الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne démocratique et populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique
جامعة سعد دحلب بالبليدة
Université SAAD DAHLAB de BLIDA 1
كلية التكنولوجيا
Faculté de Technologie
قسم الإلكترونيك
Département d'Électronique

Mémoire de master

Mention Électronique

Spécialité : Instrumentation Biomédicale

Présenté par :

Bouaiache Amina

&

Djezairi chaima

IMPLEMENTATION FPGA D'UNE TRANSMISSION SECURISE PAR CHAOS DE L'ECG (électrocardiogramme)

Encadré par :

Mr. CHIKHI. Med Lazhar.

Année Universitaire 2017-2018

Remerciements

Tout d'abord, nous tenons à remercier Mr CHIKHI.L de nous avoir encadrés. Ses conseils et son expérience ont beaucoup aidé à la réussite de notre travail.

Les travaux présentés dans ce mémoire ont été effectués au Laboratoire LABSET du département d'électronique de l'université de Blida 1. Nos remerciements les plus sincères vont à tous les membres du laboratoire qui nous ont permis de réaliser ce travail dans de très bonnes conditions.

Nous exprimons notre profonde gratitude à notre chef de filière Mr CHERFA.Y ainsi qu'à tous nos professeurs.

Enfin, nous remercions nos parents pour leur soutien et leurs encouragements pendant toute la période de préparation de ce mémoire.

Résumé

Les systèmes chaotiques sont des systèmes dynamiques non linéaires, qui sont déterministes et sensibles aux conditions initiales. Dans ce travail, on a étudié et réalisé une transmission sécurisée de l'électrocardiogramme basée sur le multiplexage et le démultiplexage temporel. Le signal message est ajouté au signal chaotique de Colpitts afin de le crypter, en utilisant la méthode de cryptage par addition. Le message crypté est multiplexé avec le signal chaotique et est transmis. Au niveau du récepteur, le démultiplexeur reçoit le signal multiplexé, en soustrayant les deux sorties de ce dernier, on récupère le signal message (ECG). Les résultats de simulation sous environnement Matlab Simulink-Xilinx System Generator sont présentés, et une implémentation sur circuit FPGA de la transmission chaotique est réalisée avec une présentation des résultats expérimentaux.

Abstract

Chaotic systems are nonlinear dynamic systems which are deterministic and sensitive to initial conditions. In this work, we studied and realized a secure transmission of the electrocardiogram based on multiplexing and time demultiplexing**.** The message signal is added to the chaotic signal of Colpitts in order to encrypt it using the addition encryption method. The encrypted message is multiplexed with the chaotic signal and is transmitted. At the receiver, the demultiplexer receives the multiplexed signal, substracting his two outputs, the message signal is recovered. Simulink –Xilinx System Generator simulation results are presented and an FPGA implementation of chaotic transmission is performed with a presentation of the experimental results.

الملخص

الأنظمة الفوضوية هي أنظمة ديناميكية غير خطية تتسم بالحساسية للظروف الأولية. في هذا العمل, درسنا و أدركنا النقل الآمن لمخطط كهربية القلب بناء على أساس تعدد الإرسال الزمني. تضاف إشارة الرسالة إلى إشارة Colpitts الفوضوية من أجل تشفيرها وذلك باستخدام طريقة التشفير بالإضافة. يتم إرسال الرسالة المشفرة مع الإشارة الفوضوية. في المستقبل, يستقبل مزيل التعدد الإشارة المتعددة الإرسال بطرح مخرجي هذا الأخير يتم استرجاع إشارة الرسالة. يتم عرض نتائج المحاكاة في بيئة Matlab Simulink-Xilinx System Generator كما يتم تنفيذ تطبيق نظام الإرسال الفوضوي في دارة FPGA مع عرض نتائج التجارب.

Liste des symboles et des abréviations

x : Vecteur d'états du système.

x_0 : Point initial.

μ : Paramètre de bifurcation.

y : Vecteur de sortie du système.

$\dot{x} = \frac{dx}{dt}$: Dérivée de la variable x par rapport au temps.

$\mathbb{R}$: Ensemble des nombres réels.

$\mathbb{R}^n$: Espace vectoriel de dimension n .

$U \subseteq \mathbb{R}^n$: Espace d'états.

$\bar{x}$: Point fixe.

$Df(x)$: Matrice Jacobienne.

λ_i : Valeur propre.

$\sum_p$: Surface de dimension n -1 .

λ_i : Exposant de Lyapounov.

α : Gain en courant de transistor en base commune.

g : Gain de la boucle de réaction.

ω : Pulsation angulaire.

diag [λ_i] : Matrice diagonale.

ECG : Electrocardiogramme.

CSK : Chaos Shift Keying.

TDM : Time Division Multiplexer.

TDD : Time Division Demultiplxer.

VLSI : Very Large Scal Integration.

CAO : Conception Assistée par Ordinateur.

FPGA : Field Programmable Gate Array.

CPLD : Complex Programmable Logic Devise.

CAN : Convertisseur Analogique Numérique.

CNA : Convertisseur Numérique Analogique.

VLSI : Very Large Scal Integration.

CLB : Configurable Logic Bloc.

HDL : Hardware Description Language .

Table des matières

Liste des illustrations, graphiques et tableaux

Introduction générale

Les maladies cardiovasculaires représentent la cause la plus fréquente de décès dans le monde selon les études statistiques annuelles faites au niveau de l'organisation mondiale de la santé (OMS) [1]. Par conséquent, le signal électrocardiogramme (ECG) reflète l'activité électrique du cœur et constitue ainsi l'un des outils le plus prédominant et le plus utilisé pour diagnostiquer les anomalies cardiaques.

Le besoin de cryptage du signal ECG ne peut être que trop souligné, car d'une part, les dossiers des patients doivent souvent passer d'un expert à un autre et d'autre part, les enregistreurs portables d'ECG permettant aux patients d'utiliser leurs propres enregistrements. Ces enregistrements sont régulièrement signalés à un centre médical pour une analyse. Récemment, afin de réduire le coût et d'améliorer le service, les formes électroniques de dossiers médicaux ont été envoyés par des réseaux des laboratoires aux centres médicaux ou aux cabinets médicaux. Dans tous ces cas, le signal ECG doit être crypté pour protéger l'intimité du patient.

La cryptographie composée des mots grecs kruptos (caché, secret) et graphien (écrire), est la science des écritures secrètes. Elle recouvre l'étude et la conception des procédés de chiffrement des informations ; elle est devenue aujourd'hui un moyen quotidien de protection des données qui doivent être communiquées ou stockées sur une longue période. Les principes de bases de la cryptographie moderne reviennent à Auguste Kerkhoff, énoncés dans son article intitulé " La cryptographie militaire " publié en 1883 et dont l'idée la plus importante est que la sécurité du chiffre ne doit pas dépendre de ce qui ne peut être facilement changé. En d'autres termes, aucun secret ne doit résider dans l'algorithme de cryptage mais plutôt dans la clé. Le temps de calcul des algorithmes est long, ce qui entraîne une diminution du débit des messages transmis. Il y'a aussi la question de réduction du niveau de confidentialité dans ces algorithmes. Ces failles ont poussé les recherches vers le développement de nouveaux systèmes. L'usage du chaos a été une des alternatives proposées.

En 1963, le météorologue Edward Lorenz expérimentait une méthode lui permettait de prévoir les phénomènes météorologiques. C'est par pur hasard qu'il observa qu'une modification minime des données initiales pouvait changer de manière considérable ses résultats. Lorenz venait de découvrir le phénomène de sensibilité aux conditions initiales. Les systèmes répondants à cette propriété seront à partir de 1975 dénommés : systèmes chaotiques.

La cryptographie chaotique est un mode de communication à clé secrète, la connaissance de cette clé est nécessaire pour le chiffrement et le déchiffrement du message. Alors on doit disposer au niveau du récepteur, d'un signal chaotique identique à la porteuse

pour pouvoir récupérer le message masqué. Pour résoudre ce problème, en 1990, T.Pecora et L.Caroll ont réussi à reproduire de manière exacte un signal électrique en synchronisant deux signaux chaotiques. Cette découverte a permis d'utiliser le chaos comme moyen de modulation de l'information. Les propriétés des systèmes chaotiques (spectre continu et sensibilité aux conditions initiales) font de ces systèmes de bons candidats pour la cryptographie. Malgré l'allure aléatoire et imprédictible à long terme du chaos, ce type de systèmes reste déterministe.

Notre projet consiste à étudier et à réaliser un système de transmission sécurisée du signal ECG à base du chaos. Pour cela, on a transmis l'électrocardiogramme avec un système chaotique basé sur la synchronisation par multiplexage temporel. Le signal message est ajouté au signal chaotique généré par l'oscillateur de Colpitts pour le cryptage par la méthode dite d'addition. Le signal crypté est multiplexé avec le même signal chaotique et transféré. Le signal transmis est décrypté avec le démultiplexeur temporel, en soustrayant les deux sorties de démultiplexeur pour récupérer le signal message. Le système de transmission chaotique sera implémenté sur la carte FPGA. Le signal message reconstitué au niveau du la partie réceptrice est visualisé sur l'oscilloscope numérique, grâce à une carte de conversion analogique-numérique (pour l'inclusion du message) et numérique-analogique (pour la visualisation) intégrés au niveau du codec AC97 de la carte FPGA ML501-VIRTEX 5. Une simulation sous les environnements Matlab-Simulink et System Generator-Xilinx nous permettra de comparer les signaux obtenus par simulation et ceux provenant de la carte FPGA et de valider la bonne transmission sécurisée du système de communication.

Ce mémoire est ainsi organisé comme suit :

Le premier chapitre est un rappel sur le système cardiovasculaire avec une description de l'électrocardiogramme.

Le second chapitre présente des définitions de base des systèmes dynamiques chaotiques tels que le point fixe, la stabilité de point fixe, la bifurcation, etc…, qui seront utilisées pour l'analyse de l'oscillateur chaotique de Colpitts.

Dans le troisième chapitre, les différents types de transmissions sécurisées par chaos seront présentés ainsi que la méthode utilisée. La notion de multiplexage et de démultiplexage temporel va être décrite afin d'avoir une synchronisation entre l'émetteur et le récepteur afin d'optimiser l'implémentation hardware de notre système.

Le dernier chapitre sera consacré à implémenter la transmission sécurisée par chaos sur le circuit FPGA VIRTEX 5 ainsi qu'à la présentation des résultats expérimentaux et leurs comparaison avec les résultats simulés.

On termine par une conclusion générale qui reprend tous les points abordés dans ce mémoire ainsi que quelques perspectives qui pourront être développées ultérieurement.

Chapitre 1

Généralités sur l'électrocardiogramme

L'électrocardiographie correspond à la traduction du fonctionnement du cœur sous forme électrique à travers des électrodes cutanées positionnées dans différents points du corps humain.

L'électrocardiogramme est le signal biomédical le plus étudié pour caractériser les anomalies cardiaques ; l'analyse de ces enregistrements permet ainsi de diagnostiquer un grand nombre de pathologies [1].

Dans ce chapitre, nous présentons le fonctionnement général du système cardiovasculaire, ses principales composantes, puis le principe de l'électrocardiographie et les caractéristiques du cycle cardiaque ainsi que son processus de propagation. Pour une bonne compréhension, des nombreux ouvrages médicaux disponibles sur le sujet comme [2][3][4] .

1.1 Anatomie du cœur:

Le cœur est un organe musculaire creux comparable à une pompe qui assure la circulation du sang dans les veines et les artères. Il est connecté au reste de l'organisme par le biais de vaisseaux associés : les deux veines caves (inférieure et supérieure), les artères pulmonaires, et l'artère aorte, comme l'illustre la figure (1.1). Il se situe dans la cage thoracique, dans un espace appelé médiastin antérieur, et plus précisément entre les deux poumons, en arrière du sternum, en avant de la colonne vertébrale et au dessus de diaphragme.

Le cœur est un muscle brin rouge qui pèse chez l'adulte entre 300 et 350g et mesure environ 13 cm de long, 8 cm de large et bat 3 milliard de fois dans une vie. Il a une forme de pyramide triangulaire dont le sommet est en bas. Il est séparé en deux moitiés (droite et gauche), chacune des moitiés comporte une oreillette et un ventricule qui communiquent entre eux par des valves (tricuspide à droite, mitrale à gauche) qui empêchent le sang de se refluer.

La partie droite contient le sang pauvre en oxygène et assure la circulation pulmonaire, la partie gauche renferme du sang riche en oxygène, qui est propulsé dans tous les tissus.

Les parois du cœur sont constituées par un muscle cardiaque appelé « myocarde » (Figure 1.2), il est composé d'Endocarde, myocarde, épicarde, la cavité péricardique et le péricarde, le cœur assure une pression sanguine suffisante et un débit cardiaque égale presque à 6 L/min dépendant des besoins de l'organisme [2].

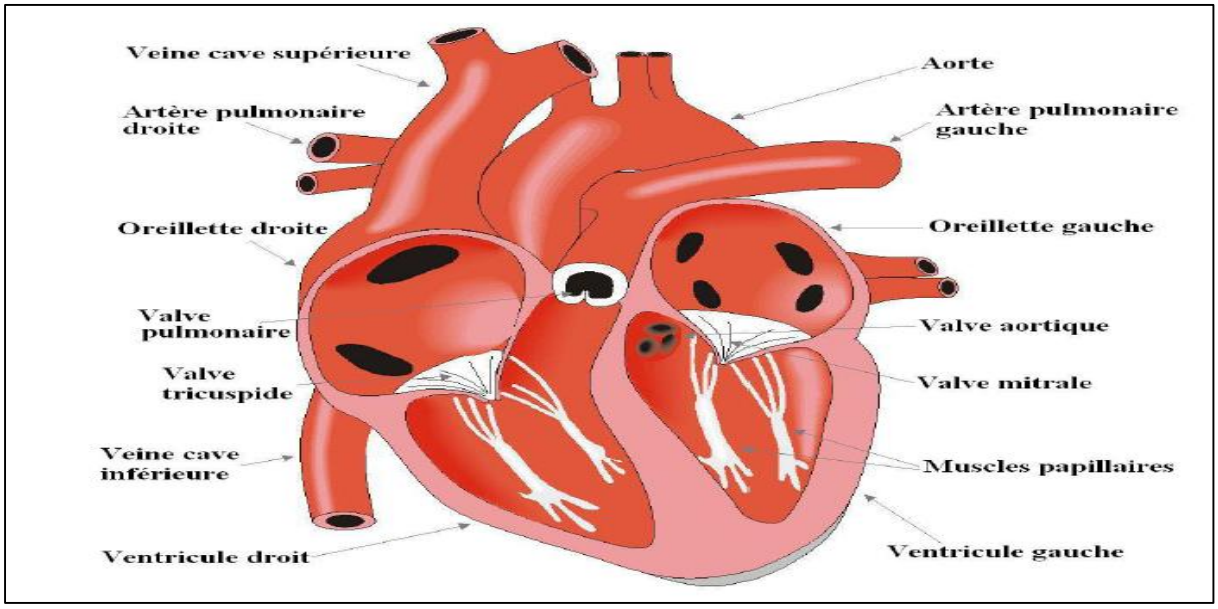


Figure 1.1. Système cardiovasculaire [1]**.**

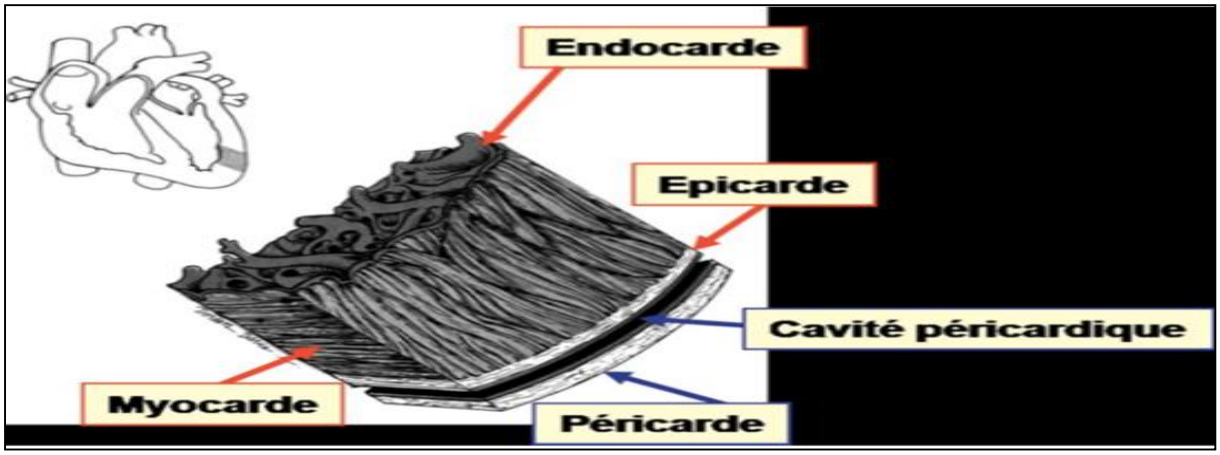


Figure 1.2. Myocarde [2].

1.2 Cycle cardiaque:

Le cycle cardiaque est une séquence d'évènements mécaniques et électriques entraînée par chaque battement du cœur. Il est constitué de trois étapes majeures : la systole auriculaire, la systole ventriculaire et la diastole.

La systole auriculaire : les oreillettes se contractent et projettent le sang vers les ventricules. Dès que le sang est expulsé des oreillettes, les valvules auriculo-ventriculaires se ferment pour éviter un reflux du sang vers les oreillettes.

La systole ventriculaire : les ventricules se contractent et expulsent le sang vers le système circulatoire (Figure1.3). Une fois le sang expulsé, les valvules (pulmonaire à droite et aortique à gauche) se ferment.

La diastole : est la période de relaxation cardiaque et de remplissage des oreillettes par les veines.

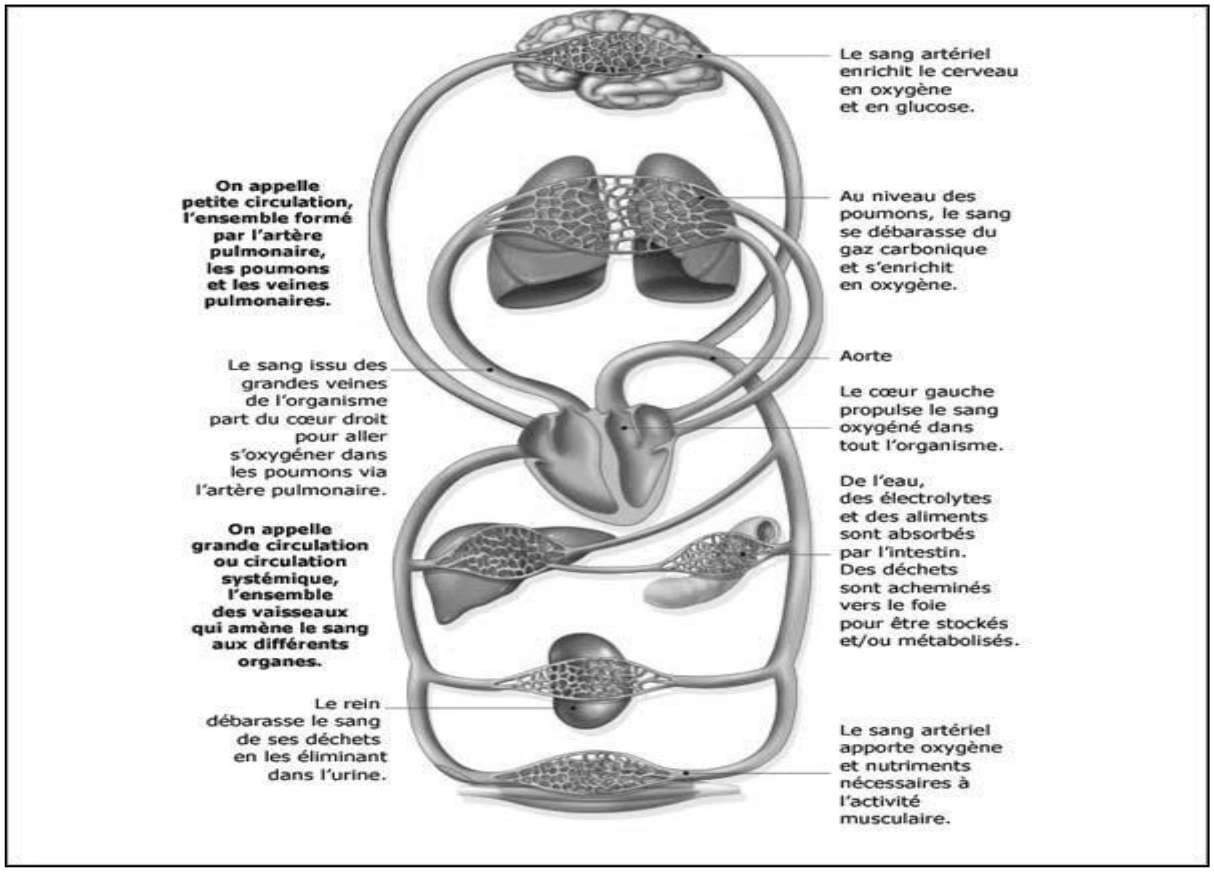


Figure1.3. Circulation sanguine.

1.3 La genèse du signal électrique cardiaque:

La dépolarisation des cellules musculaires cardiaques induit une propagation d'une impulsion électrique le long des fibres musculaires cardiaques, cette dernière provoque la contraction du myocarde. L'onde d'activation naît dans l'oreillette droite, dans le nœud sinusal, situé au pied de la veine cave supérieure, ce nœud est constitué d'un ensemble de cellules auto-excitables qui génère un courant de dépolarisation 60 à 100 fois par minute. Ce nœud est considéré comme le "pacemaker" du cycle cardiaque.

Cette onde diffuse ensuite à travers les deux oreillettes, atteint le nœud auriculo-ventriculaire d'ASCHOFF-TAWARA (Figure 1.4) seul point de passage entre les oreillettes et

les ventricules situé dans le septum inter-ventriculaire. L'onde de dépolarisation subite un ralentissement à ce niveau, et elle permet aux ventricules d'être stimulés avec un certain retard par rapport aux oreillettes, ce qui favorise le remplissage ventriculaire, passif complété en fin de diastole par la contraction auriculaire. L'activation électrique auriculaire a une durée d'environ 0,10 seconde en moyenne. Le ralentissement auriculo-ventriculaire dure en moyenne de 0,12 à 0,20 seconde, et l'activation des ventricules se fait habituellement de 0,06 à 0,08 seconde.

En effet, le cœur contient un réseau intrinsèque de cellules conductrices qui génèrent et dispersent des impulsions électriques ainsi que des cellules qui réagissent à ces impulsions par une contraction.

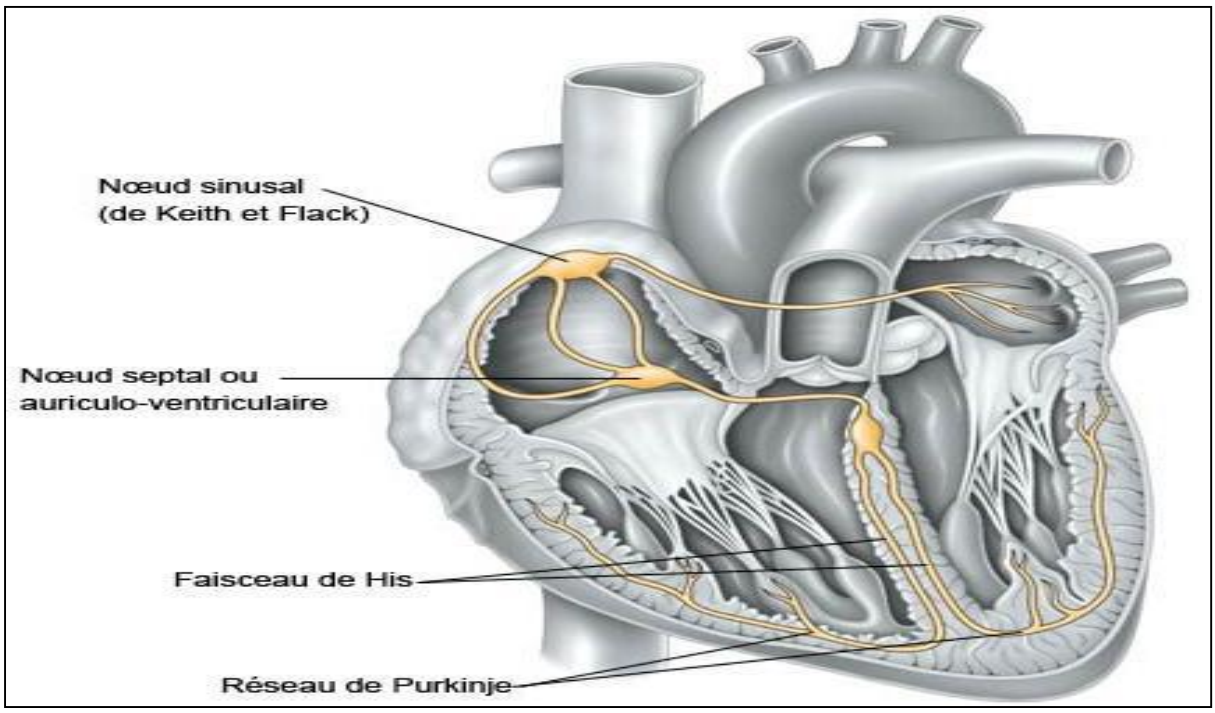


Figure1.4. Nœuds du muscle cardiaque.

