arduino Uno. », Tizi Ouzou, 2014.

[16] Mangiarotti, Sylvain, et Christophe Letellier. La théorie du chaos fête ses 130 ans : quelles sont ses applications aujourd'hui ? Université de Rouen Normandie. https://www.univrouen.fr/actualites/la-theorie-du-chaos-fete-ses-130-ans-quelles-sont-ses-applicationsaujourdhui/ Alvarez, Aurélien. L'attracteur de Lorenz.

[17] IMAGINARY. https://www.imaginary.org/fr/gallery/lattracteur-de-lorenz.

[18] M.MAMMERI,Mémoire Présenté pour l'obtention du diplôme de MAGISTER, "Sur la stabilité Structurelle des Difféomorphismes Quadratiques en Dimension 2",OUARGLA,2011.

[19] Marot, J.C. Les bifurcations de Feigenbaum ou cascade de doublements de période [PDF]. (2021).

[20] H. ZERROUKI, Mémoire De Master, « Diagramme de bifurcation d'une dynamique non linéaire simulée », Bouira, 2021.

[21] C. ABDELDJALIL & F. ABDELHAK, Mémoire De Master, « Implémentation d'un système de transmission sécurisée des données à base de chaos sur carte Arduino », Blida, 2021.

[22] O. MEGHERBI, Mémoire De Magister « Etude et réalisation d'un système sécurisé à base de systèmes chaotiques », Tizi-Ouzou, 2013.

[23] Lorenz, Edward N. Deterministic Nonperiodic Flow, Journal of the Atmospheric Sciences, 1963.

[24] Devaney, Robert L. Chaos: An Introduction to Dynamical Systems, Westview Press, 1989.

[25] Gleick, James. Chaos: Making a New Science, Penguin Books, 1987.

[26] Strogatz, S.H. Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering (2nd ed.). CRC Press, 2015.

[27] L. OMARI & K. OUALI, Mémoire De Master, « Conception d'un crypto-système à base des systèmes chaotiques : Application à la transmission d'un message audio », Tizi-Ouzou, 2022.

[28] A. Berkane, « Transmission sécurisé a base de la synchronisation impulsive de deux systèmes chaotique discrets », Mémoire de Master, département d'électronique, Université Mouloud Mammeri, Tizi-Ouzou, 2016.

[29] ZHAO, Hongxiang, XIE, Shucui, ZHANG, Jianzhong, et al. A dynamic block image encryption using variable-length secret key and modified Henon map. Optik, 2021, vol. 230, p. 166307.

[30] https://www.futura-sciences.com/tech/definitions/tech-cryptologie-4565/

[31]https://www.larousse.fr/dictionnaires/francais/cryptographie/20864?q=cryptographie#20

[32] https://www.larousse.fr/dictionnaires/francais/cryptanalyse/10910295

[33] Dumont. R, " Cryptographie et Sécurité informatique", livre informatique, 2009 - 2010.

[34] https://goferproject.wordpress.com/

[35] https://etablissementbertrandeborn.net/IMG/pdf/indice9_maths.pdf

[36]https://www.frenchweb.fr/petit-histoire-de-la-cryptographie-de-jules-cesar-a-lordinateurquantique/257767

[37] https://fr.vikidia.org/wiki/Chiffre_de_Vigen%C3%A8re

[38] https://www.apprendre-en-ligne.net/crypto/subst/playfair.html

[39] https://fr.wikipedia.org/wiki/Cryptographie_sym%C3%A9trique

[40] S. G. Lian, J. Sun and Z. Wang, “A Novel Image Encryption Scheme Based-on JPEG Encoding”, Proceedings of 8th International Conference on Information Visualization, pp. 217220, 2004.

[41] R. Kusters and M Tuengerthal, “Universally Composable Symmetric Encryption”, The 2 nd IEEE Computer Security Foundations Symposium (CSF), pp. 293- 307, July 2009. [42] W. Diffie and M. E. Hellman. “New directions in cryptography”. IEEE Transactions on Information Theory (IT), Vol. 22, No. 6, pp.644–654, November 1976.

[43] B. Martin, Codage, cryptologie et applications, Presses polytechniques et universitaires Romandes, 2004.

[44] Karaali, Djamila.Synchronisation des quelques systèmes chaotiques. Mémoire de magister, Université de Constantine 2007.

[45] https://www.chosesasavoir.com/quel-est-le-mystere-des-pendules-synchrones/

[46] Habib Dimassi. Synchronisation des systèmes chaotiques par observateurs et applications à la transmission d'informations. Autre [cond-mat.other]. Université Paris Sud - Paris XI; Université de Tunis El Manar, 2012. Français. ⟨NNT : 2012PA112255⟩.

[47] ROSTANE, Aboubekr Essedik. Observateur à mode glissant d’ordre suppérieur et inversion à gauche. 2014. Thèse de doctorat.

[48] M. HALIMI, Thèse De Doctorat, « Observation et détection de modes pour la synchronisation des systèmes chaotiques : une approche unifiée », Lorraine, 2013.

[49] F. Anstett. Les systèmes dynamiques chaotiques pour le chiffrement synthèse et cryptanalyse.2006.

[50] Pham, C. *Cours Arduino*. Université de Pau et des Pays de l'Adour.https://cpham.perso.univ-pau.fr/ENSEIGNEMENT/PAU-UPPA/RESA-M2/DOC/coursArduino.pdf

[51] "Qu'est-ce que Arduino ? Définition et description simple." *Positron-libre*, https://www.positron-libre.com/electronique/arduino/arduino.php

[52] [52]Bartmann, Erik. *Legrandlivred'Arduino* .Eyrolles, 2018.

http://www.multimedialab.be/doc/erg/2018/2019/Arduino/Le_grand_livre_d_Arduino_Erik_Bartmann_Eyrolles_2018/Le_grand_livre_d_Arduino_Erik_Bartmann_Eyrolles_2018.pdf

[53] J.Denéchaud, Rapport de projet de fin d’étude : Sécurité de l’internet des objets, 2017.

[54] GUILLAUME Schreiner, JEAN Melounou, MANUEL Yguel. Retour d’expérience d’un déploiement LoRaWAN à Strasbourg, 2019.

[55] H.E. BENHAMZA & A. DJOUADA, Projet de Fin de Cycle, « Étude et Réalisation d'une Carte Électronique de Gestion d'un Afficheur LCD », Bordj Bou Arreridj, 2022.

[56] K. ZAZOUN & A. LALLAL, Mémoire de Master, « Détection de feux de forêts par drone en mission planifiée »,Tizi-Ouzou,2020.

[57] LAFOREST, M., & SAUCIER, A, Le chaos dans les équations de Lorenz. Éditeur ou publication (si applicable).

[58] Harir, Y., & Mecheri, H. La coexistence de la synchronisation généralisée et la synchronisation généralisée inverse entre deux systèmes chaotiques et hyper chaotiques. Université de Tébessa, 2021.

[59] Benayad, H., & Elmokrefi, A. Synchronisation entre deux systèmes hyper-chaotiques. Université Saad Dahlab Blida 1, 2022.

[60] E. Cherrier. Estimation de l'état et des entrées inconnues pour une classe de systèmes non linéaires.Thèse de doctorat, 2006.

[61] Chabane, A., & Fechit, A. Implémentation d'un système de transmission sécurisée des données à base de chaos sur carte Arduino. Université des Sciences et de la Technologie d'Oran Mohamed Boudiaf, 2021.