1.4 Propriétés électro-physiologiques des cellules cardiaques :

Chaque cellule cardiaque est le siège d'échanges membranaires dans lesquels sont impliqués plusieurs ions (Sodium Na^+, Potassium K^+, Calcium Ca^{2+}, Chlorure Cl^-). Au cours d'un cycle cardiaque, des variations de potentiel sont observées qui correspondent au changement de perméabilité membranaire et sont liées aux échanges ioniques. Au repos, la référence prise est l'intérieur de la cellule membranaire qui est chargée négativement par

rapport à l'extérieur, cette différence de potentiel dépend des concentrations ioniques dans les milieux intra et extracellulaire. Pour les cellules ventriculaires, sa valeur est voisine de -90 mV (Figure1.5). Dés qu'une impulsion électrique d'amplitude suffisante agit sur une cellule excitable, l'intérieur de la cellule devient rapidement positif par rapport à l'extérieur à cause des échanges ioniques. Ce processus est appelé la dépolarisation cellulaire suivi par une repolarisation cellulaire (le retour de la cellule à son état de repos) [1].

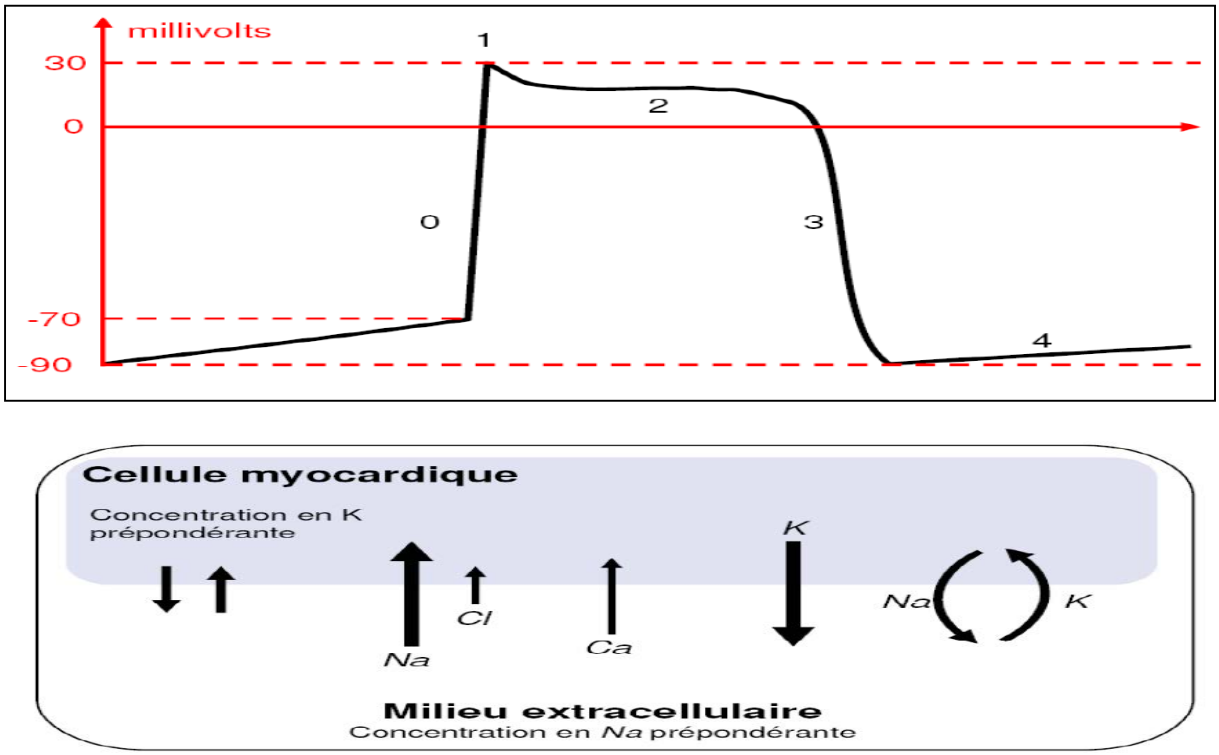


Figure1.5. Genèse du signal ECG [1]**.**

La phase 0 (dépolarisation rapide): un afflux rapide d'ions Na^+ pénètre dans la cellule et inverse immédiatement sa polarité après une excitation électrique au-dessus de seuil d'activation de cette dernière.

La phase 1 : c'est une repolarisation rapide et de courte durée dûe à l'activation des canaux K^+ et à la désactivation des canaux Na^+.

La phase 2 (Repolarisation lente) : Elle est dûe à l'activation des canaux Ca^{2+} qui atténue l'influence des canaux K^+ continuant à sortir, ce phénomène résulte d'une repolarisation lente.

La phase 3 (Repolarisation) : Elle est dûe à la fermeture des canaux ioniques spécifiques qui ramène la cellule à son état de repos, au cours de cette phase, les canaux K^+ restent toujours activés.

La phase 4 (Le repos) : Elle correspond au potentiel de repos. Durant cette phase la cellule est facilement excitée.

1.5 L'électrocardiogramme:

Un électrocardiogramme *(ECG)* désigne l'examen permettant l'enregistrement du rythme cardiaque. L'*ECG* consiste à étudier précisément l'activité du cœur, grâce à des électrodes posées sur la poitrine, les poignets et les chevilles. Cette activité est mesurée en plusieurs points du cœur, appelés dérivations. Elle est enregistrée sous la forme d'une courbe pour chacune d'entre elles. 12 dérivations sont classiquement apparentes sur le tracé et peuvent être étendues à 18 dans certaines circonstances. L'électrocardiogramme est pratiqué en cas de suspicion de maladie cardiaque.

Comme exemple, on peut citer une douleur thoracique faisant suspecter un infarctus du myocarde, pour surveiller l'évolution d'une pathologie ou pour s'assurer de l'absence d'anomalie. L'examen est rapide et indolore. L'*ECG* permet de découvrir des troubles du rythme cardiaque, des troubles de la conduction cardiaque, des signes de souffrance cardiaque.

1.5.1 Les dérivations de l'électrocardiogramme:

Une dérivation est un circuit électrique déterminé par un couple d'électrodes qui sont positionnées à des endroits bien précis, de manière à explorer le champ électrique cardiaque.

En cardiologie, pour avoir un examen ECG complet, il faut 12 dérivations. 6 explorent le plan frontal : ce sont les 3 dérivations bipolaires et les 3 dérivations unipolaires ; 6 explorent le plan horizontal : ce sont les dérivations précordiales.

- Les 3 dérivations bipolaires (Figure1.6) Ⅰ, Ⅱ, Ⅲ dites d'Einthoven :

DⅠ : enregistre les différences de potentiel électrique entre le poignet droit et le poignet gauche.

DⅡ : enregistre les différences de potentiel électrique entre le poignet droit et la jambe gauche.

DⅢ : enregistre les différences de potentiel électrique entre le poignet gauche et la jambe gauche.

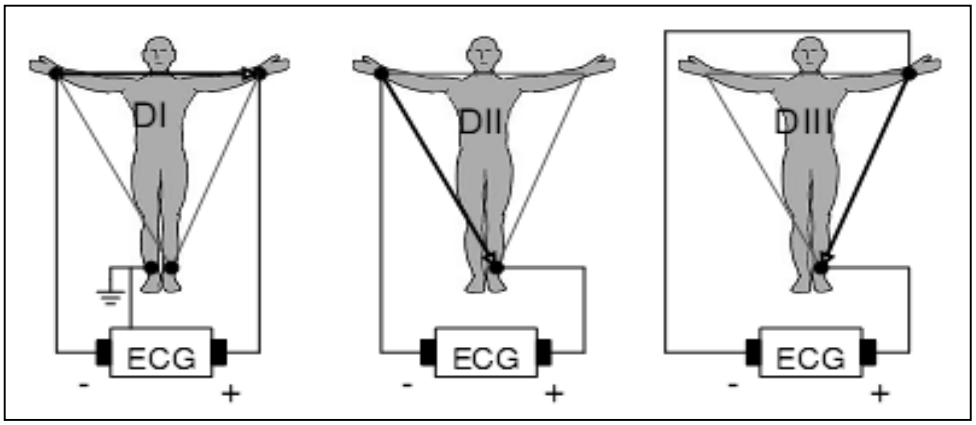


Figure1.6. Dérivations bipolaires d'Einthoven [5]**.**

- les 3 dérivations unipolaires (Figure 1.7) aVR , aVL ,aVF dites de Wilson :

  aVR : (arm , ventricular , right) l'avant -bras droit.

  aVL :(arm ,ventricular , left) l'avant -bras gauche.

  aVF :(Foot) jambe gauche.

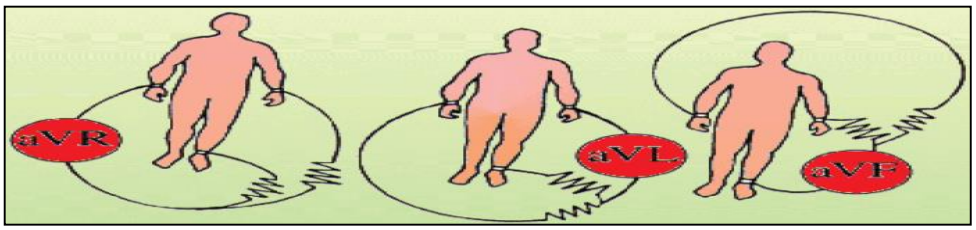


Figure1.7. Dérivations unipolaires [6].

- Les 6 dérivations précordiales (Figure 1.8) de V1 à V6 dites de Kossman :

  V1 et V2 : d'un coté et d'un autre du sternum le 4ème espace intercostal (EIC).

  V3 : au milieu de V2 et V4.

  V4 : 5ème EIC sur la ligne médio-claviculaire.

  V5 : 5ème EIC les lignes axillaires antérieures.

  V6 : 5ème EIC les lignes axillaires et médianes.

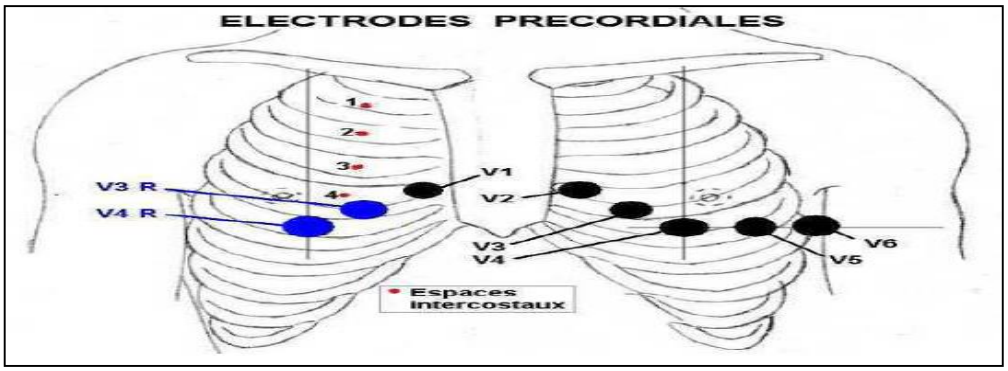


Figure1.8. Dérivations précordiales [1].

1.5.2 Les différentes déflexions de l'ECG :

Le signal électrocardiographique normal est formé de plusieurs ondes qui correspondent à l'activation électrique des diverses parties du cœur, désignées sur l'ECG de surface standard par les lettres de l'alphabet P, Q, R, S, T et U. À chaque cycle cardiaque, on distingue successivement :

- l'onde P, correspondant à la dépolarisation des oreillettes ; elle est de petite amplitude.
- le complexe QRS, correspondant à la dépolarisation des ventricules ; elle est de grande amplitude (signal de quelques millivolts), car la masse des ventricules est très supérieure à celle des oreillettes.
- l'onde T, correspondant à la repolarisation des ventricules.
- l'onde U, inconstante, qui traduit la repolarisation du réseau de Purkinje.

1.5.3 Les différents segments et intervalles dans un ECG :

En plus des différentes ondes qui sont les paramètres de base pour une bonne caractérisation du signal ECG, il existe un certain nombre d'intervalles et de segments qui contiennent des informations très utiles sur la vitesse de conduction de l'impulsion électrique dans les différentes parties du cœur (Figure 1.9).

Les intervalles et les segments les plus importants sont :

-Intervalle RR :

L'intervalle RR correspond au délai entre deux dépolarisations des ventricules. C'est cet intervalle qui permet de calculer la fréquence cardiaque.

-Intervalle PR :

C'est un segment isoélectrique mesuré du début de l'onde P jusqu'au début du complexe QRS. C'est le temps que met l'onde pour aller du nœud sinusal, dépolariser les oreillettes, parcourir le nœud auriculo-ventriculaire et le faisceau de HIS, jusqu'au début des deux branches de ce dernier (temps de conduction auriculo-ventriculaire).

-Le segment ST :

Il correspond au temps séparant le début de la dépolarisation ventriculaire représentée par le complexe QRS et le début de l'onde T. Le segment ST normal est isoélectrique du point J au début de l'onde T.

-Point J: Il correspond au point de transition entre le complexe QRS et le segment ST. Il est normalement isoélectrique.

-Intervalle PQ :

Il représente l'intervalle du temps entre le début de la dépolarisation des oreillettes et le début de la dépolarisation ventriculaire. Il représente le temps nécessaire à l'impulsion électrique pour se propager du nœud sinusal jusqu'aux ventricules et il est mesuré entre le début de l'onde P et le début du complexe QRS.

-L'intervalle QT :

Il représente la durée entre le début du complexe QRS et la fin de l'onde T. Cet intervalle reflète la durée de la dépolarisation et repolarisation ventriculaire. En effet, sa dynamique peut être associée à des risques d'arythmie ventriculaire et de mort cardiaque soudaine.

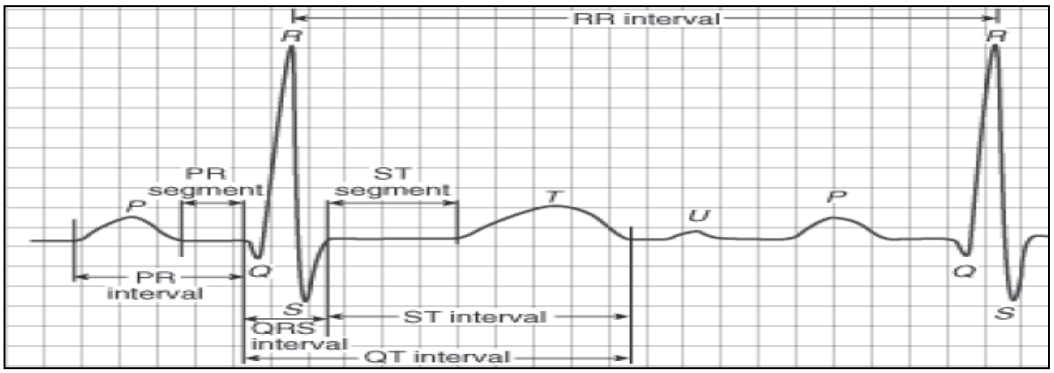


Figure1.9. ECG Normal [06]**.**

1.6 Les bruits présents dans l'ECG:

Il y a des bruits de hautes fréquences, provoqués par l'activité musculaire extracardiaque et les interférences dues aux appareils électriques, et des bruits de basses

fréquences provoqués par les mouvements du corps liés à la respiration, les changements physicochimiques induits par l'électrode posée sur la peau et les micro-variations du flux sanguin.

Pour réduire ces bruits**,** il faut demander au sujet de respirer calmement et d'éviter les mouvements ou de toucher du métal. Il faut bien préparer la peau avant de placer une électrode. Il faut aussi éviter les chevauchements des fils d'enregistrement (boucle).

La figure (1.10) représente un exemple de bruit dus au mauvais contact électrode-peau.

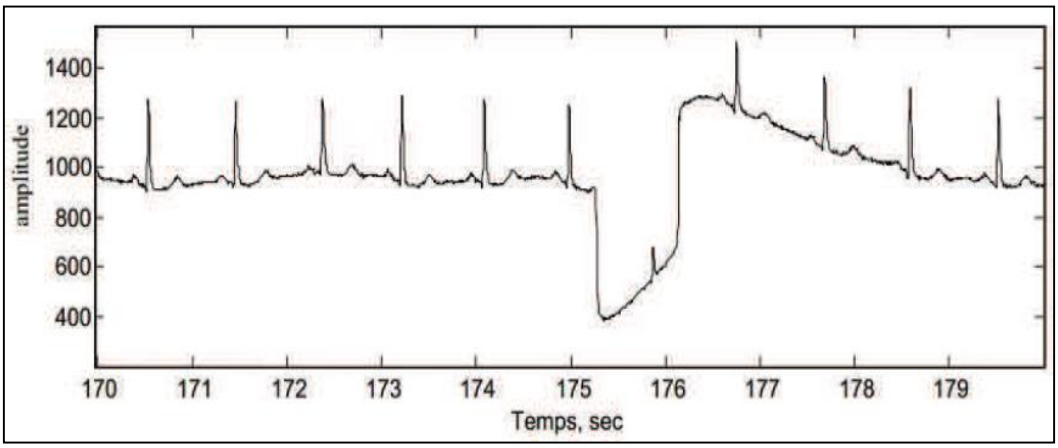


***Figure1.10*.** Bruits dus au mauvais contact électrode-peau [06]**.**

1.7 Etude fréquentielle d'un électrocardiogramme:

Pour supprimer l'interférence du courant électrique ainsi que les bruits à très basse fréquence avec la fréquence de secteur, on utilise un filtre classique passe-haut « High-pass» qui élimine en mode réel les bruits en dessous du seuil de 0,05 Hz. Un filtre passe-haut calibré à 0,5 Hz, en temps réel enregistre/engendre des distorsions du segment ST.

L'information utile de signal ECG est comprise entre 0Hz et 100Hz ; Pour supprimer les bruits à haute fréquence, on utilise un filtre classique passe-bas « low-pass » qui supprime en mode réel les bruits au-dessus de 150 Hz. Un filtre passe-bas calibré à 75 Hz ou moins réduit légèrement l'amplitude des QRS et la capacité à détecter de petites déflexions (micro onde Q, complexes QRS fragmentés). Il lisse d'avantage le tracé et fait disparaître de nombreux artefacts rapides.

La bande passante recommandée en routine se situe entre 0,05 Hz et 150 Hz chez l'adulte (250 Hz chez l'enfant). Mais la majorité des appareils du marché proposent des filtres préréglés entre 0,5Hz et (40-50) Hz, car le tracé est plus stable et moins parasité [07][08][09].

La figure (1.11) représente le spectre d'amplitude de la tension cardiaque (U_{card}) en microvolt.

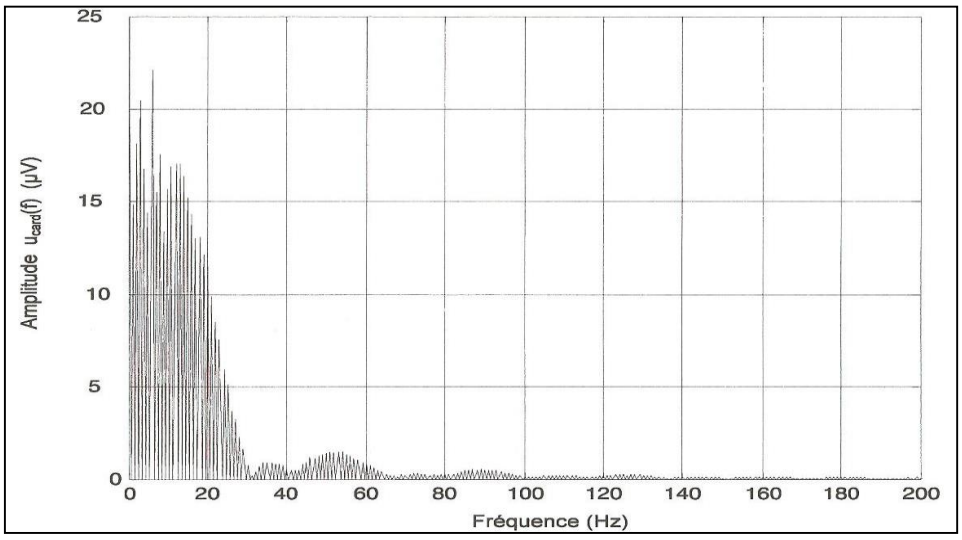


Figure 1.11. Spectre d'amplitude de la tension cardiaque [10]**.**

Dans ce chapitre, on a présenté des généralités sur le système cardiovasculaire avec une description de l'électrocardiogramme, ses caractéristiques, les bruits qui perturbent le signal ECG ainsi que son étude fréquentielle. Le prochain chapitre sera consacré à l'analyse des systèmes dynamiques chaotiques et de l'oscillateur chaotique de Colpitts.

Chapitre 2

Généralités sur les systèmes chaotiques

Le terme « chaos » désigne le désordre : il définit un état particulier d'un système dynamique dont le comportement ne se répète jamais, qui est imprédictible à long terme et sensible aux conditions initiales .Henri Poincaré est le mathématicien qui a introduit pour la première fois le concept de la dynamique chaotique lorsqu'il a étudié le phénomène des trois corps en interaction (une étoile et deux planètes); il a remarqué que des orbites très compliquées (chaotiques) pourraient se produire à travers un ensemble des conditions initiales[11].

Notre travail se focalise sur l'usage du chaos dans la transmission sécurisée de l'information. Dans cette perspective, ce chapitre est destiné à l'étude des caractéristiques et des propriétés des systèmes dynamiques chaotiques à savoir la stabilité des points fixes, l'attracteur étrange, la section de Poincaré ainsi que les exposants de Lyapunov et la bifurcation, nous allons présenté le système de Lorenz comme exemple,en terminant le chapitre par l'étude de l'oscillateur de Colpitts qui sera utilisé comme un générateur de signaux chaotiques pour le cryptage du signal ECG.

2.1 Définitions :

Un système dynamique non linéaire est défini par l'équation différentielle suivante :

$$\frac{dx}{dt} = \dot{x} = f(t, x, \mu) \tag{2.1}$$

Où : $x \in \mathrm{U} \subseteq \mathbb{R}^{\mathrm{n}}$ est un vecteur de dimension n représentant l'état du système et $\mu \in V \subseteq \mathbb{R}^{\mathrm{P}}$ représente le vecteur paramètre du système. $\mathbb{R}^{\mathrm{P}}$ est appelé l'espace des paramètres et $\mathbb{R}^{\mathrm{n}}$ est appelé l'espace de phases.

On dit qu'un système dynamique est autonome s'il ne dépend pas explicitement du temps, on peut le représenter par les équations suivantes :

$$\begin{cases} \dot{x} = f(x, \mu) \\ \dot{y} = f(y, \mu) \end{cases} \tag{2.2}$$

Par un changement de variable, on peut toujours transformer un système autonome en un système non autonome.

2.1.1 Flot et espaces de phase:

Soit le système autonome suivant :

$$\dot{x} = \frac{dx}{dt} = f(x) \ , x \in \mathbb{R}^{\mathrm{n}} , f \in C^{\mathrm{r}}(\mathrm{U}) , \mathrm{U} \subseteq \mathbb{R}^{\mathrm{n}} . \tag{2.3}$$

Définition : soit (x_0, t) ,$x_0 \in D$, une solution de (2.3) avec comme condition initiale $x(0) = x_0$.

On appelle flot de (2.3) ou du champ de vecteurs f , l'application $\varphi_t : D \to \mathbb{R}^n$ définit par :

$$\varphi_t(t) = x(x_0, t) \tag{2.4}$$

Qui possède les propriétés suivantes :

- $\varphi_0(x_0) = x_0$
- $\varphi_{t+s}(x_0) = \varphi_t(\varphi_s(x_0))$

On appelle l'espace $x_1, x_2, x_3 \dots \dots \dots x_n$ dans un système, un espace des phases (espace d'états), et le chemin parcouru par le système est appelé trajectoire, et $x_1, x_2, x_3 \dots \dots \dots x_n$ sont les états du système.

2.1.2 Point fixe :

On appelle point d'équilibre (point critique ou point stationnaire) de (2.1), le point $\bar{x}$ de l'espace des phases obtenu en annulant le second membre de (2.1) :

$$f(\bar{x}) = 0 \tag{2.5}$$

Par un changement de variables $\varepsilon = x - \bar{x}$, on peut ramener le point $\bar{x}$ à l'origine.

Grace aux points fixes, on peut caractériser les trajectoires voisines.

2.1.3 Stabilité de point fixe :

L'étude de la stabilité des points d'équilibre permet l'analyse de comportement des solutions sans résoudre les équations différentielles. Particulièrement, elle sert à l'étude locale des solutions autour des points fixes.

a) Stabilité au sens de Lyapounov :

Soit le système autonome suivant :

$$\dot{x} = f(x) \;\; ; \;\; f : D \;\to\; \mathbb{R}^n \tag{2.6}$$

On suppose que $\bar{x}$ est un point d'équilibre : $f(\bar{x}) = 0$

- On dit que $\bar{x}$ est stable si et seulement si :

$$\forall \varepsilon > 0, \exists \alpha > 0 \; telque : \|x(0) - \bar{x}\| < \alpha \Rightarrow \|x(t) - \bar{x}\| < \varepsilon, \forall\, t \geq 0 \tag{2.7}$$

C'est-à-dire le point fixe est stable si toutes les solutions issues des points voisins du point d'équilibre restent proches de celui-ci.

- On dit que le point fixe est instable s'il n'est pas stable au sens de Lyapounov.
- On dit que le point fixe est asymptotiquement stable s'il est stable et on peut choisir $\delta > 0$ telque :

$$\|x(0) - \bar{x}\| < \delta \Rightarrow \lim_{t\to\infty} x(t) = \bar{x} \tag{2.8}$$

La stabilité asymptotique permet de déterminer un voisinage de point fixe tel que toute trajectoire issue d'un point x (0) appartenant à un voisinage de $\bar{x}$ tende vers $\bar{x}$ quand t tend vers l'infini.

L'inconvénient est que les définitions précédentes concernent que les orbites proches de point fixe alors qu'on veut étudier le comportement de tout le système. Pour cela, Lyapounov à donné une méthode permettant de résoudre ce problème.

b) Stabilité par méthode indirecte de Lyapounov :

Supposons que, par un changement de coordonnées, le point fixe est à l'origine : $f(0) = 0$, le développement en série de Taylor en $x = 0$ s'écrit :

$$f(x) = Df(0)x - \frac{1}{2!}\mathrm{D}^2 f(0)(x,x) + \frac{1}{3!}\mathrm{D}^3 f(0)(x,x,x) \tag{2.9}$$

La matrice :

$$Df(x) = \left(\frac{df_i(x)}{dx_j}\right) \tag{2.10}$$

s'appelle matrice Jacobienne de $f(x)$, son déterminant est le Jacobien. Pour x petit le comportement de système est celui de système linéairisé :

$$\dot{x} = Df(0)x \tag{2.11}$$

Où :

$$Df(0) = \begin{bmatrix} \frac{df_1}{dx_1} & \cdots & \frac{df_1}{dx_n} \\ \vdots & \ddots & \vdots \\ \frac{df_n}{dx_1} & \cdots & \frac{df_n}{dx_n} \end{bmatrix}_{x=0} \tag{2.12}$$

Dans le cas où la matrice possède n valeur propre λ_i , i=1…..n ,la solution de (2.11) est :

$$x = \sum_{i=1}^{n} c_i\, a^{(i)} \exp(\lambda_i t) \tag{2.13}$$

Ou $a^{(i)}$ est le vecteur propre correspondant à la valeur propre λ_i et les c_i, $i = 1 \ldots\ldots n$, sont déterminées par les conditions initiales [12] . On en déduit que :

- Si toutes les valeurs propres λ_i ont leur partie réelle négative, le point fixe est asymptotiquement stable.
- Si une des valeurs propres a sa partie réelle positive, le point fixe est instable.
- Si une ou plusieurs valeurs propres sont des imaginaires pures, les autres valeurs propres ayant leur partie réelle négative, le point fixe est un centre ou un point elliptique (stable mais pas asymptotiquement stable).
- Si $Df(0)$ n'a pas de valeur propre nulle ou purement imaginaire, le point fixe est un point hyperbolique, dans le cas contraire, c'est un point non-hyperbolique.
- S'il existe i et j tel que $\mathrm{C}\lambda_i < 0$ et $\mathrm{C}\lambda_i > 0$, le point fixe est un point selle.
- Si toutes les valeurs de $Df(0)$ sont réelles et de même signe, le point fixe est nœud. Un nœud stable est un puit, un nœud instable est une source.

2.2 Les caractéristiques d'un système dynamique chaotique:

Un système dynamique non linéaire est dit chaotique lorsqu'il dépend de plusieurs paramètres ainsi que son évolution dans le temps est très sensible aux conditions initiales, il peut même sembler aléatoire alors qu'il est parfaitement déterministe, mathématiquement, on dit qu'une fonction f est sensible aux conditions initiales si et seulement si [13] :

$$\exists \delta > 0\,, \forall x \in D\,, \forall \varepsilon > 0\,, \exists (y,p) \in D : \quad \begin{cases} \|x-y\| < \varepsilon \\ \|f^p(x) - f^p(y)\| > \delta \end{cases} \tag{2.14}$$

Les systèmes chaotiques sont caractérisés par les propriétés suivantes :

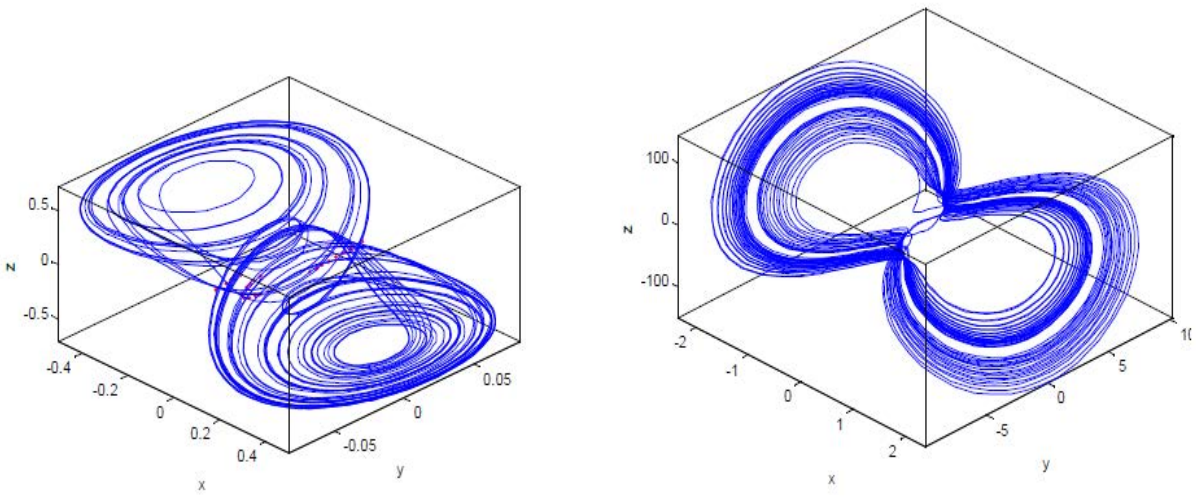
2.2.1 Attracteur étrange:

On appelle attracteur étrange ou chaotique tout objet géométrique vers lequel tendent toutes les trajectoires générées par un système chaotique quelles que soient ses conditions initiales, qui est extrêmement complexe à cause des repliements, des étirements et des contractions s'opérant dans une région bornée de l'espace d'état.

Un attracteur possède les propriétés suivantes [14]:

- Tout point de l'espace d'état qui appartient à un attracteur demeure à l'intérieur de cet attracteur pour tout t tendant vers l'infini.
- Un attracteur est indécomposable ; ainsi la réunion de plusieurs attracteurs n'est pas un attracteur.

La figure (2.1) représente deux exemples d'attracteurs étranges :

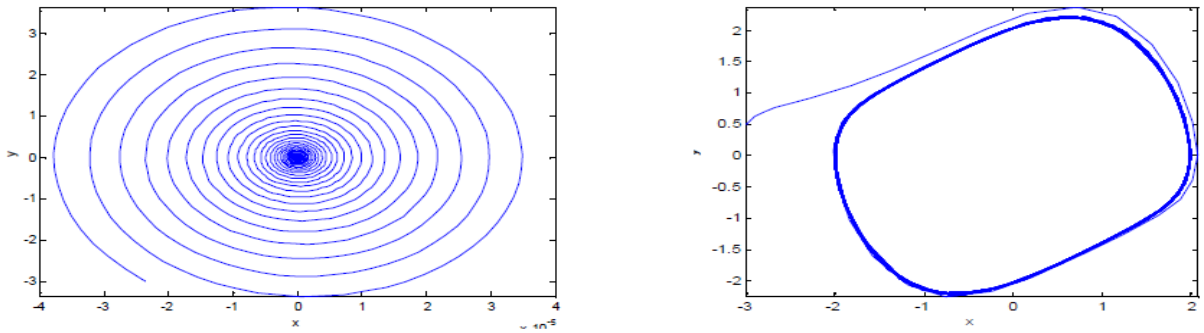


Oscillateur de Chua Oscillateur de Moore Spiegel

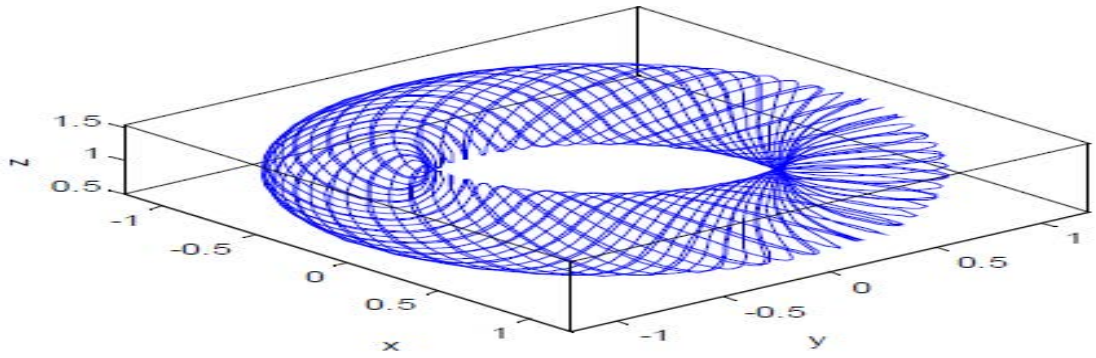
Figure 2.1. Attracteurs étranges.

Il existe un autre type d'attracteurs qui caractérise les systèmes non chaotiques qu'on appelle les attracteurs réguliers et peuvent être de trois sortes :

- **Le point fixe :** est le cas le plus simple, dans lequel le système évolue vers un état de repos, ce point s'appelle le puit (Figure (2.1.a)).
- **Le cycle limite périodique :** quand la trajectoire se referme sur elle-même, le système présentant des oscillations permanentes, alors l'évolution est cyclique (Figure (2.1.b)).
- **L e cycle limite pseudopériodique :** est un cas particulier du type précédent, le système possède deux périodes alors la trajectoire ne se referme pas sur elle-même mais s'enroule sur une variété de dimension 2, elle forme un tore (Figure (2.1.c)).



(a) Point fixe (b) Cycle limite



(c) Tore

Figure 2.2. Différents types d'attracteurs réguliers.

2.2.2 Section de Poincaré :

Henri Poincaré a apporté une contribution très utile dans la théorie des systèmes dynamiques chaotiques : c'est la section de Poincaré. Faire une section de Poincaré veut dire couper la trajectoire chaotique dans un espace d'au moins trois dimensions par un hyperplan d'une dimension inferieure, afin d'étudier les intersections, chaque intersection correspond à une orbite et une seule. Ainsi, on convertit le système continu en un système discret dont le nombre d'interactions remplace le temps, sachant qu'en mathématique, ses propriétés restent toujours conservées, la section de Poincaré est plus détaillée dans [15][16].

Concidérons le système dynamique autonome suivant :

$$\frac{dx}{dt} = f(x), x \in \mathbb{R}^n \tag{2.15}$$

On appelle section de Poincaré une hyper surface $\sum_p$ de dimension n -1 ,tel que l'ensemble des points $p_0, p_1, p_2, \ldots$ correspond aux intersections successives de la trajectoire $\varphi_t(x_0)$ avec l'hyper surface $\sum_p$ comme illustre la figure suivante :

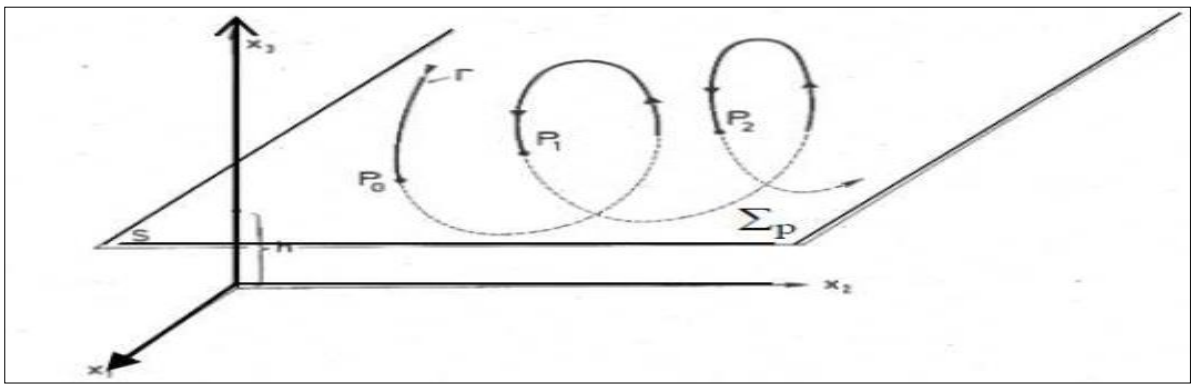


Figure 2.3. Section de Poincaré et application du premier retour.

Le système initial de dimension n est transformé en un système de dimension n-1 qui est représenté par :

$$p_{k+1} = T(p_k) \quad , \; k = 0,1,2 \ldots \ldots \ldots \tag{2.16}$$

Où : T est l'application du premier retour qui à un point p_i de $\sum_p$ fait correspondre le prochain point p_{i+1} d'intersection de la trajectoire $\varphi_t(x_0)$ avec l'hyper surface $\sum_p$.

K = 1, 2…… caractérise le système dynamique dont les propriétés sont données dans le tableau suivant :

Application de Poincaré	Attracteur
1 point	Cycle limite
P points	Cycle limites avec P maxima par période
Courbe fermée	Attracteur quasi-périodique
Courbe ouverte	Attracteur étrange

Tableau 2.1. Application de Poincaré [13].

Par une analyse de l'application de premier retour T, on peut étudier la stabilité d'une orbite périodique [13].

2.2.3 Les exposants de Lyapounov :

Le mathématicien Alexander Lyapounov a étudié le phénomène de la sensibilité aux conditions initiales des systèmes chaotiques et a développé un degré permettant de mesurer la vitesse à laquelle ces petites variations peuvent s'amplifier ; cette quantité est appelée « Exposant de Lyapounov ». Autrement dit, l'exposant de Lyapounov est le taux de divergence entre l'évolution des trajectoires issues de conditions initiales proches au sein de l'attracteur étrange [17].

Lyapounov a démontré que le nombre des exposants est égal à la dimension de l'espace des phases, caractérisant ainsi le comportement du système non linéaire (chaotique ou non).

a) Calcul des exposants de Lyapounov :

Soit le système dynamique autonome suivant :

$$\begin{cases} \dot{x} = f(x) \ ; f: \mathbb{R}^n \ \rightarrow \ \mathbb{R}^n \\ x(0) = x_0 \end{cases} \tag{2.17}$$

Où $\varphi(x_0, t)$ est une trajectoire solution du système de condition initiale x_0 , $x_p = \varphi(x_0, t_p)$ est un point de cette trajectoire à $t = t_p$.

Le calcul des exposants de Lyapounov consiste d'abord à linéariser le vecteur de champs (une fonction qui associe un vecteur à chaque point d'un espace euclidien) au voisinage de la trajectoire considérée [18].

Considérons la trajectoire $\varphi(x_0, t)$ et un point de cette trajectoire x_p .

Soit une petite perturbation $\delta x_p(t)$ appliquée au voisinage de x_p . En utilisant le développement en série de Taylor, le système linéarisé s'écrit :

$$\frac{d\delta x_p}{dt} = J_f(x_p)\delta x_p \tag{2.18}$$

Où $J_f(x_p)$ est la matrice Jacobienne du système au point x_p.

On intègre chacune des composantes $x_k(t)$ avec k = 1, 2,....., n de la trajectoire $\varphi(x_0, t)$ à partir de l'équation (2.14). Chacune de ces composantes $x_k(t)$ intégrées est introduite dans (2.17). Au final, on intègre le système (2.14) lui-même. On obtient alors une matrice $\phi_t(x_p)$ appelée matrice de la solution fondamentale, elle est de dimension $n \times n$.

Toute perturbation $\delta x_p(t)$ à $t = t_p$ au voisinage d'un point x_p de la trajectoire pourra s'écrire sous la forme :

$$\delta x_p(t) = \phi_t(x_p(t_p)) \tag{2.19}$$

Considérons $\eta_i(t)$ de cette matrice, i=1, 2……n. L'exposant de Lyapounov du $i^{ième}$ ordre est lié aux valeurs propres et s'écrit :

$$\lambda_i = \lim_{t \to +\infty} \frac{1}{t} Ln\,|\eta_i(t)| \tag{2.20}$$

Si $\lambda_i > 0$ alors la distance entre les trajectoires augmente exponentiellement c'est-à-dire qu'un régime chaotique atteint. Sinon, si $\lambda_i < 0$ alors la distance converge vers 0 lorsque t tend vers l'infini c'est-à-dire le régime n'est pas chaotique [13].

b) Comportement de système en fonction des exposants de Lyapounov :

On peut définir le comportement de système (type d'attracteur) en étudiant les exposants de Lyapounov [18]:

- Si $\lambda_n \leq \cdots \ldots \ldots \leq \lambda_2 \leq \lambda_1 \leq 0$, il existe un point fixe.
- Si $\lambda_1 = 0$ et $\lambda_n \leq \cdots \ldots \ldots \leq \lambda_2 \leq 0$, l'attracteur est une orbite fermé.
- Si $\lambda_1 = \lambda_2 = 0$ et $\lambda_n \leq \cdots \ldots \ldots \leq \lambda_3 \leq 0$, l'attracteur est quasi-périodique (deux périodes).
- Si $\lambda_1 > 0$ et $\sum_{i=1}^{n} \lambda_i < 0$, l'attracteur est chaotique.
- Si $\lambda_1 > \cdots \ldots \ldots > \lambda_k > 0$ et $\sum_{i=1}^{n} \lambda_i < 0$, l'attracteur est hyper-chaotique.

2.2.4 Bifurcation :

La bifurcation est l'étude mathématique des changements qualitatifs de la structure d'un système dynamique ; elle survient lorsqu'une variation qualitative d'un paramètre engendre un changement qualitatif des propriétés d'un système telles que la stabilité, le nombre de points fixes ou la nature des régimes permanents. Les valeurs des paramètres provoquant un changement sont appelées «valeurs de bifurcation ». On peut citer deux types de bifurcation :

a) Bifurcation de co-dimension k [12]:

Soit le système dynamique dépendant d'un paramètre μ donné par l'équation suivante :

$$\dot{x} = f(t, x, \mu) \tag{2.21}$$

Si l'ensemble des valeurs de la bifurcation est défini par k conditions :

$$C_1(\mu) = C_2(\mu) = \cdots \ldots \ldots C_k(\mu) = 0 \qquad avec \quad 1 \leq k \leq p \tag{2.22}$$

Alors la bifurcation est dite de co-dimension k qui est divisée en quatre types représentés sous les diagrammes de bifurcation suivants :

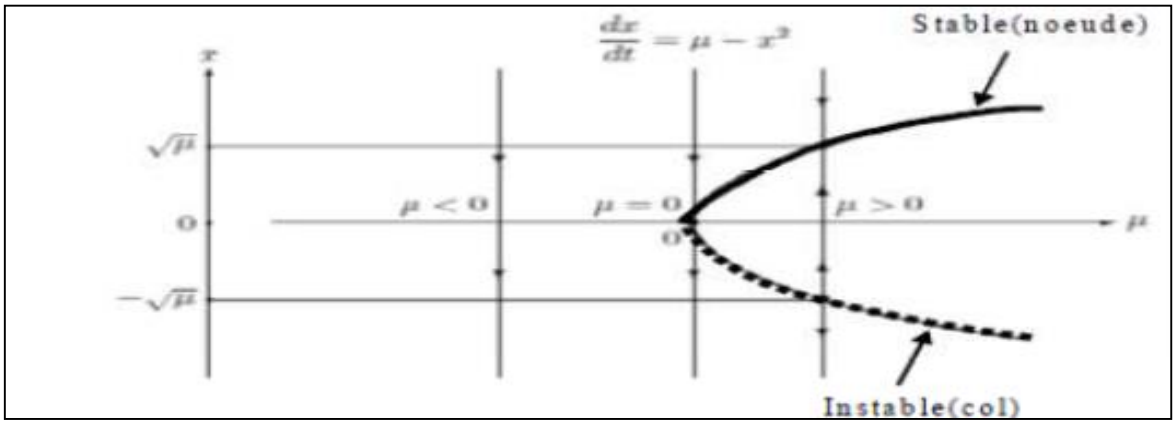


Figure 2.4. Diagramme de bifurcation nœud-col [13].

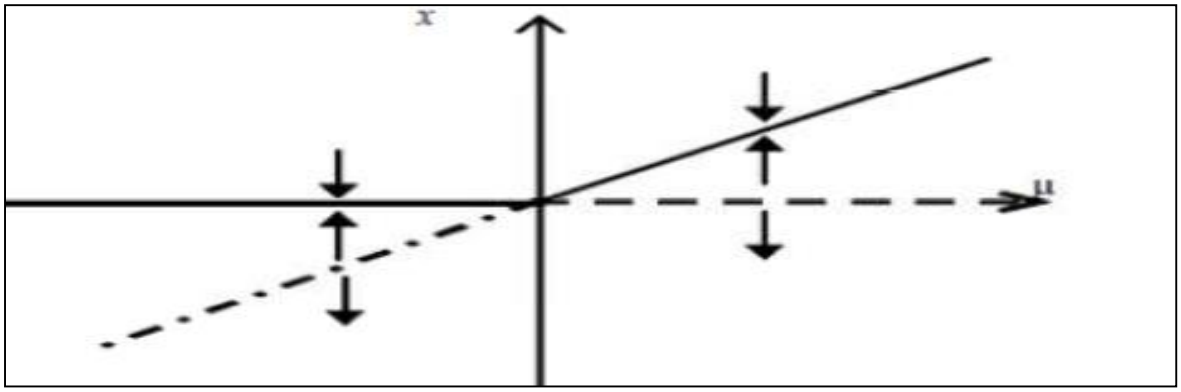
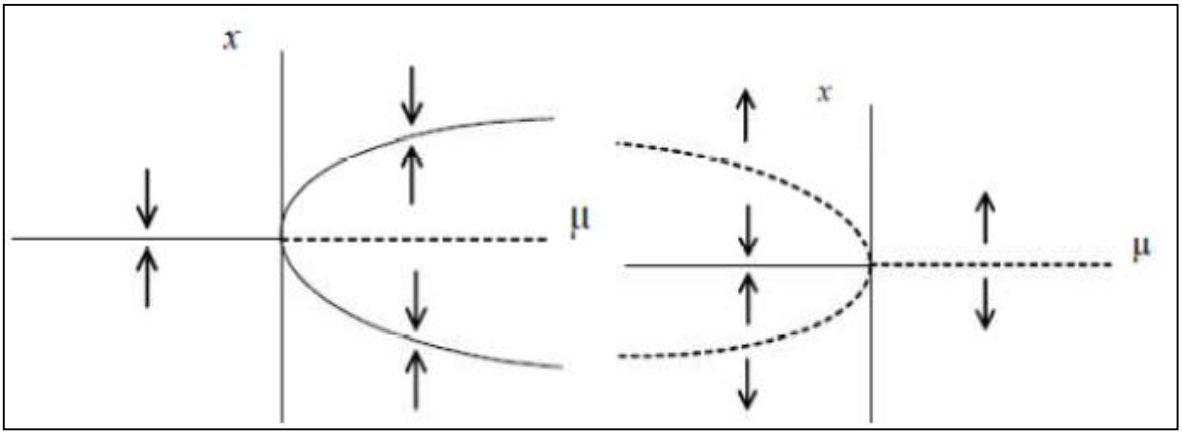


Figure 2.5. Diagramme de bifurcation transcritique [13].



(a) (b)

Figure 2.6. Diagramme de bifurcation fourche (a) sur-critique (b) sous-critique [13].

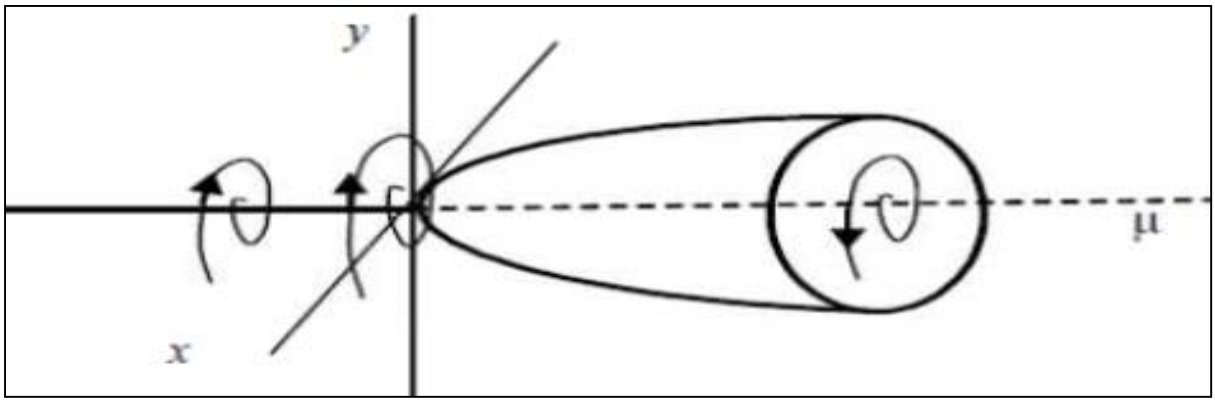


Figure 2.7. Diagramme de bifurcation de Hopf [13].

b) Bifurcation doublement de période ou Flip :

Soit le système dynamique (2.21) qui a un point d'équilibre stable pour $\mu < \mu_0$. Lorsque μ augmente au-delà de μ_0 ,le point fixe devient instable et une bifurcation se produit

et donne naissance à un cycle stable d'ordre 2. Si μ continue à augmenter, le cycle d'ordre 2 se déstabilise et une bifurcation se produit dans chacun des deux points résultant un cycle d'ordre 4. Si μ toujours augmente, des bifurcations apparaissent avec doublement de période jusqu'à arriver à une suite infinie de bifurcations qui caractérise le chaos.

2.3 Exemple de système chaotique : Système de Lorenz :

Parmi les systèmes dynamiques au comportement chaotique pour certaines valeurs de ses paramètres, nous représentons le système de Lorenz, donné par les équations différentielles suivantes :

$$\begin{cases} \dot{x} = \delta(y - x) \\ \dot{y} = -rx - y - xz \\ \dot{z} = -bz + xy \end{cases} \tag{2.23}$$

Avec: $\delta = 10$, $r = \frac{8}{3}$, $b = 28$ on a un système dynamique chaotique. Pour la simulation nous avons choisi les conditions initiales suivantes : $x_0 = 8$, $y_0 = 3$, $z_0 = 33$, on a obtenu trois points fixes. La figure (2.8) représente l'attracteur étrange du système de Lorenz :

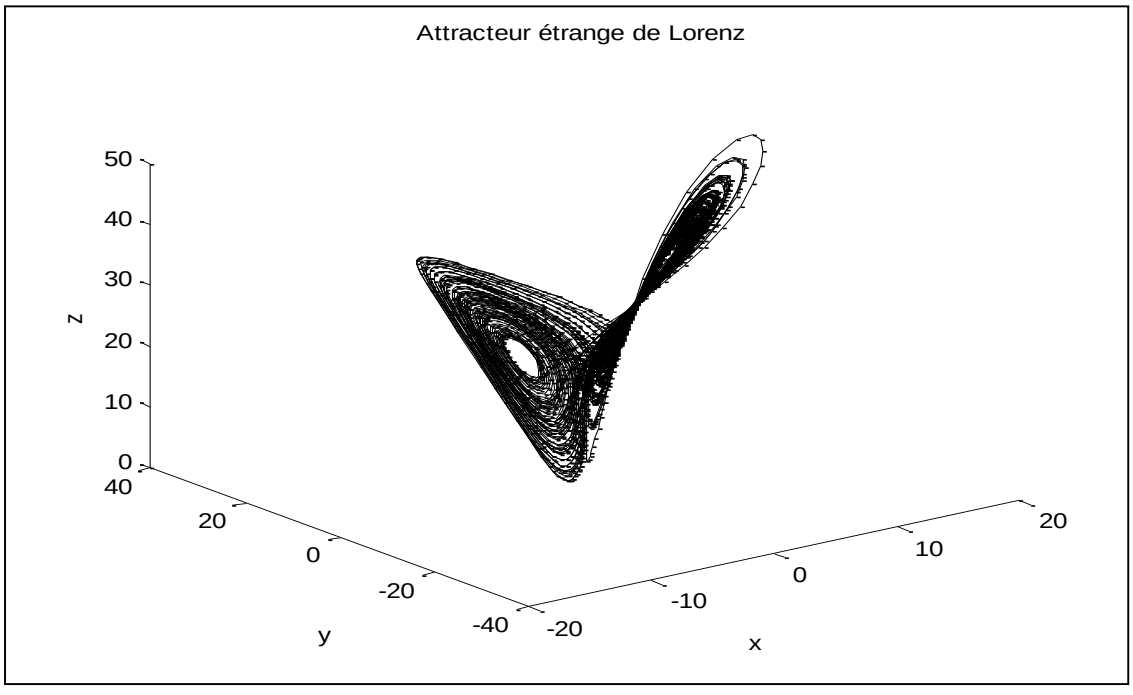


Figure 2.8. Attracteur étrange de système de Lorenz.

Ainsi que les coordonnées x, y et z en fonction du temps sont données par la simulation du système de Lorenz sous simulink et représentées sur la figure (2.9):

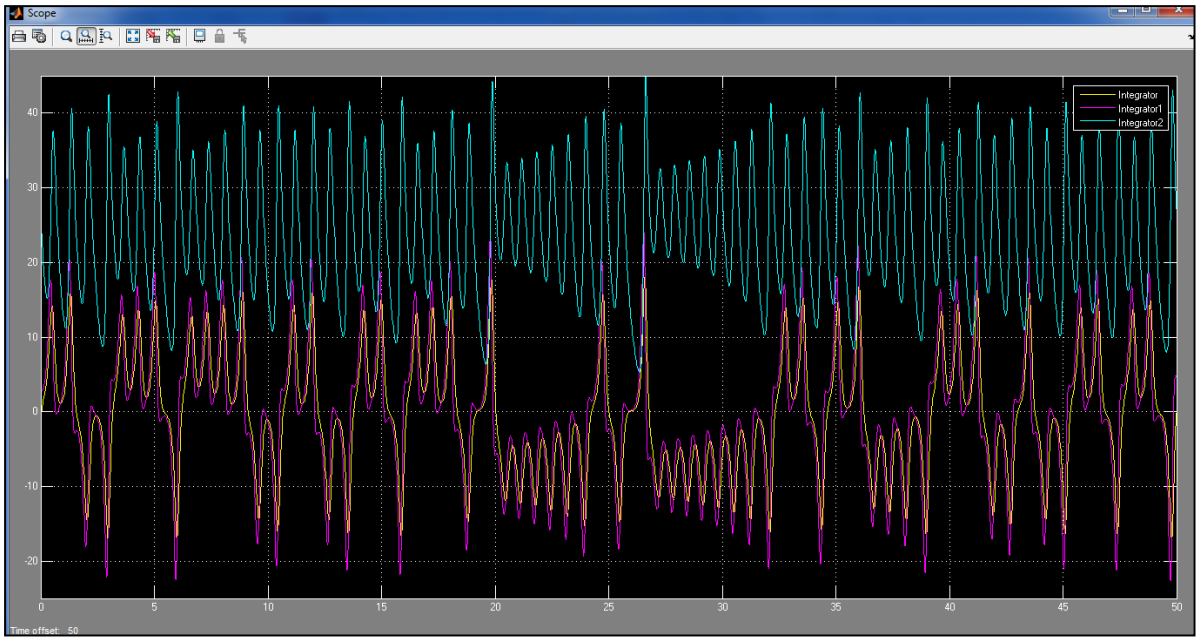


Figure 2.9. Solutions de système de Lorenz.

On a obtenu des signaux $x(t), y(t), z(t)$ chaotiques, se ressemblent aux signaux bruités mais ils sont déterministes.

Les exposants de Lyapounov sont représentés sur la figure ci-dessous ; il existe un exposant positif et la somme des exposants est négative. Cela signifie que le système est chaotique.

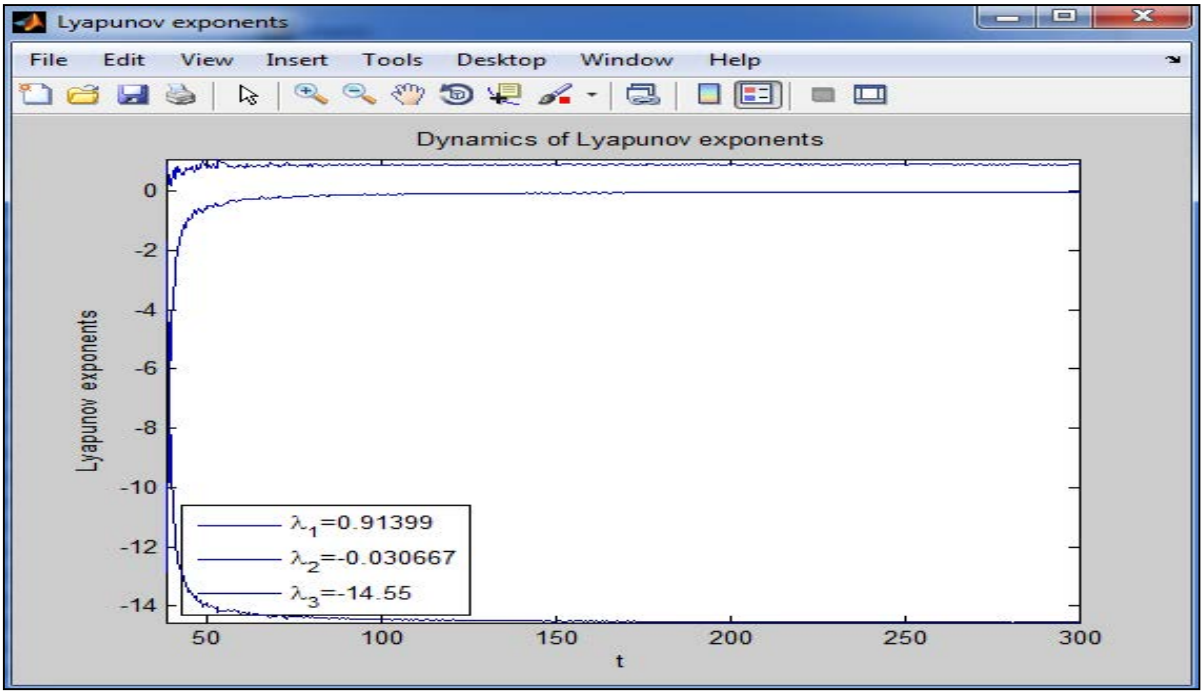


Figure 2.10. Exposants de Lyapounov de système de Lorenz.

On a étudié le comportement de système de Lorenz en faisant varier la valeur du paramètre r ; on a obtenu le diagramme de bifurcation suivant :

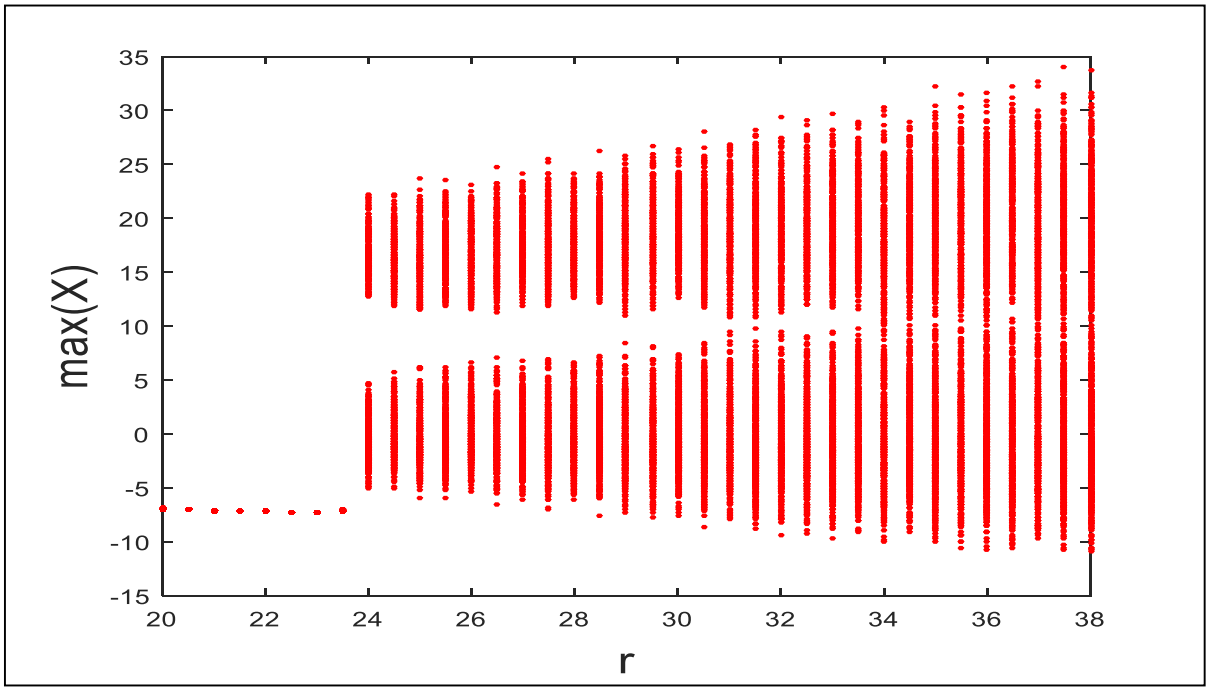


Figure 2.11. Diagramme de bifurcation du système de Lorenz.

Si $r < 24$, le système possède un nombre petit de maximums, cela signifie qu'il a un comportement périodique (non chaotique). Dés que r dépasse la valeur 24, plusieurs maximums apparaissent, ce phénomène nous permet de déduire que le système est chaotique.

La figure (2.12) représente l'espace des phases $y(t)$ en fonction de $x(t)$ de dimension 2 :

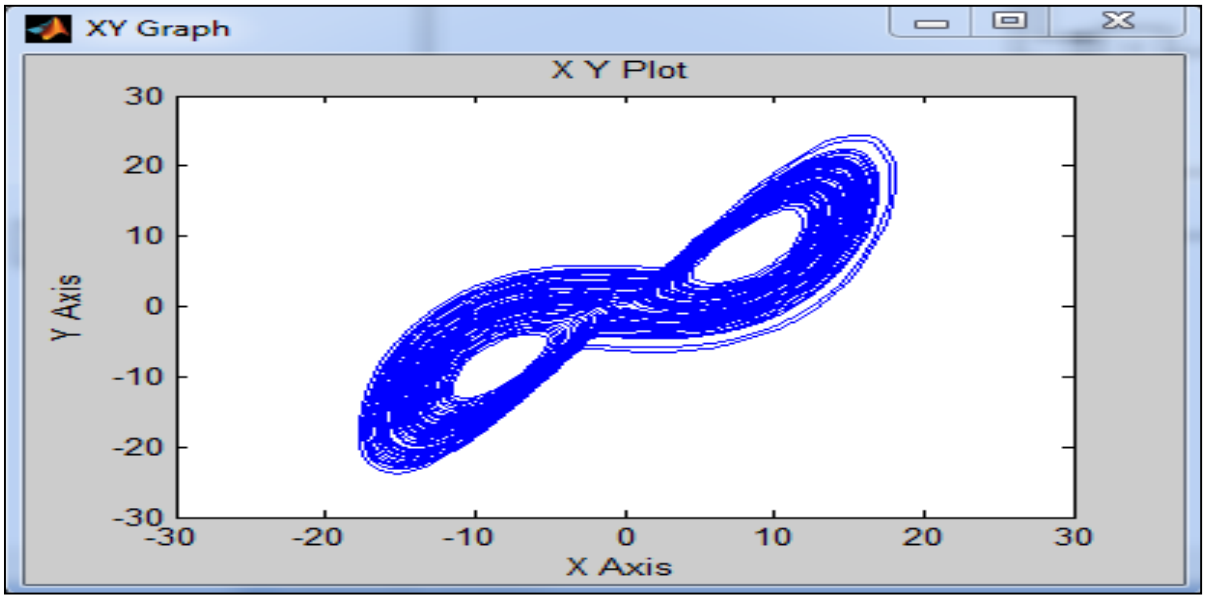


Figure 2.12. Espace des phases $y(x)$.

En coupant cet espace de phase par un plan de l'équation $x = 0$, on a obtenu la section de Poincaré représentée par la figure suivante :

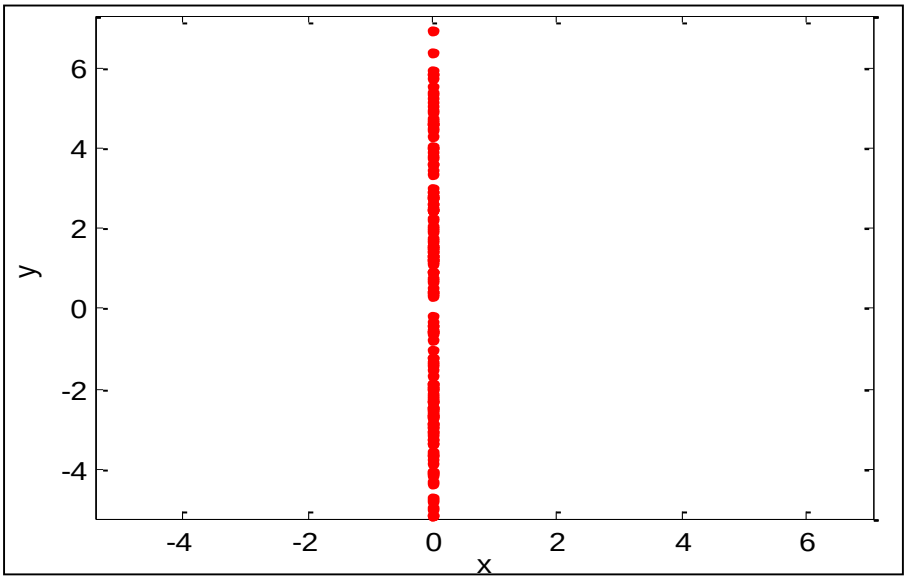


Figure 2.13. Section de Poincaré de système de Lorenz.

On remarque qu'il existe une infinité des points d'intersection (courbe ouverte) ce qui caractérise le système chaotique.

2.4 Oscillateur chaotique de Colpitts:

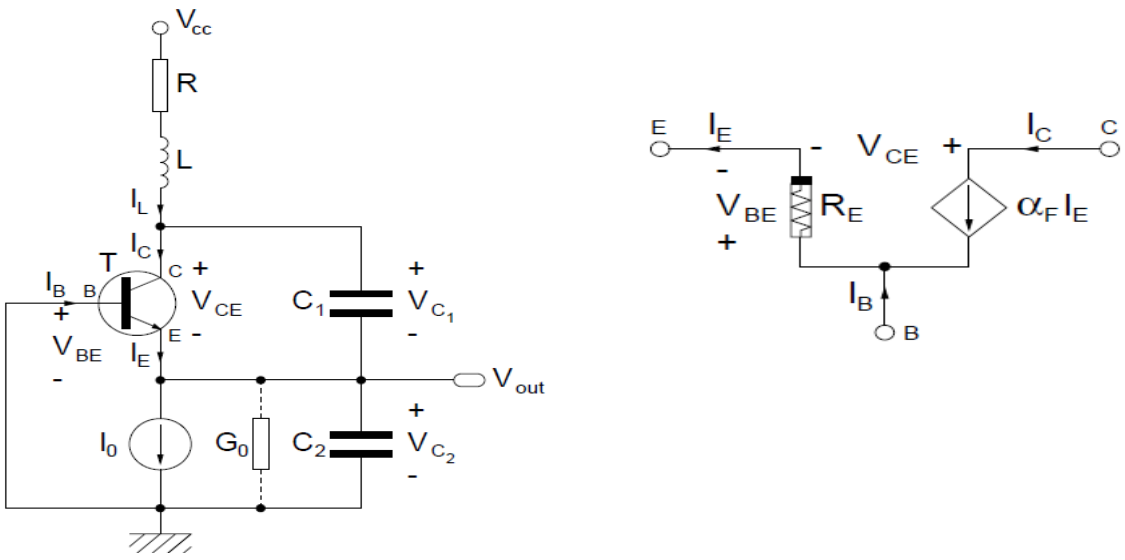
Pour le cryptage du signal ECG, on a choisi l'oscillateur de Colpitts afin de générer un signal chaotique, Ce choix est expliqué par les points suivants [19]:

- L'oscillateur de Colpitts a une large gamme de fréquences (de très basses fréquences jusqu'à très hautes fréquences).
- La simplicité de la structure de l'oscillateur de Colpitts parce qu'il peut être réalisé par un seul transistor, et en modifiant ses conditions de fonctionnement, il peut avoir un comportement chaotique.
- La structure de l'oscillateur de Colpitts possède une caractéristique exponentielle du transistor (non linéaire).
- L'oscillateur de Colpitts est utilisé dans les systèmes de communication pour la transmission et le cryptage des signaux binaires et continus.

2.4.1 Représentation de l'oscillateur de colpitts :

Dans notre travail, on considère l'oscillateur de Colpitts en basses fréquence comme générateur chaotique ; il est représenté par un montage base commune permettant d'obtenir un gain plus élevé en autorisant une bande passante plus large. L'oscillateur comporte deux

éléments, le premier est le transistor (élément actif), le second (l'élément passif) est le résonateur RCL représenté sur la figure suivante :



(a) (b)

Figure 2.14. Oscillateur de Colpitts : (a) schéma électronique de l'oscillateur de Colpitts, (b) schéma équivalent du transistor T.

Le transistor T est modélisé par la résistance non linéaire R_E et une source de courant $\alpha_F I_E$ tel que $\alpha_F = \frac{I_C}{I_E} = \frac{\beta+1}{\beta} \simeq 1$, $\beta = \frac{I_C}{I_B} = 100$

2.4.2 Critère d'oscillation de Barkhausen :

La figure (2.15) montre la représentation élémentaire d'un oscillateur électronique, $A(j\omega)$ est la fonction de transfert de l'amplificateur et $B(j\omega)$ est la fonction de transfert du filtre.

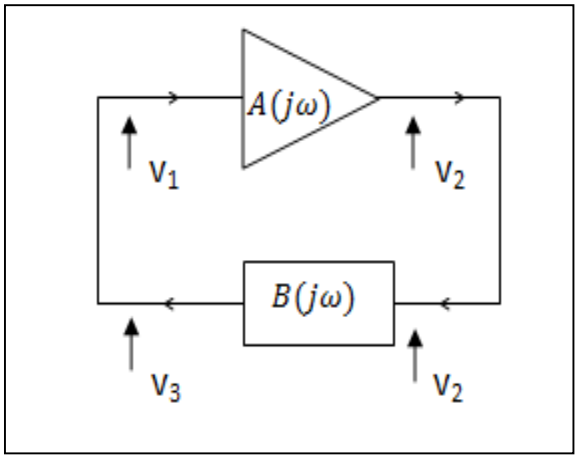


Figure 2.15. Modèle de Barkhausen.

Le critère d'oscillation de Barkhausen nécessite deux conditions :

$$\begin{cases} |A|.|B| = 1 \\ \phi_A + \phi_B = 0 + 2k\pi \qquad k \in \mathbb{Z} \end{cases} \tag{2.24}$$

Or, pratiquement, les oscillations apparaissent à partir de fluctuations qui sont amplifiées, ce qui nécessite la condition d'oscillation : $|A|.|B| > 1$. Mais les oscillations ne peuvent croitre indéfiniment, elles s'arrêtent sur une non-linéarité de l'amplificateur. Ce qui signifie que dans un oscillateur, l'amplificateur possède toujours une caractéristique non linéaire [20].

2.4.3 Détermination de la condition d'oscillations :

La figure (2.16) nous permet d'étudier le fonctionnement de l'oscillateur de Colpitts :

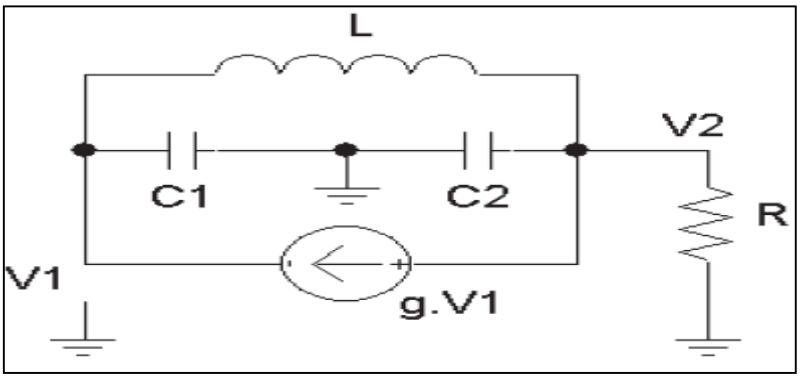


Figure 2.16. Schéma de principe de l'oscillateur de Colpitts.

En utilisant la loi de Kirchoff, les équations aux bornes de l'inductance L s'écrit :

$$\begin{cases} -gV_1 - \frac{V_2}{R} - jC_2V_2\omega + \frac{V_1-V_2}{jL\omega} = 0 \\ \frac{V_2-V_1}{jL\omega} - jC_1\omega V_1 + gV_1 = 0 \end{cases} \tag{2.25}$$

On calcul V_2 dans la deuxième équation et on le remplace dans la première, on aura l'expression suivante :

$$\left[-g + \frac{1}{jL\omega}\right] - \left[jC_1\omega + \frac{1}{jL\omega}\right]\left[\frac{1}{R} + jC_2\omega + \frac{1}{jL\omega}\right] = 0 \tag{2.26}$$

En annulant la partie imaginaire, on obtient :

$$C_1C_2RL\omega^2 - (C_1 + C_2)R\omega = 0 \tag{2.27}$$

Alors, la pulsation d'oscillation de l'oscillateur de Colpitts est :

$$\omega_0 = 2\pi f_0 = \sqrt{\frac{(C_1+C_2)}{C_1C_2L}} \tag{2.28}$$

$$\Rightarrow f_0 = \frac{1}{2\pi}\sqrt{\frac{1}{L\frac{C_1C_2}{(C_1+C_2)}}}$$

On annule la partie réelle de (2.26), on trouve :

$$-Rg + LC_1\omega_0^2 - 1 = 0 \quad \Rightarrow \quad R = \frac{LC_1\omega_0^2 - 1}{g} \tag{2.29}$$

En remplaçant ω_0 par sa valeur, on obtient la condition d'oscillation de montage de Colpitts :

$$R > \frac{C_1}{gC_2} \tag{2.30}$$

Dès que R est supérieur à la valeur obtenue par (2.30), l'oscillation démarre.

2.4.4 Les équations d'état de l'oscillateur de Colpitts :

On considère les variables d'état $V_{C1}, V_{C2}\ et\ I_L$ représentées sur la figure (2.14) pour écrire les équations d'état de l'oscillateur de Colpitts, afin de le décrire sous un modèle mathématique.

Les équations sont alors données par :

$$\begin{cases} \frac{dV_{C1}}{dt} = -\frac{1}{C_1} f(-V_{C2}) + \frac{1}{C_1} I_L \\ \frac{dV_{C2}}{dt} = \frac{1}{C_2} I_L - \frac{1}{C_1} I_0 \\ \frac{dI_L}{dt} = -\frac{1}{L} V_{C1} - \frac{1}{L} V_{C2} - \frac{R}{L} I_L + \frac{V_{CC}}{L} \end{cases} \tag{2.31}$$

Tel que : $f(-V_{C2})$ est la caractéristique courant-tension du transistor bipolaire permettant de calculer le courant d'émetteur donnée par :

$$I_E = f(V_{BE}) = f(-V_{C2}) = I_S\left[\exp(\frac{V_{BE}}{V_T} - 1)\right] \simeq I_S\left[\exp(\frac{V_{BE}}{V_T})\right] \simeq I_S\left[\exp(\frac{-V_{C2}}{V_T})\right] \tag{2.32}$$

Avec : I_S est le courant de saturation inverse de la jonction base-émetteur de transistor.

$V_T \simeq 27mV$ à la température ambiante.

Par un changement de repère, les équations présentées par (2.31) sont transformées en des équations d'états dépendent des paramètres et des variables suivants [21] :

$$x = \frac{V_{C1}}{V^*}\ , z = \frac{V_{C2}}{V^*}\ , y = \frac{\rho I_L}{V^*}\ , t = \frac{1}{\tau}\ , \tau = \sqrt{LC_1}\ , \varepsilon = \frac{C_2}{C_1}\ , \rho = \sqrt{\frac{L}{C_1}}\ , a = \frac{\rho}{r}\ , b = \frac{R}{\rho},$$

$c = \frac{V_0}{V^*}\ , d = \frac{\rho I_0}{V^*}\ , V^* \simeq 0.7\ v$ (pour le Silicium).

On obtient alors la représentation mathématique de l'oscillateur de Colpitts :

$$\begin{cases} \dot{x} = y - a\,F(z) \\ \dot{y} = c - x - by - z \\ \dot{z} = y - d \end{cases} \tag{2.33}$$

Où : $F(z) = \begin{cases} -(z+1) & , z < -1 \\ 0 & , z \geq -1 \end{cases}$ (2.34)

est la fonction non linéaire.

La figure (2.17) montre la simulation sous simulink de l'oscillateur de Colpitts :

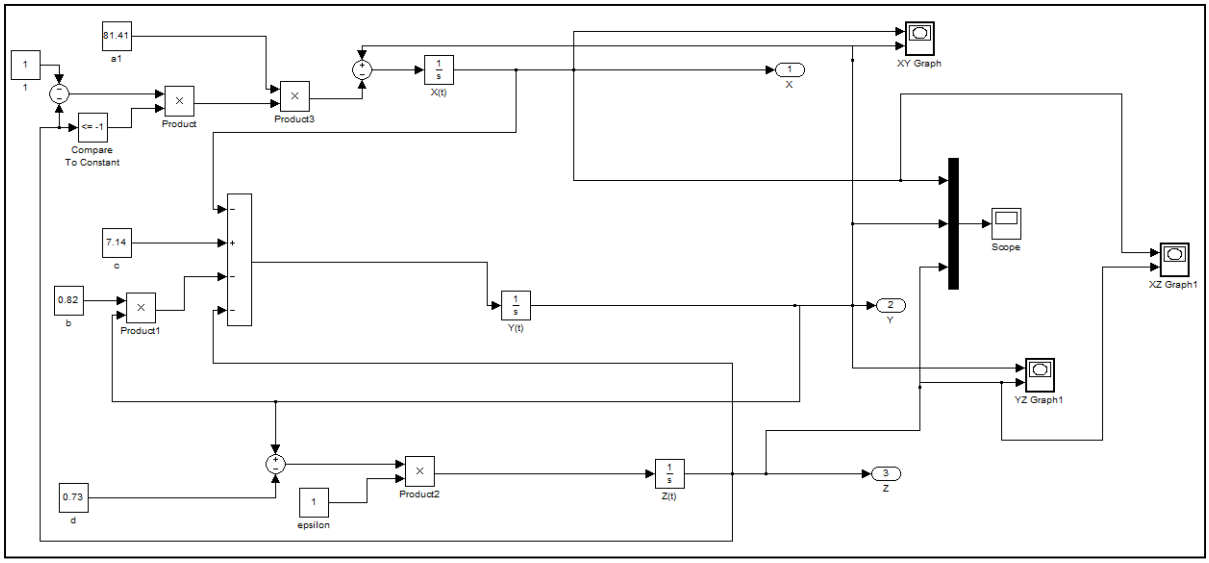


Figure 2.17. Simulation de l'oscillateur de Colpitts sous simulink.

La représentation temporelle des signaux $x(t), y(t), z(t)$ est donnée par la figure (2.19) :

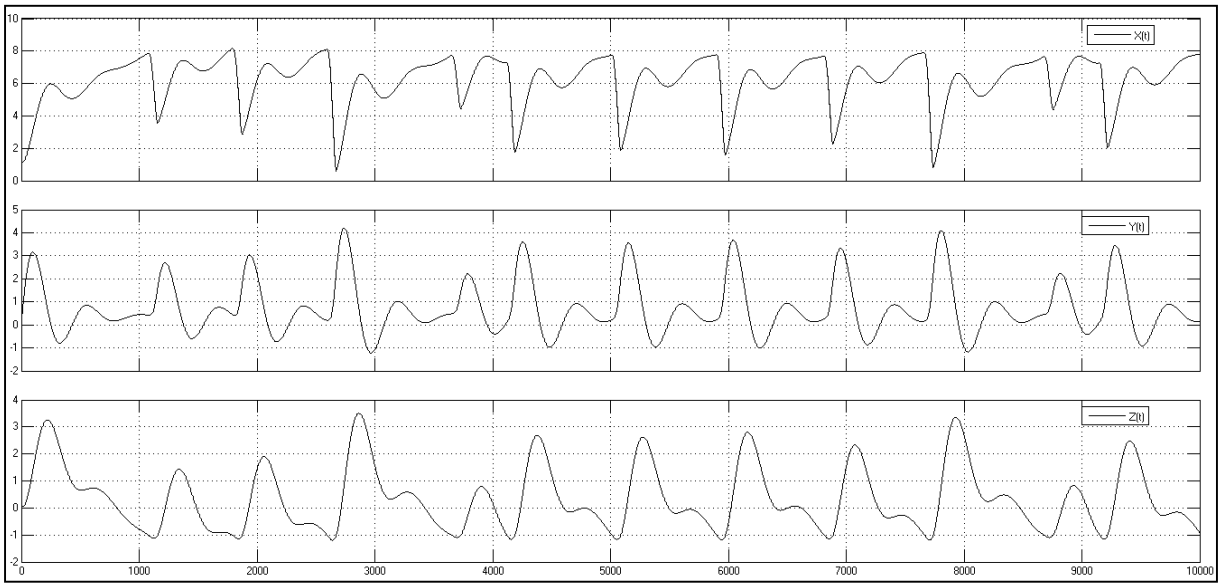


Figure 2.18. Représentation temporelle des signaux $x(t), y(t), z(t)$.

Les signaux apparaissent comme des signaux bruités mais ils sont déterministes, alors ça nous permet de déduire que l'oscillateur de Colpitts a un comportement chaotique pour les valeurs des paramètres prises dans la Simulation sous Simulink.

La figure suivante nous montre les plans de phases de gauche à droite $y(x), z(x)$, $z(y)$de l'oscillateur de Colpitts :

On remarque que l'oscillateur de Colpitts a un comportement chaotique car il existe des repliemets et des étirements complexes.

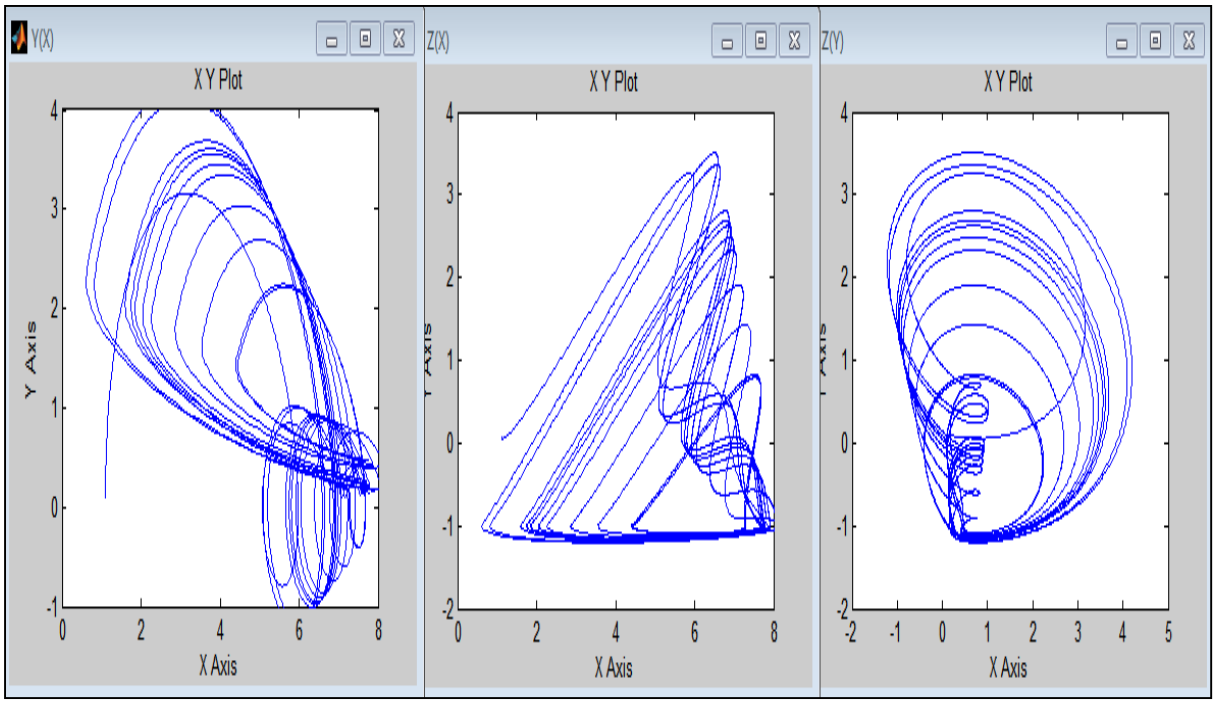


Figure 2.19. Plans de phases $y(x)$, $z(x)$, $z(y)$de l'oscillateur de Colpitts.

La figure (2.21) représente l'attracteur étrange de l'oscillateur de Colpitts :

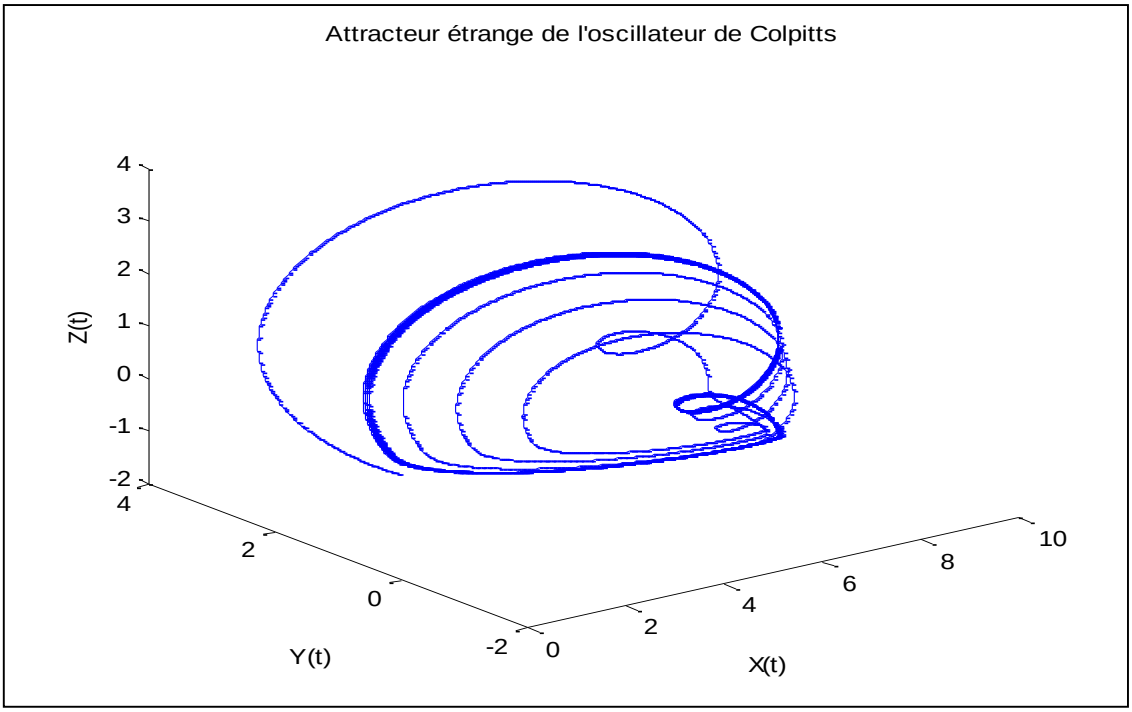


Figure 2.20. Attracteur étrange de l'oscillateur de Colpitts.

Dans ce chapitre, quelques définitions et notions sur les systèmes dynamiques chaotiques ont été présentées à savoir le point fixe, la stabilité de point fixe, la bifurcation, les exposants de Lyapounov et la section de Poincaré.

L'oscillateur chaotique de Colpitts a été analysé en mettant en évidence, ses propriétés chaotiques, en vue de son utilisation pour le cryptage d'un signal ECG, et qui sera développé dans le prochain chapitre.

Chapitre 3

Cryptage chaotique d'un ECG

La cryptographie ou l'art de chiffrer, de coder les messages est une science aussi vieille que l'écriture, elle assure la confidentialité, l'authenticité (la validation de la source du message pour assurer que l'expéditeur est correctement identifié), l'intégrité (l'assurance que le message n'a pas été modifié pendant la transmission) et la non répudiation (un expéditeur ne peut pas nier d'avoir envoyé le message et le récepteur ne peut pas nier sa réception).

Les premières applications des systèmes chaotiques en cryptographie sont proposées par Pecora et Carroll sur la possibilité de la synchronisation des deux systèmes chaotiques [22]. Les systèmes chaotiques ont plusieurs caractéristiques significatives favorables pour sécuriser les communications comme la sensibilité aux conditions initiales et l'aspect ressemblant à l'aléatoire.

Le principe du cryptage chaotique est de brouiller le signal message dans un signal chaotique par des différentes méthodes afin d'avoir un signal crypté y(t).

La figure suivante représente le schéma général d'un système de communication :

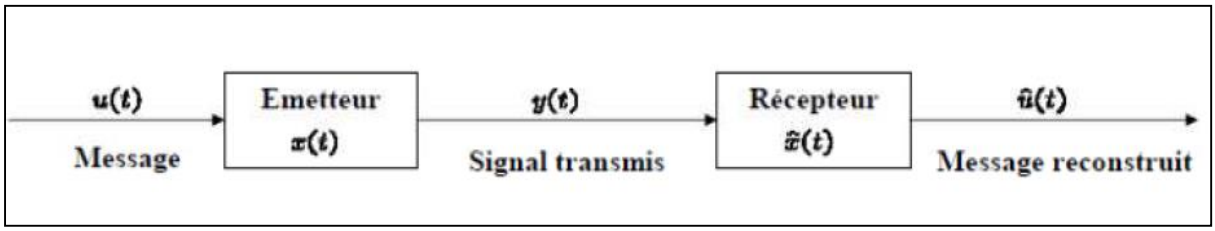


Figure3.1. Principe général d'un système de communication.

Dans ce chapitre, nous discuterons les différentes méthodes de cryptage et l'objectif de celui-ci ainsi que la différence entre le cryptage classique et le cryptage chaotique, puis nous présenterons la méthode utilisée dans notre travail qui est la méthode de cryptage par addition pour réaliser une transmission sécurisée du signal d'ECG.

3.1 Historique de cryptage :

La cryptographie a eu une histoire intéressante ; ses racines remontent vers 2000 avant J.C en Egypte, lorsque les hiéroglyphes furent utilisés pour décorer les tombes afin de raconter l'histoire de la vie du défunt. Une méthode de cryptographie de l'alphabet Hébreu requis pour être retournée afin que chaque lettre dans l'alphabet d'origine soit associée à une lettre différente dans l'alphabet inversé. Cette méthode de cryptage a été appelée méthode d'Atbash.

Vers 400 avant J.C, les Spartiates utilisaient un système de cryptage des informations, en écrivant un message sur une bande de papyrus puis l'enroulaient autour d'une scytale, qui

est considérée comme l'ancêtre des systèmes de transmissions secrètes [23]. C'est le premier instrument employé en cryptographie et le seul système fonctionnant à cette époque. Le message n'était lisible que s'il était entouré sur la bonne scytale (Figure 3.2).

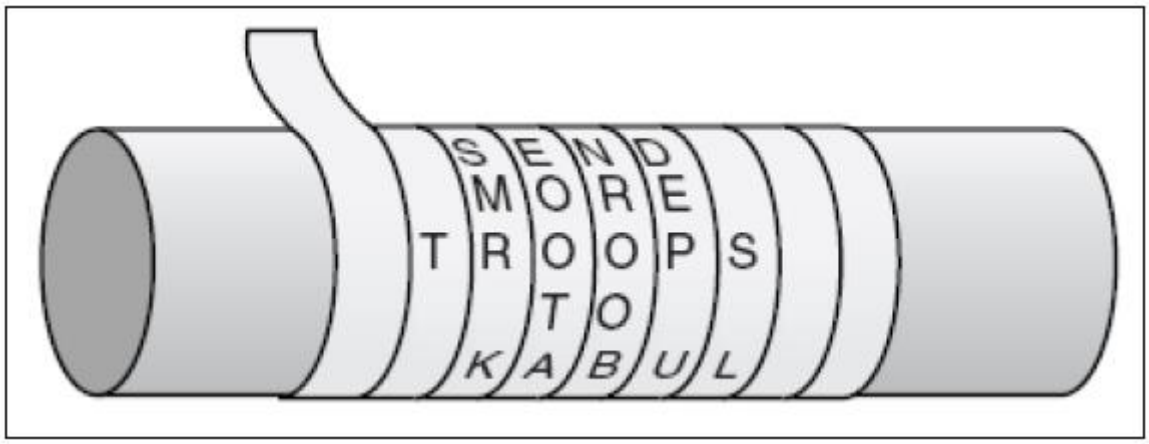


Figure 3.2. La scytale utilisée par les spartiates pour la transmission sécurisée [14].

En transmission sécurisée d'information binaire, le message appelée « texte » est transformée de manière à le rendre incompréhensible. Ce processus est appelée « chiffrement » ou « cryptage ». Par ailleurs, le destinataire doit engager un processus, appelée « déchiffrement » ou « décryptage », pour reconstruire le message à partir du texte chiffrée. Au cours de la Seconde Guerre Mondiale, des dispositifs de cryptage simplistes ont été utilisés pour la communication tactique, qui a été améliorée grâce à la technologie mécanique et électromécanique fournissant au monde le télégraphe et la communication radio.

La machine de chiffrement (Figure 3.3) la plus célèbre de l'histoire à ce jour est la machine allemande Enigma.

Figure 3.3. La machine allemande Enigma**.**

L'idée d'utiliser des signaux aléatoires pour la communication sécurisée a été mise en œuvre en 1926 par Vernam. Il proposa dans son article d'utiliser un alphabet binaire et de coder chaque bit à l'aide d'un bit de la clef, choisi de façon arbitraire [13].

Plus tard, dans les années 90, cette idée a été développée dans le contexte des signaux chaotiques, la nature semblable au bruit des signaux chaotiques a motivé les chercheurs en essayant de camoufler un message confidentiel à l'aide d'un signal chaotique, de façon a ne pas pouvoir le distinguer.

Les premières applications des systèmes chaotiques en cryptographie sont proposées par Pecora et Carroll comme une possible application de la synchronisation des systèmes dynamiques chaotiques [24].

Des différentes méthodes ont été proposées afin de masquer le message dans un système chaotique et ensuite de le restaurer. Ces méthodes sont toutes basées sur la synchronisation des systèmes chaotiques et ont été améliorées au fil des années, dans le but d'augmenter de plus en plus la sécurité et la rapidité de la transmission de l'information. Ces méthodes sont parfois appelées méthodes de cryptographie chaotique.

3.2 Méthodes de transmission chaotique :

La méthode de cryptage chaotique a été la première solution proposée dans la littérature comme application du chaos aux communications. Il a été possible d'employer des signaux chaotiques continus comme porteur d'informations. Dans ce cas, le message est codé par l'émetteur et il est décodé et extrait du signal chaotique par le récepteur [23].

Parmi les méthodes de transmission chaotique, on peut citer la méthode par addition, la commutation chaotique, la modulation chaotique, et la méthode par inclusion.

3.2.1 Méthode par addition :

Dans cette méthode, appelée aussi masquage chaotique, son principe est de brouiller le signal message dans un signal chaotique, par une opération d'addition directe avant de le transmettre. L'émetteur est ainsi un système chaotique autonome dont le signal de sortie est ajouté au signal message. La somme des deux signaux est transmise au récepteur à travers le canal de transmission, qui est un canal public. Le récepteur est constitué d'un système chaotique identique à l'émetteur et d'un simple soustracteur.

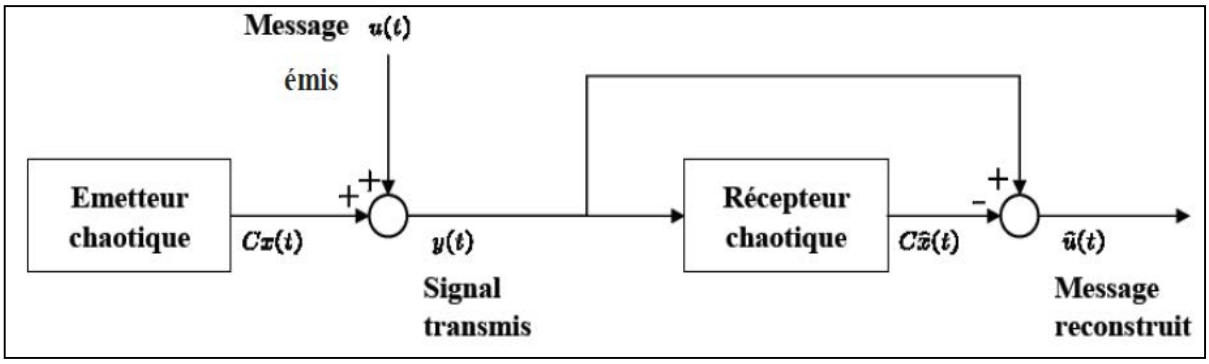


Figure 3.4. Cryptage par addition [23].

3.2.2 Méthode par commutation chaotique :

Cette méthode (appelée aussi Chaos Shift Keying ou CSK) est utilisée pour transmettre un message binaire. L'émetteur est composé de deux systèmes chaotiques et pour chaque niveau du message (0 ou 1), l'un des systèmes envoie sa sortie sur la ligne de transmission.

Le récepteur est constitué de deux systèmes chaotiques identiques à ceux de l'émetteur. Pour chaque valeur du message, l'un des deux systèmes se synchronise avec l'émetteur et un bloc de comparaison permet de relever la valeur du message. Le schéma représentatif de cette méthode est montré dans la figure (3.5).

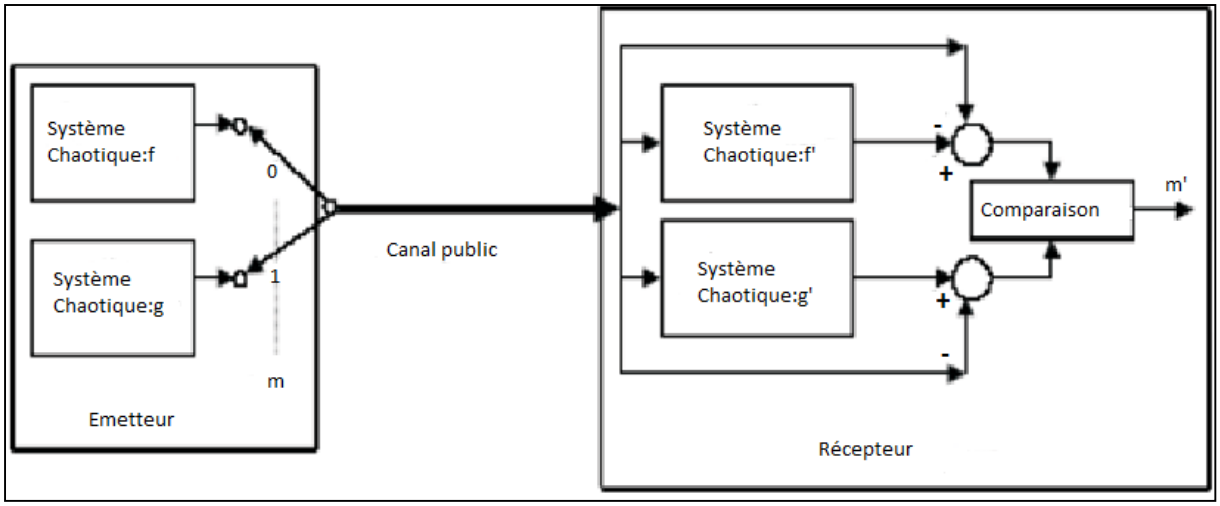


Figure 3.5. Méthode par commutation chaotique [13].

3.2.3 Méthode par modulation chaotique :

L'approche par modulation utilise le message contenant l'information pour moduler un ou plusieurs paramètres de l'émetteur chaotique .Un controleur adaptatif est chargé de maintenir la synchronisation au niveau du récepteur, tout en suivant les changements du paramètre modulé (Figure 3.6).

Au niveau de l'émetteur , le fait de moduler un ou plusieurs paramètres impose à la trajectoire un changement continu d'attracteur, de ce fait, le signal transmis est plus complexe qu'un signal chaotique « normal ». Cependant, la façon d'injecter le message est donc la fonction de modulation des paramètres ne doivent pas supprimer le caractère chaotique du signal envoyé au récepteur [23].

Cette technique exploite les qualités et les propriétés des systèmes chaotiques, elle n'a pas d'équivalent parmi les systèmes de communication « classique ».

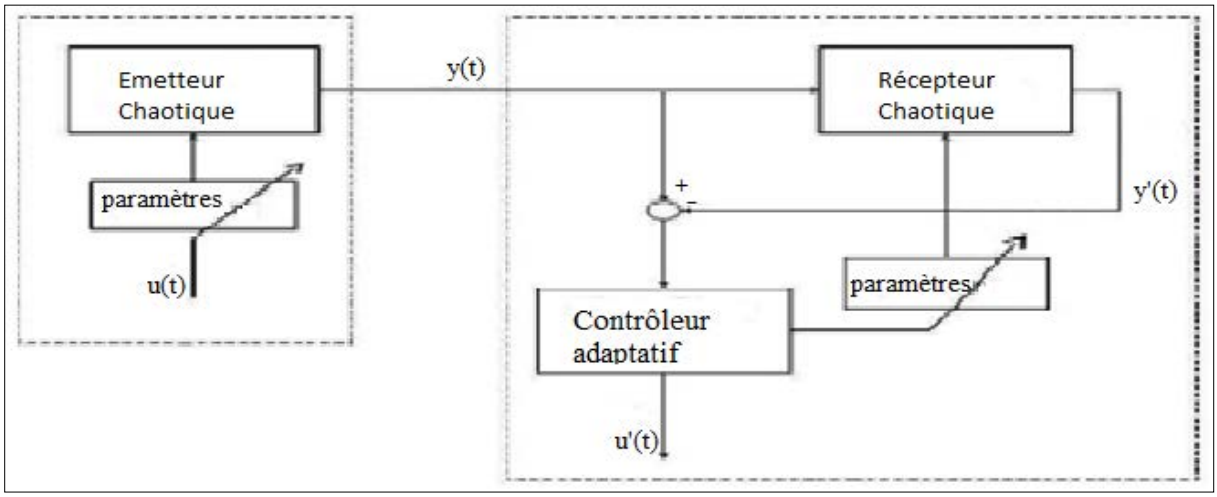


Figure 3.6. Méthode par modulation chaotique [23].

3.2.4 Méthode par inclusion :

Cette technique de cryptage consiste à injecter le message dans la dynamique de l'émetteur, sans toutefois réaliser une modulation de paramètre. La restauration de l'information se fait principalement par deux techniques, reposant soit sur les observateurs à entrées inconnues, soit sur l'inversion du système émetteur [13].

3.3 Objectifs de la transmission chaotique :

L'utilisation du signal chaotique dans la transmission sécurisée a deux objectifs principaux :

-Le premier objectif est de protéger l'information transmise (on retrouve ainsi le même type d'application que celles des méthodes de cryptographie classiques).

-le deuxième objectif est d'étaler le signal informationnel (étalement de spectre), dans ce cas, on retrouve aussi des méthodes développées comparables aux systèmes classiques à étalement de spectre.

3.4 Comparaison entre la cryptographie classique et chaotique :

Cryptographie classique	Cryptographie chaotique
Valeurs entières sur un corps fini	Valeurs continues en utilisant une représentation en virgule fixe ou flottante
Méthodes algébriques	Méthodes analytiques
Réalisation numérique en arithmétique entière	Réalisation numérique en arithmétique non entière

Tableau3.1. La comparaison entre le cryptage chaotique et classique [23].

3.5 Synchronisation chaotique :

La synchronisation de deux systèmes dynamiques signifie que chaque système évolue en suivant le comportement de l'autre système. Plusieurs concepts de synchronisation chaotique ont été proposés en commençant avec Yamada et Fujisaka qui ont utilisés une approche locale de la synchronisation chaotique [14], puis Afraimovich et all ont développés les concepts importants liés à la synchronisation chaotique. Par la suite, Pecora et Carrol ont défini la synchronisation chaotique sous le nom de « synchronisation identique », développée sur la base de circuits chaotiques couplés, l'un est le maitre, l'autre est l'esclave.

Il existe deux grands types de synchronisation dépendant de la méthode de couplage de ces deux systèmes chaotiques, à savoir la synchronisation unidirectionnelle et la synchronisation bidirectionnelle.

3.5.1 Synchronisation Unidirectionnelle :

Si avec un moyen quelconque, on permet à deux oscillateurs chaotiques d'échanger leur énergie, c'est une action que l'on nomme « couplage », les deux systèmes changent de comportement vers un comportement commun : « ils se synchronisent ». Dans le cas d'un couplage unidirectionnel, l'énergie est transférée d'un système à l'autre, à l'aide d'un élément de couplage fonctionnant dans un seul sens comme par exemple un suiveur.

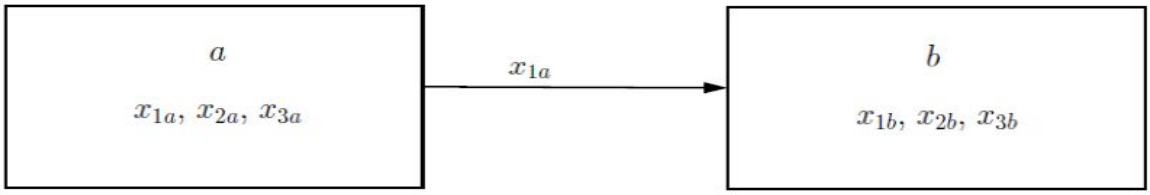


Figure 3.7. Synchronisation Unidirectionnelle [23].

Supposons qu'on a deux systèmes dynamiques identiques représentés par les deux équations suivantes :

$$\dot{x} = f(x,t) \tag{3.1}$$

$$\dot{y} = f(y,t) \tag{3.2}$$

Si l'équation (3.2) va être modifié par l'effet d'accouplement, et si le résultat de cette modification nous donne de nouvelles équations de la forme:

$$\dot{x} = f(x,t) \tag{3.3}$$

$$\dot{y} = g(y,x,t) \tag{3.4}$$

tel que $g(y,x,t)= f(y,t)$ pour $x = y$, dans ce cas, on parle de l'accouplement unidirectionnel.

Le premier système s'appelle système émetteur (maître), et le deuxième système récepteur (esclave).

3.5.2 Synchronisation bidirectionnelle :

Dans le cas d'un couplage bidirectionnel, l'énergie est transférée d'un système à l'autre, à l'aide d'un élément de couplage fonctionnant dans les deux sens, comme par exemple une simple résistance (Figure 3.8).

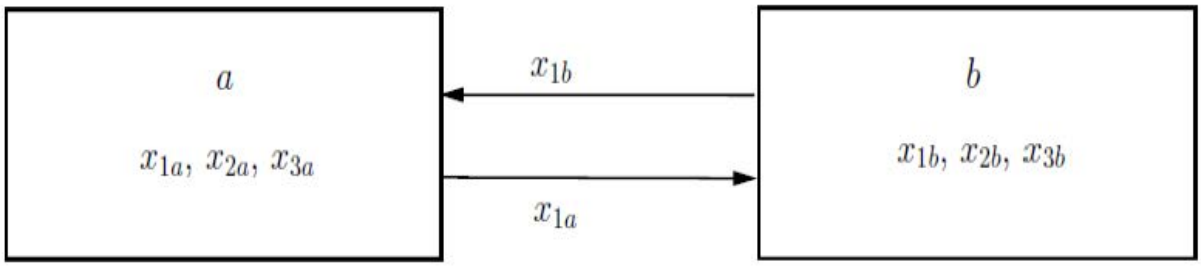


Figure 3.8. Synchronisation bidirectionnelle [23].

On considère les deux systèmes donnés ci-dessous :

$$\begin{cases} \dot{x} = f(x) + \lambda\,(z - x) \\ \dot{z} = g(z) + \mu(x - z) \end{cases} \tag{3.5}$$

où x ,z ∈ $\mathbb{R}^n$ et λ , μ sont des matrices diagonales n×n. λ = diag [λ_i], μ =diag[μ_i]

i=1,2,..... n. On suppose que $f(0) = g(0) = 0$. Le problème de synchronisation consiste alors à trouver λ et μ de telle manière que :

$$\lim_{i\to\infty} = \|z(t) - x(t)\| = 0.$$

Cette méthode a été étudiée dans [25] et a été appliquée à l'oscillateur de Colpitts dans [21][26]. La figure (3.9) illustre ce type de synchronisation.

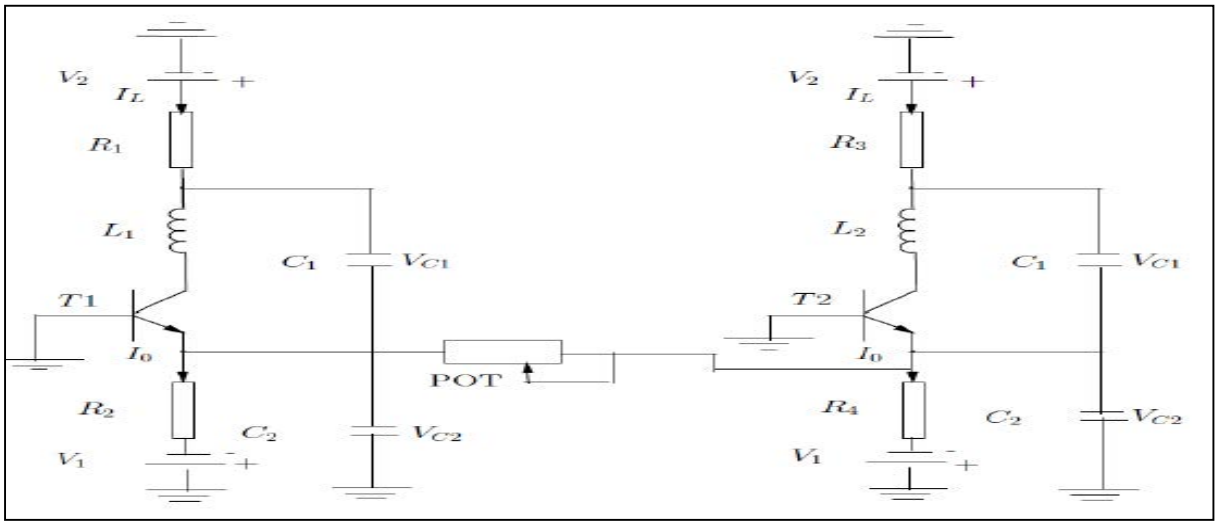


Figure 3.9. Synchronisation bidirectionnelle de deux oscillateurs de colpitts [23].

3.5.3 Synchronisation par décomposition du système :

Cette méthode a été utilisée dans les travaux de Carroll et Pecora [24]. Son principe est de décomposer le système émetteur, qui est représenté par l'équation (3.1) en deux sous systèmes représentés par :

$$\begin{cases} \dot{x} = f(x,t) & (3.6) \\ \dot{x}1 = f1(x1,x2) & (3.7) \\ \dot{x}2 = f2(x1,x2) & (3.8) \end{cases}$$

Avec $x1 \in R^d$, $x2 \in R^m$, d + m = n. et $x = (x1, x2)$.

Dans ce cas le système récepteur est donné par l'équation suivante :

$$\dot{Y} = f2(x1, Y) \quad (3.9)$$

3.6 Multiplexage temporel :

On appelle multiplexage temporel, la capacité à transmettre sur un seul support physique (appelé *voie haute vitesse*), des données provenant de plusieurs paires d'équipements ; on parle alors de *voies basse vitesse*. Le principe de fonctionnement de multiplexage temporel est représenté sur la figure (3.10) :

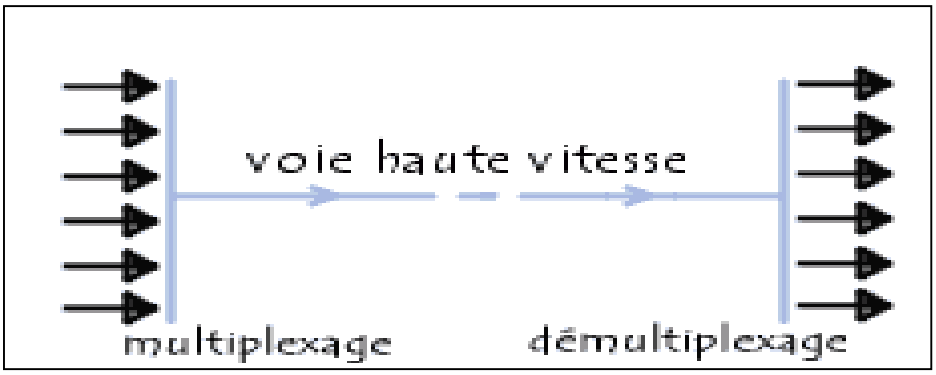


Figure 3.10. Multiplexage temporel.

On appelle « multiplexeur » ou TDM (Time Division Multiplexer), l'équipement de multiplexage permettant de combiner les signaux provenant des émetteurs pour les faire transiter sur la voie haute vitesse. On nomme « démultiplexeur » ou TDD (Time Division Demultiplexer), l'équipement de multiplexage sur lequel les récepteurs sont raccordés à la voie haute vitesse.

Ce multiplexage permet, entre autres, de faire passer des flux synchrones ou asynchrones sur une liaison synchrone. Les paquets n'arrivent pas nécessairement dans l'ordre d'émission selon les chemins empruntés, le rôle du démultiplexeur est alors de les réordonner et de séparer les flux des différents canaux, de manière à restituer l'information telle qu'elle était avant son transport sur le réseau multiplexé.

La figure (3.11) donne le schéma bloc du système de la transmission chaotique basée sur le multiplexage temporel qui est utilisé dans notre travail. L'oscillateur chaotique de Colpitts permet la génération du signal chaotique qui sera ensuite ajouté au signal message. Cette technique est simple dans sa conception et approprié pour les signaux de faible amplitude comme l'ECG.

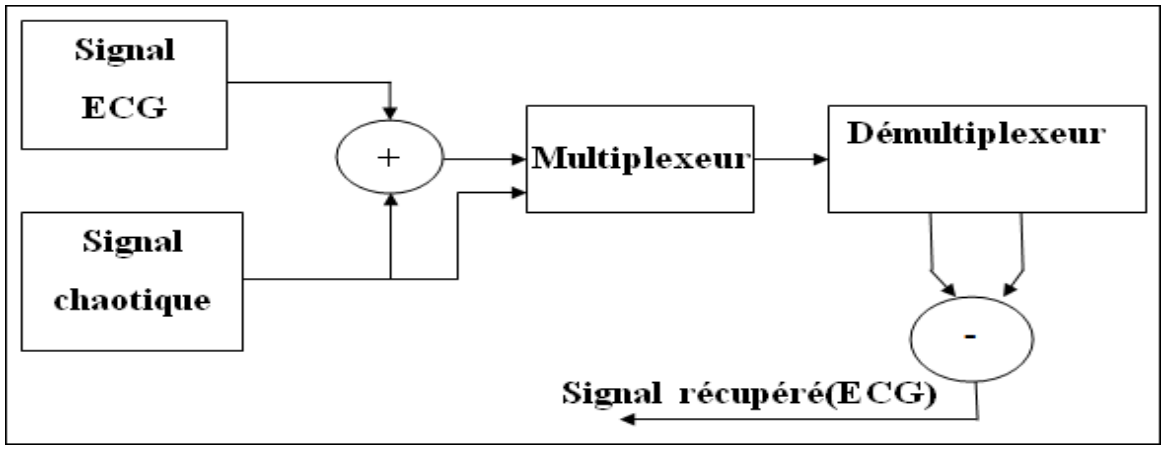


Figure 3.11. Schéma synoptique de la transmission chaotique.

3.7 Résultats de simulation :

La figure suivante représente la simulation de la transmission chaotique en utilisant le TDM et le TDD sous environnement Matlab Simulink :

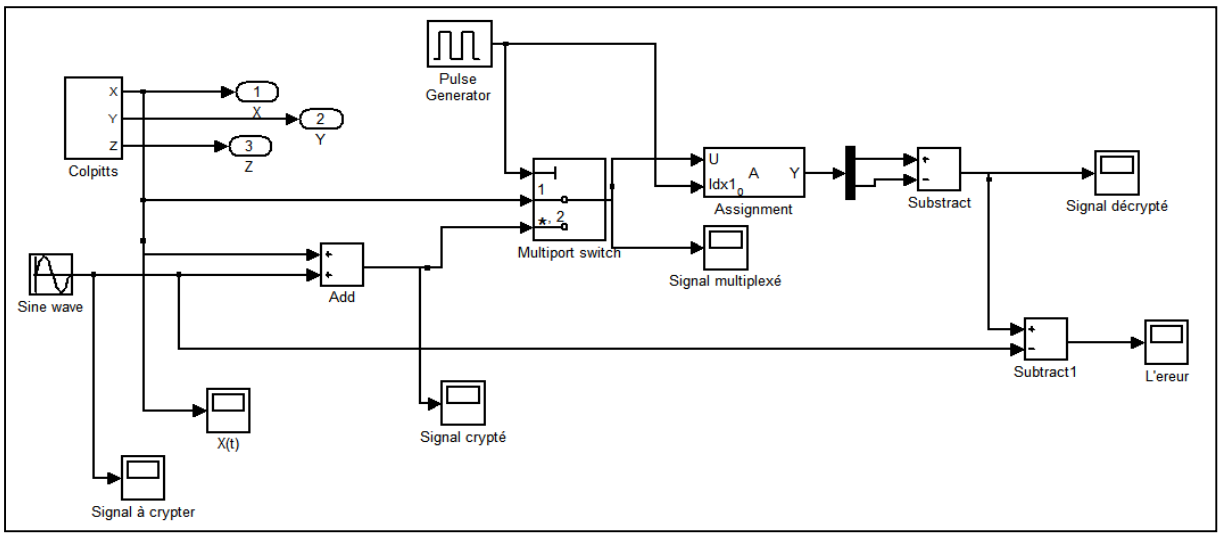


Figure 3.12. Transmission chaotique sous Simulink.

Le signal informatif est ajouté au signal chaotique de Colpitts en utilisant le bloc « add ». La sortie de l'additionneur (le signal crypté) est multiplexé avec le même signal chaotique dans le bloc « Multiport Switch » donnant le signal transmit, ce dernier est décrypté par le bloc « Assignment » pour récupérer le signal crypté ainsi que le signal chaotique.

En utilisant le bloc « Substract », on soustraite les deux sorties de démultiplexeur afin d'avoir le signal informatif.

Le bloc « Pulse Generator » a pour but de générer des impulsions pour le TDM et le TDD, il joue le rôle d'une horloge.

Par une soustraction de message décrypté avec le message d'origine, on a obtenu un erreur d'ordre de 10^{-3} (très faible), alors les signaux sont identiques.

La figure (3.13) est obtenue au niveau de l'oscillateur de Colpitts, c'est le signal chaotique :

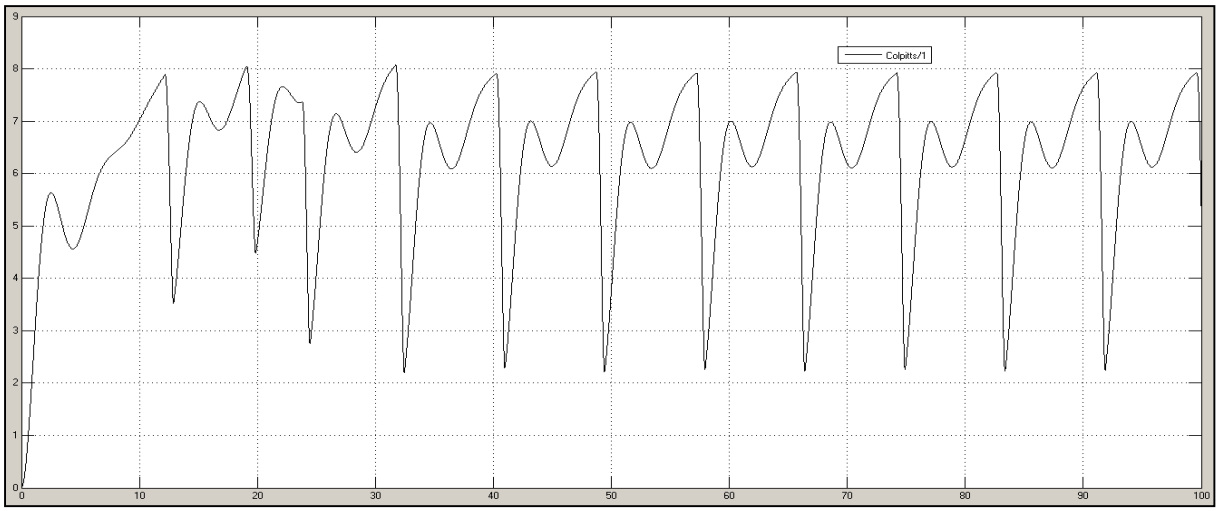


Figure 3.13. Signal chaotique x(t).

Le signal informatif est représenté sur la figure suivante :

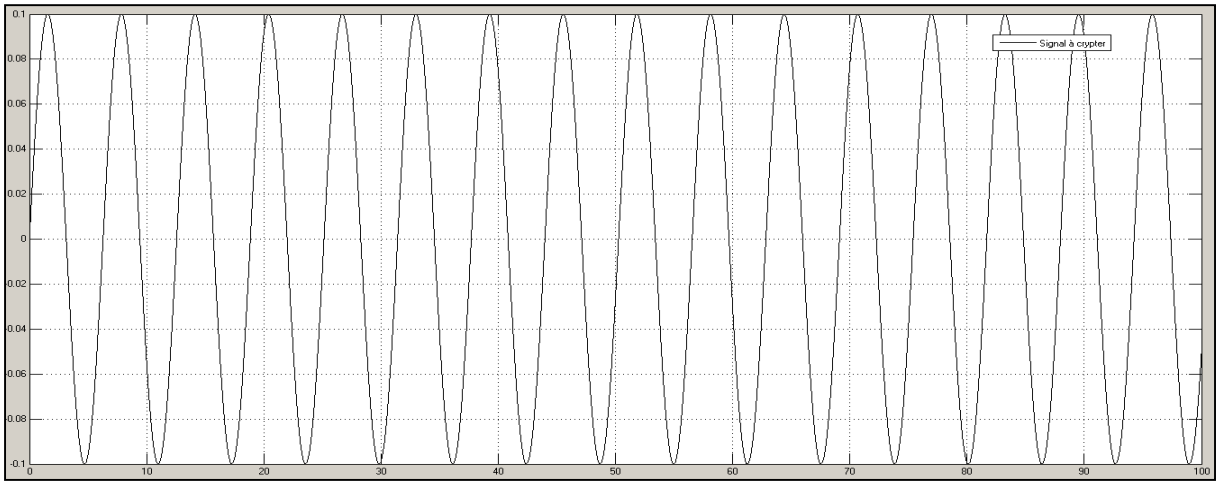


Figure 3.14. Signal à crypter.

La figure (3.15) montre le signal crypté après l'addition du signal chaotique avec le signal message :

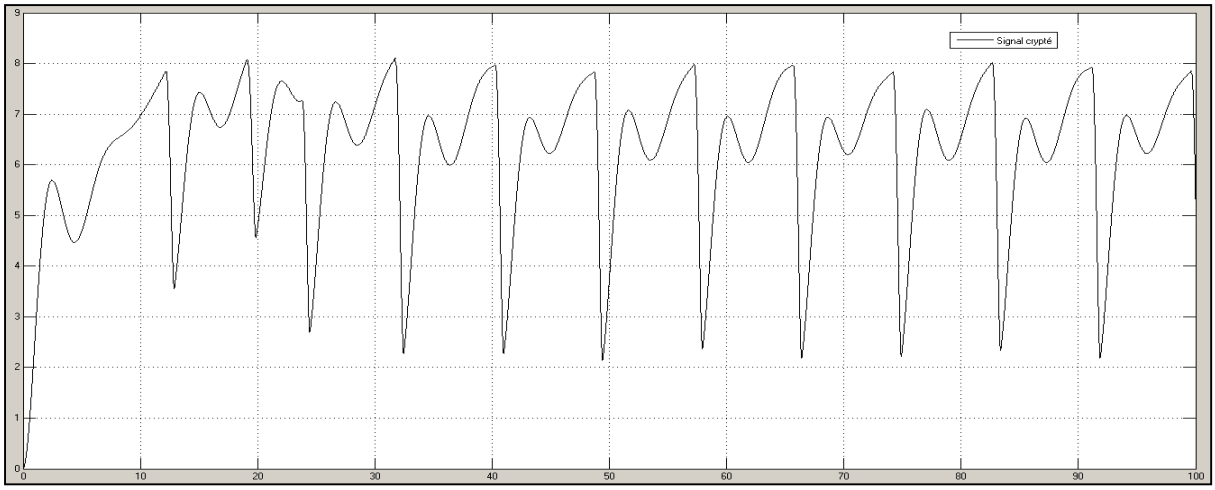


Figure 3.15. Signal crypté.

Afin de transmettre le signal crypté dans le canal de transmission, on doit multiplexé ce dernier avec le signal chaotique, le résultat de simulation est représentée dans la figure suivante :

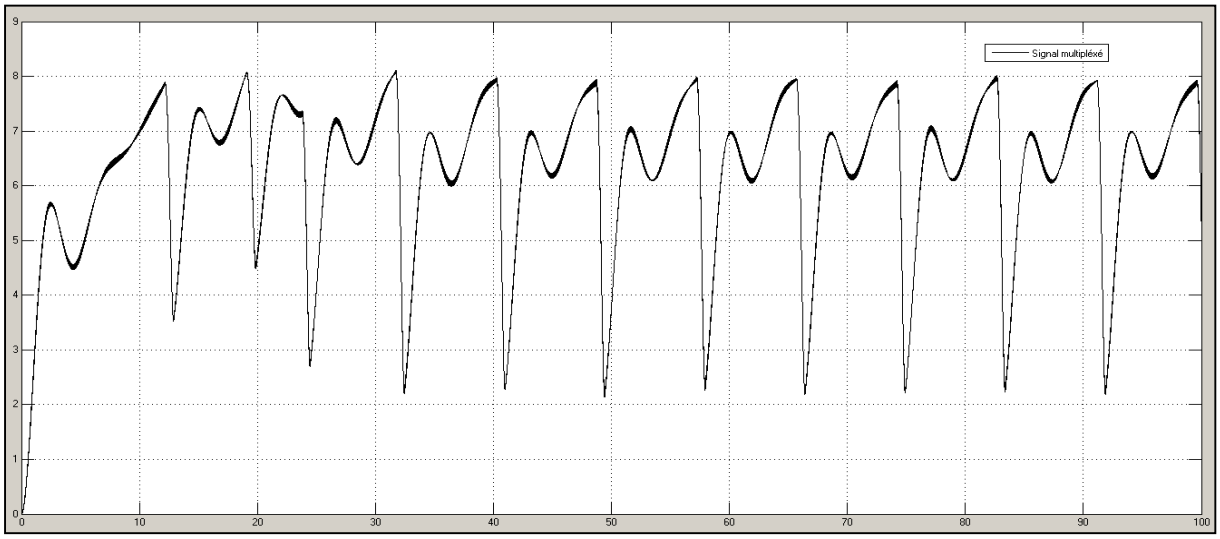


Figure 3.16. Signal multiplexé.

Au niveau du récepteur, on a démultiplexé le signal multiplexé pour récupérer le signal message et le signal chaotique, la figure (3.17) représente le signal récupéré au niveau du récepteur :

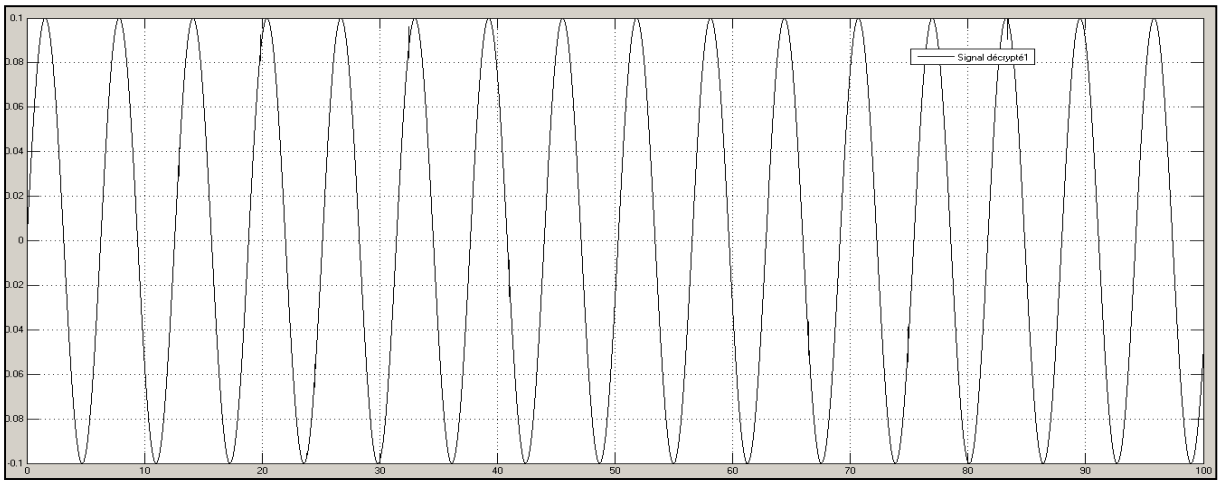


Figure 3.17. Signal décrypté.

Dans ce chapitre, les concepts de base sur les différents types de cryptage et de synchronisation chaotique ont été introduits. Puis, on présenté la méthode de cryptage par addition ainsi que le multiplexage temporel utilisé pour la transmission chaotique. Les

résultats de la simulation ont été donnés, le message crypté a bien été récupéré au niveau du récepteur.

Dans le prochain chapitre, une implémentation de la transmission chaotique de l'ECG sur une cible FPGA sera décrite et analysée.

Chapitre 4

Implémentation FPGA et résultats expérimentaux

Actuellement, la conception des composants numériques rapides et à plus forte densité d'intégration est possible grâce à l'évolution des technologies numériques. La partie expérimentale de notre projet se focalise sur l'implémentation FPGA (Field Programmable Gate Array) du système de cryptage et de décryptage chaotique étudié dans les chapitres précédents. Cependant, ce type d'implémentation numérique sur FPGA nécessite d'utiliser des outils spécifiques dans le cadre d'une méthodologie de conception adaptée [13].

Dans ce chapitre, après la description de la technologie FPGA, on présente le flot de conception ISE de Xilinx et de co-simulation sous environnement Matlab Simulink – Système Générator Xilinx qui permet l'implémentation du système de cryptage chaotique sur FPGA ainsi la simulation hardware de l'architecture implémentée. On décrit la plateforme FPGA VIRTEX5 et la carte de conversion CAN (Conversion Analogique-Numérique) et CNA (Conversion Numérique-Analogique) constitué du CODEC audio AC97 disponible au niveau de la carte FPGA Virtex 5. On termine le chapitre par la présentation des résultats expérimentaux et leurs comparaisons aux résultats simulés.

4.1 Description des composants FPGA :

Les FPGA sont des circuits contenant des milliers ou des millions de transistors connectés pour réaliser des fonctions logiques ; ceux sont des composants VLSI (Very Large Scal Integration) programmables par l'utilisateur. Ils sont constitués de trois parties essentielles :

-Une matrice de blocs logiques configurables CLB (Configurable Logic Bloc).

-Des blocs d'entrées\sorties configurables.

-Un réseau d'interconnexions programmables.

Plusieurs constructeurs fabriquent des composants FPGA tel que Actel, Xilinx qui utilisent différentes technologies. Parmi ces technologies, celles qui assurent une reprogrammation des FPGA sont les plus intéressantes car elles permettent une grande flexibilité de conception.

Les différentes technologies reprogrammables des FPGA sont : la technologie EPROM (Erasable programmable Read-Only Memory), la technologie EEPROM (Electrically Erasable Programmable Read-Only Memory), la technologie Static RAM (SRAM) ainsi que la technologie FLASH [27].

La figure (4.1) montre l'architecture générique d'un circuit FPGA :

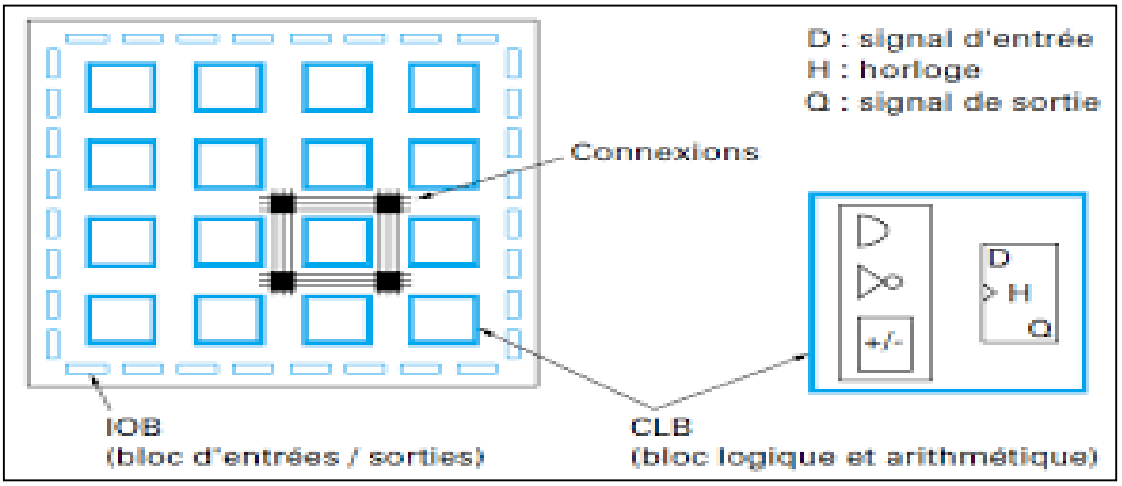


Figure 4.1. Description de l'architecture générique d'un circuit FPGA.

4.2 Processus d'implémentation :

Les outils de CAO (Conception Assistée par Ordinateur) sont utilisés pour effectuer la conception des architectures de commande. La saisie est faite graphiquement ou en utilisant un langage de description HDL (Hardware Description Language). Les deux langages standards les plus fréquemment utilisés sont : le VHDL (Very high speed integrated Hardware Description Language) [28] et le Verilog [29]. L'avantage de ces langages est la compatibilité avec toutes les technologies FPGA précédemment introduites et sont donc portables ; ils offrent au concepteur différents niveaux de description.

Les différentes étapes de programmation sur FPGA sont présentées par la figure (4.2). Premièrement, une Netlist est générée par le synthétiseur des outils CAO qui décrit la connectivité de l'architecture de façon optimale. Ensuite, l'outil de placement-routage place effectue le routage entre toutes les cellules logiques. Grace à ces deux étapes, on obtient un fichier de configuration appelé bitstream à télécharger dans la mémoire de configuration du FPGA, ce fichier pouvant être directement chargé sur FPGA à partir d'un ordinateur hôte [13].

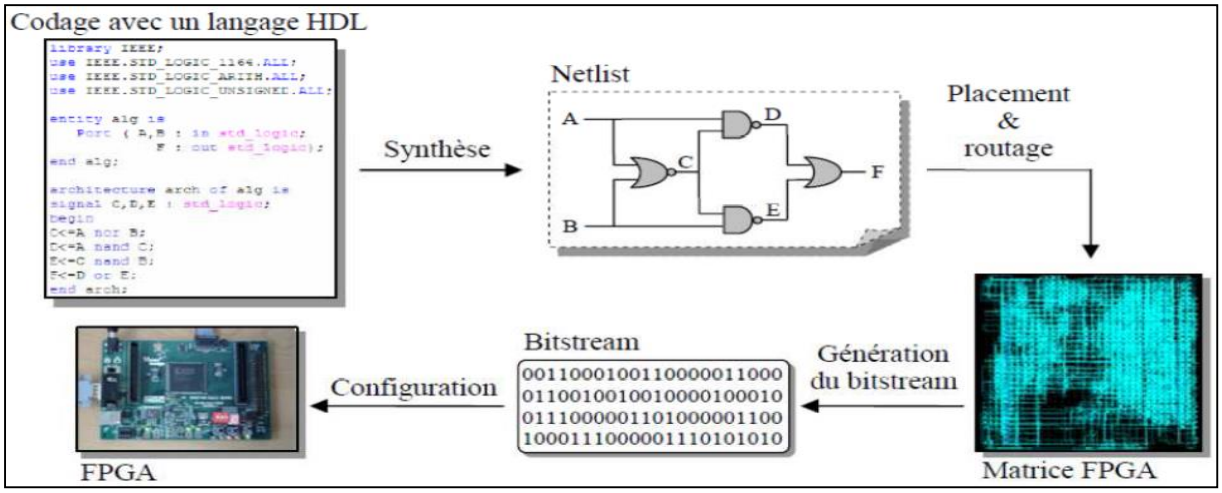


Figure 4.2. Les étapes de programmation sur un FPGA.

Afin d'élaborer l'implémentation du modèle sur FPGA, on a utilisé le logiciel System Generator sur Simulink. Cela nous permet de créer un modèle sous MATLAB-Simulink-System Generator et d'effectuer les simulations avec des résultats comparables à ceux obtenus sous Simulink. On a suivi cette approche pour réduire le temps de conception sur FPGA.

Au début, il suffit que le logiciel System Generator crée un dossier NGC contenant toutes les informations sur le bloc (ses ports d'entrée et de sortie ainsi que la façon dont laquelle il sera implémenté sur notre FPGA), par la suite, il faut importer ce fichier dans un autre environnement de travail, l'ISE de XILINX afin d'effectuer l'implémentation sur FPGA. La plate-forme FPGA utilisée est la carte VIRTEX 5 (ML501) construite autour du circuit xc5vlx50-1ff676.

4.2.1 Présentation de logiciel ISE :

L'ISE (Integrated Software Environment) est un logiciel de programmation des produits XILINX tels que les CPLD (Complex Programmable Logic Device) et les FPGA (Spartan, Virtex…). Il intègre différents outils qui permettent de passer du flot de conception à un système numérique à savoir :

-Un éditeur de schémas, de textes et de diagrammes d'états.

-Un compilateur VHDL et Verilog.

-Un simulateur.

-Un outil de la gestion des contraintes temporelles.

-Un outil de synthèse.

-Un outil de vérification.

-Un outil d'implémentation sur FPGA et CPLD.

Les étapes nécessaires pour l'implémentation d'un circuit FPGA sont présentées sur la figure (4.3) ; il y a quatre étapes [27] :

- La spécification : contient les trois groupes de saisie d'un circuit électrique (Schémas, diagramme d'états, HDL). Après la synthèse, un fichier netlist sera généré décrivant ainsi les interconnexions entre les registres.

- La vérification du design : permet au concepteur d'observer et de vérifier le comportement de code HDL avec un simulateur simulant le circuit s'il existe des vecteurs de test.

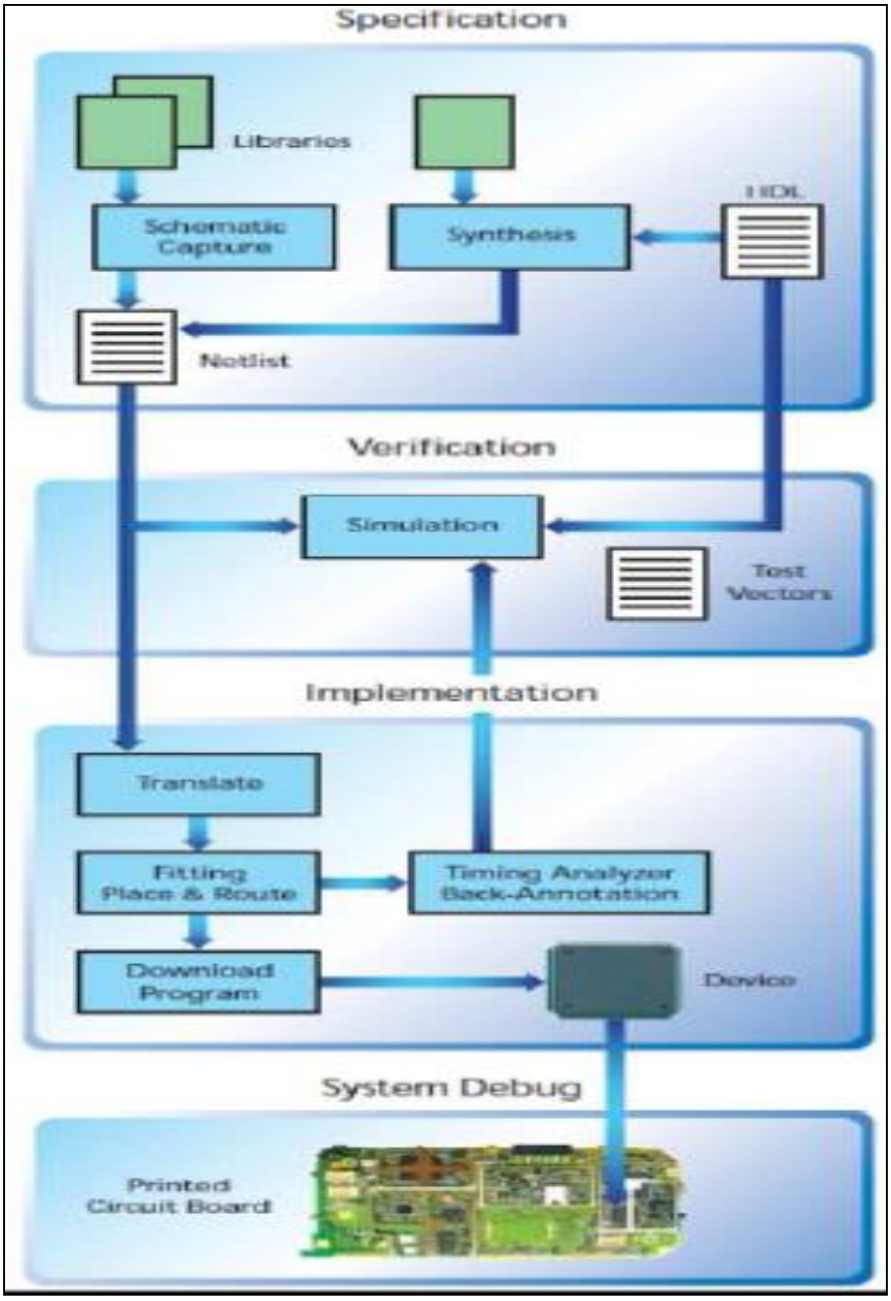


Figure 4.3. Les étapes de l'implémentation sur FPGA sous ISE [13].

- L'implémentation sur le composant : est la spécification des références exactes de celui-ci, à savoir : le boitier, la fréquence de travail et d'autres options spécifiques à chaque composant. Cette étape est décomposée en trois sous-étapes :

✓ Fitting : C'est le dimensionnement de la conception en fonction des ressources internes du composant cible.

✓ Place and Route : Après la compilation de code, les sous-programmes de placement et de routage seront exécutés.

- Place : est le processus suivi pour sélectionner les blocs logiques où les portes logiques sont placées.
- Route : est l'interconnexion entre les blocs logiques.

✓ Downloding (Programming) : Le chargement du fichier généré (bitstream) sur le FPGA ciblé par l'application.

-Le débogage du système : ce sont les tests effectués sur le circuit implémenté après le chargement des interconnexions sur le FPGA pour vérifier le bon fonctionnement de l'implémentation.

La figure (4.4) représente l'interface Project Navigator de ISE 14.2 qui permet l'accès à toutes les ressources d'un projet ainsi qu'aux outils d'implémentation.

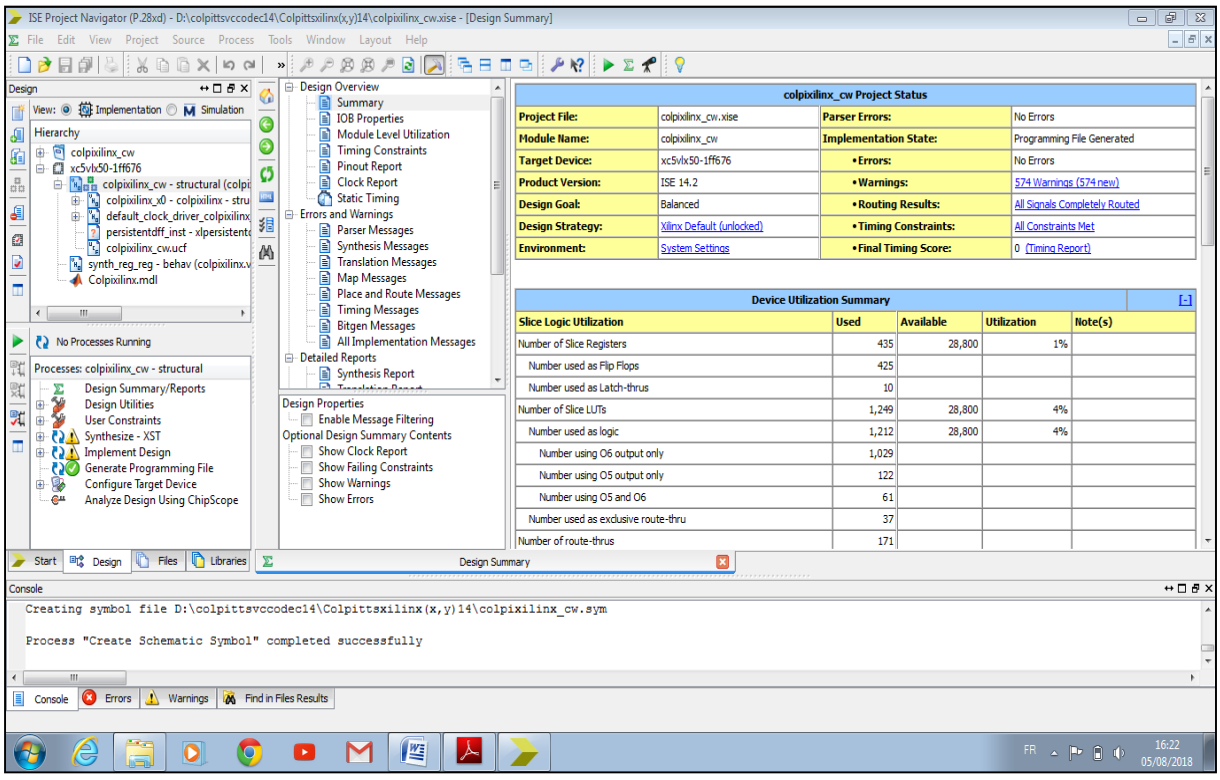


Figure 4.4. Interface Project Navigator ISE 14.2.

4.2.2 Présentation de System Generator et de la Co-simulation :

System Generator est un outil de design fourni par XILINX permettant l'utilisation de l'environnement MATLAB-Simulink afin de concevoir des applications sur les FPGA ; c'est une interface entre MATLAB-Simulink et ISE XILINX comme représenté sur la figure (4.5). Les principales tâches qui peuvent être exécutées dans cet environnement sont [30]:

- ✓ Génération automatique du code HDL (VHDL, Verilog).
- ✓ Conception et simulation des systèmes dans Simulink (environnement graghique).
- ✓ Co-simulation logicielle (Simulink)-Matérielle (FPGA) par communication JTAG ou USB.

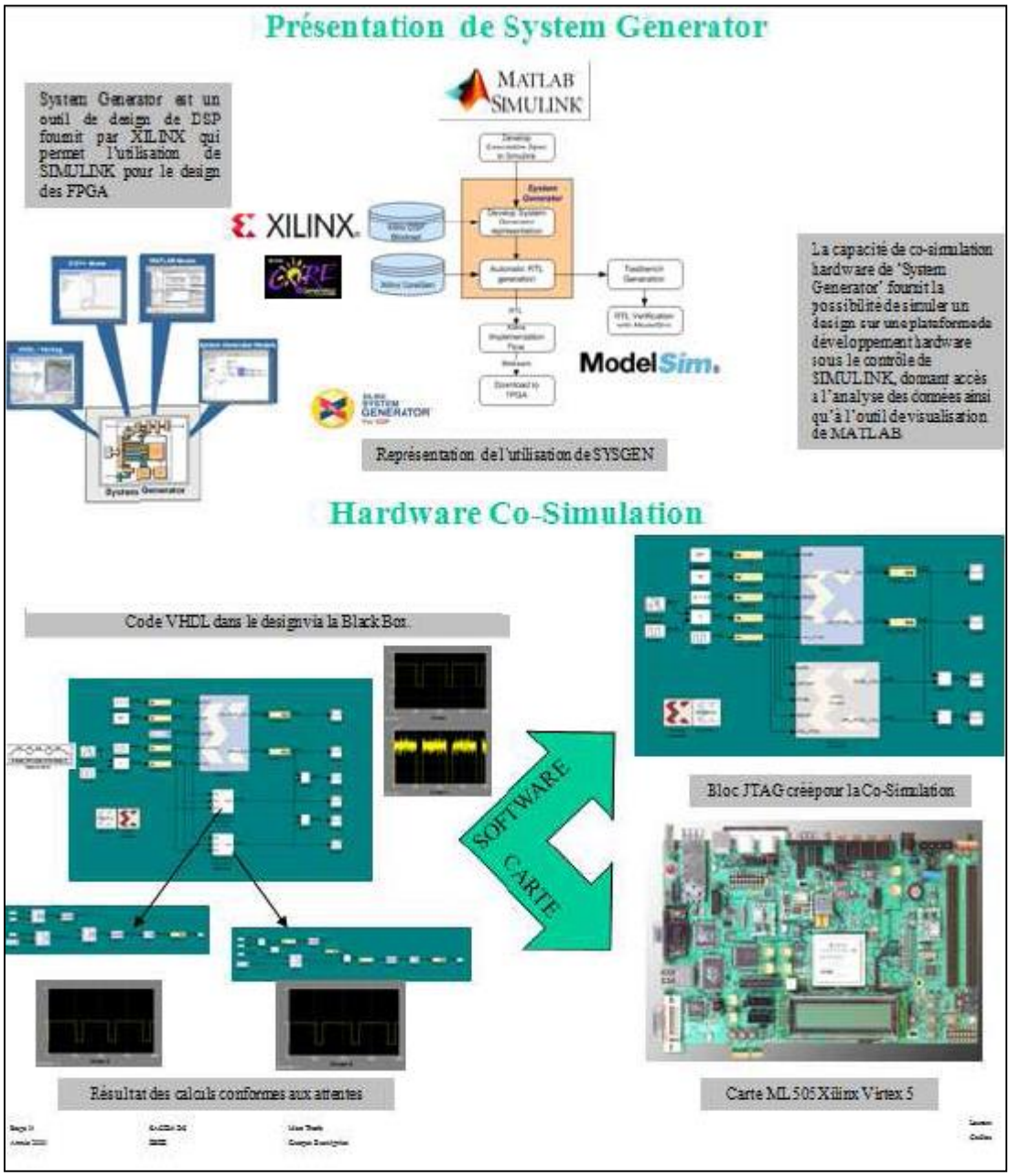


Figure 4.5. Environnement Simulink System Generator et Co-simulation [13].

4.3 Réalisation expérimentale de l'implémentation :

Le schéma bloc de l'implémentation expérimentale du cryptage chaotique est donné sur la figure (4.6). Il est constitué des éléments suivants :

- ✓ Un étage de Conversion Analogique-Numérique (CAN) afin d'inclure le message à transmettre au niveau de l'émetteur.
- ✓ La plate-forme VIRTEX5 pour implémenter la transmission chaotique.
- ✓ Un étage de Conversion Numérique-Analogique (CNA) qui a pour but de récupérer le message au niveau de récepteur et d'afficher les différents signaux sur un oscilloscope numérique.

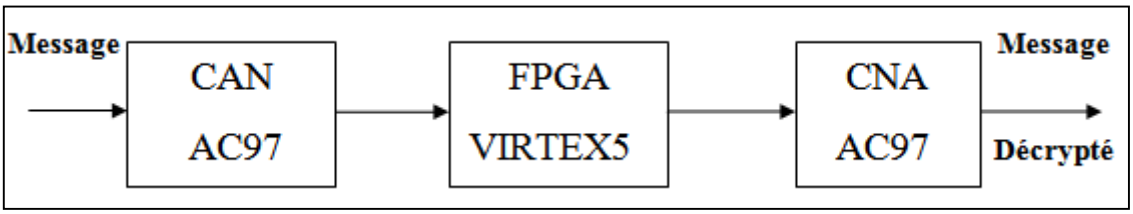


Figure 4.6. Schéma synoptique de l'implémentation de transmission chaotique.

La figure (4.7) représente l'environnement de la partie expérimentale où on peut distinguer d'une part la carte VIRTEX5 intégrant le codec (AC97) et d'autre part les oscilloscopes numérique et analogique pour la visualisation des différents signaux :

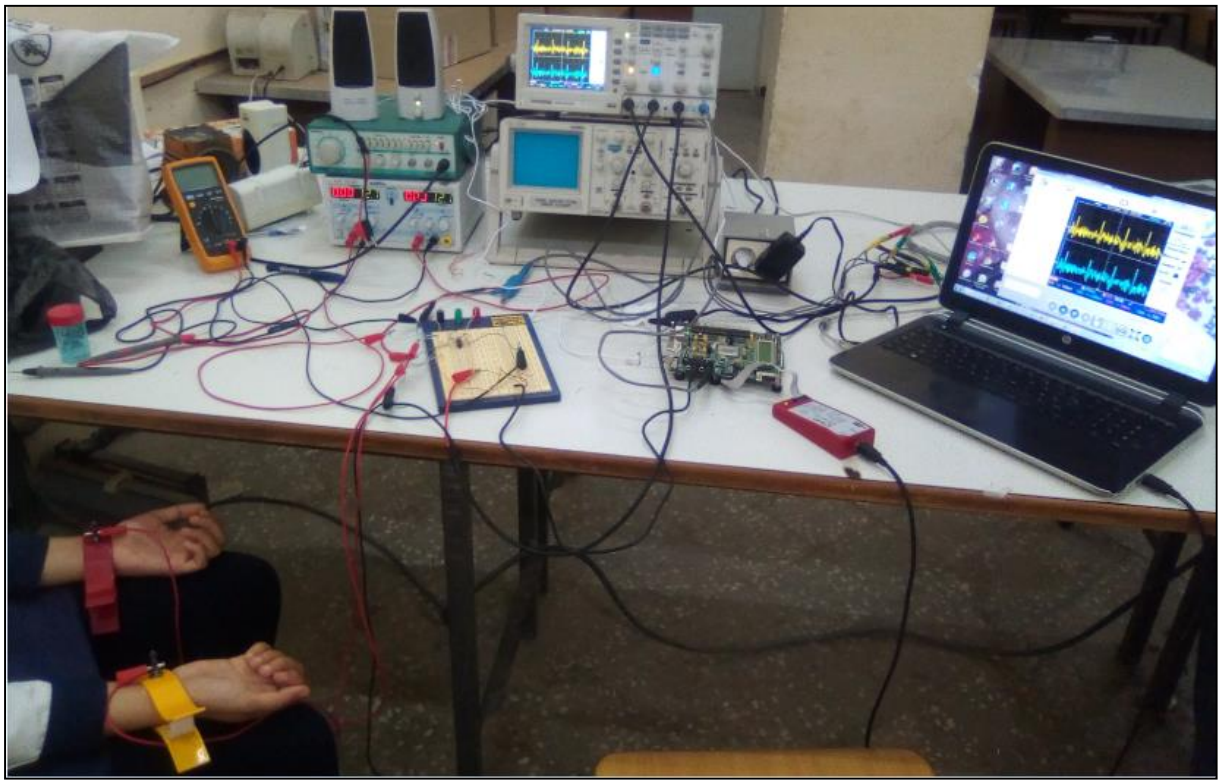


Figure 4.7. Réalisation expérimentale de l'implémentation sur FPGA.

4.3.1 Plate-forme de développement VIRTEX 5 (ML501):

La carte ML501 -VIRTEX5 est la plate-forme de conception et de mise en œuvre des circuits numériques implémentés sur circuit FPGA (xc5vlx50), comme l'illustre la figure (4.8). La famille VIRTEX 5 contient cinq plates-formes distinctes (LX, LXT, SXT, TXT et FXT). Elle possède des ports d'entrées/sorties, des ports de communication (JTAG et USB), un afficheur LCD, des boutons poussoirs….L'implémentation permet de tester et de vérifier le bon fonctionnement du circuit ou bien de détecter le disfonctionnement et les bugs.

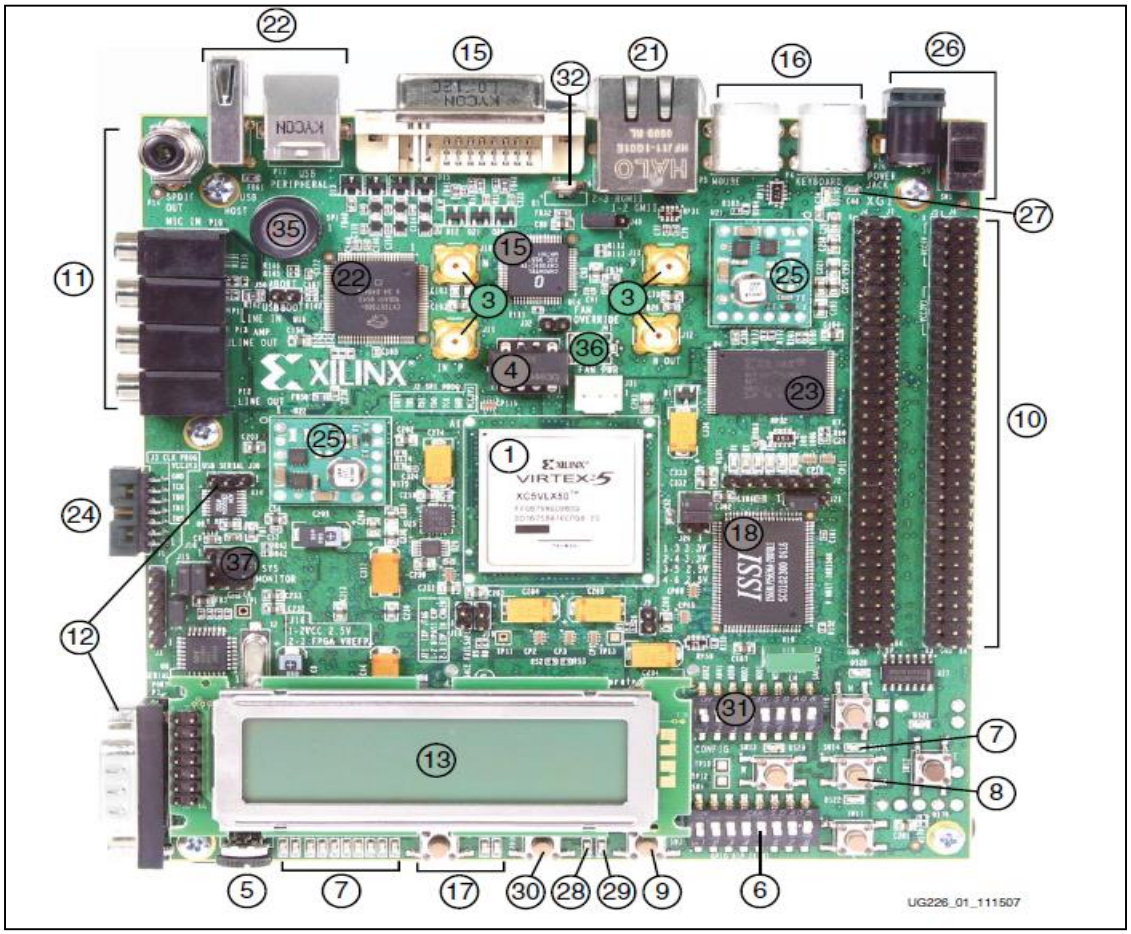


Figure 4.8. Plate forme VIRTEX 5 [31].

4.3.2 CODEC audio AC97 :

La carte de conversion analogique-numérique permet une conversion analogique-numérique du signal ECG que l'on va crypter à travers la transmission chaotique. Elle est basée sur le convertisseur AC97 codé sur 18 bits [32].

Ainsi , ce dernier est aussi utilisée comme une carte de conversion numérique-analogique qui assure la conversion numérique-analogique du signal décrypté (ECG) pour pouvoir le visualiser sur un oscilloscope numérique.

La figure (4.9) présente les branchements de codec AC97 :

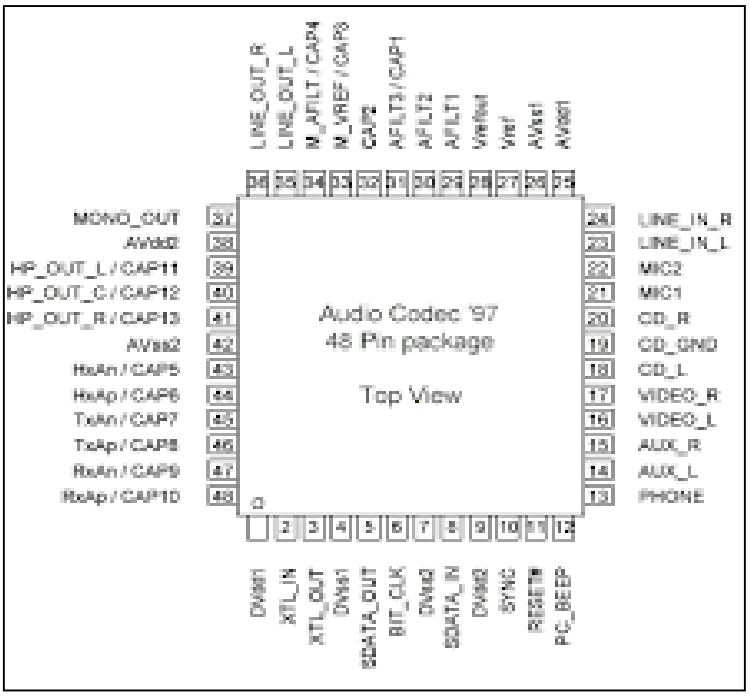


Figure 4.9. Branchement du codec AC 97.

4.4 Implémentation de l'oscillateur de Colpitts sur FPGA :

Le système chaotique normalisé de Colpitts étudié dans le deuxième chapitre est donné par le système d'équation (2.33) :

$$\begin{cases} \dot{x} = y - a\,F(z) \\ \dot{y} = c - x - by - z \\ \dot{z} = y - d \end{cases}$$

Où $F(z)$ est la fonction non linéaire.

Afin d'implémenter cette fonction non linéaire, on a utilisé l'approximation de l'exponentielle par le modèle linéaire par morceau [33]. Cette approche met en évidence les deux régimes de fonctionnement de l'élément non linéaire du transistor de l'oscillateur de Colpitts.

$$F(z) = \begin{cases} -(z+1) & , \quad z < -1 \quad (régime\ actif) \\ 0 & , \quad z \geq -1 \quad (régime\ bloqué) \end{cases}$$

La fonction « integrator » n'est pas disponible dans les bibliothèques du System Generator .Pour cela, on l'a synthétisée à l'aide des blocs de bases disponibles (figure 4.10).

Ainsi, certaines fonctions écrites sous Matlab peuvent être intégrées sous System Generator grâce au bloc MCode block.

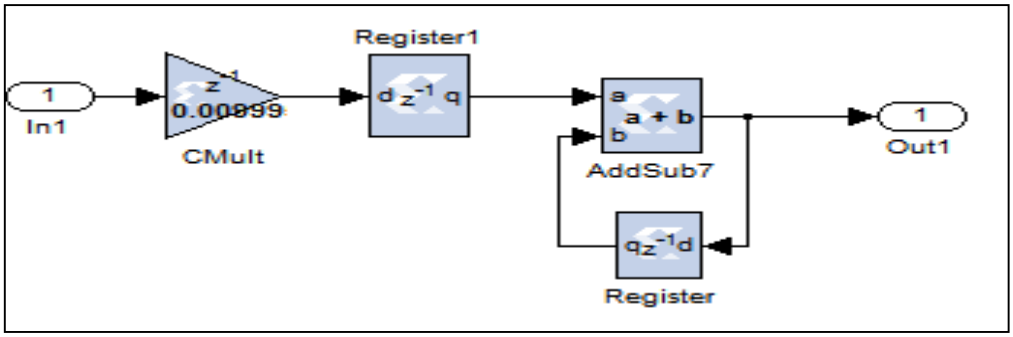


Figure 4.10. Bloc intégrateur [13].

La figure (4.11) représente l'implémentation de l'oscillateur de Colpitts sous System Generator, utilisé comme générateur de signaux chaotiques qu'on a additionné avec le signal utile (message) afin de crypter ce dernier.

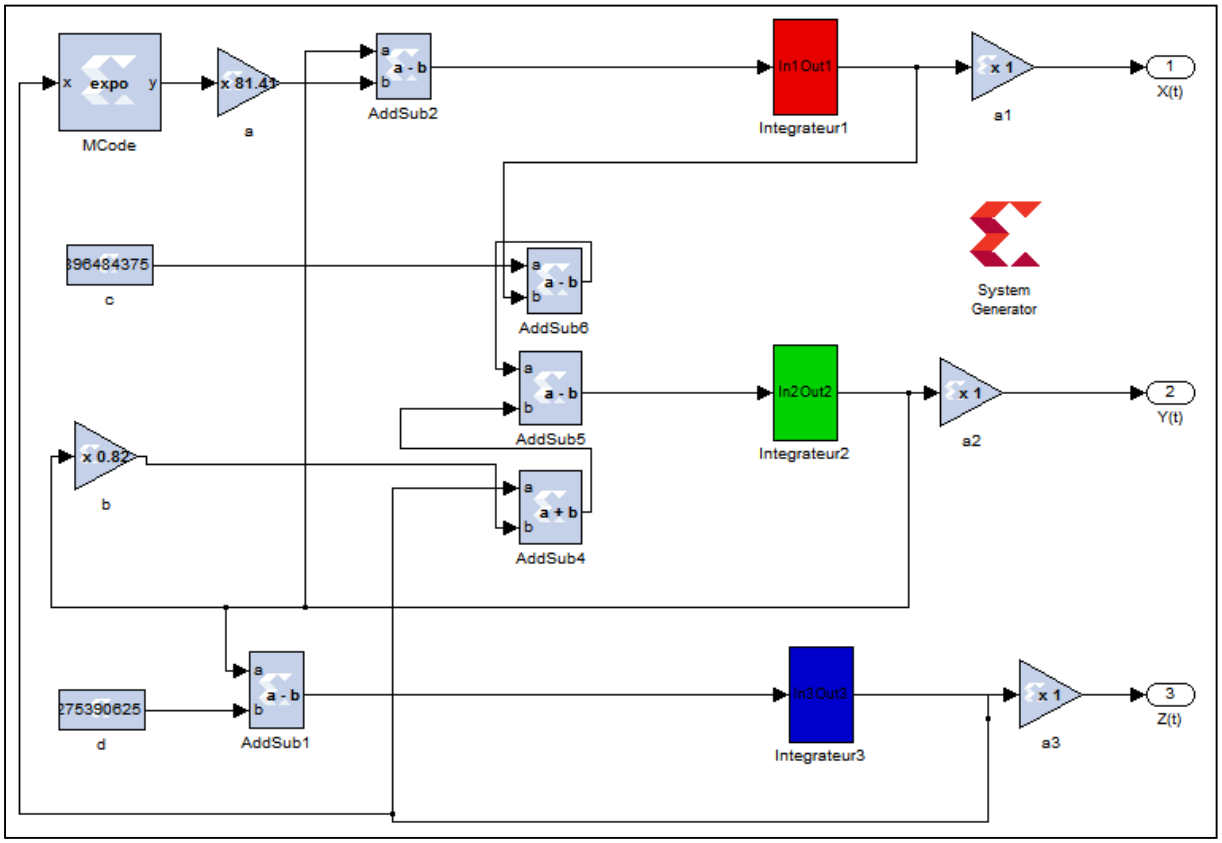
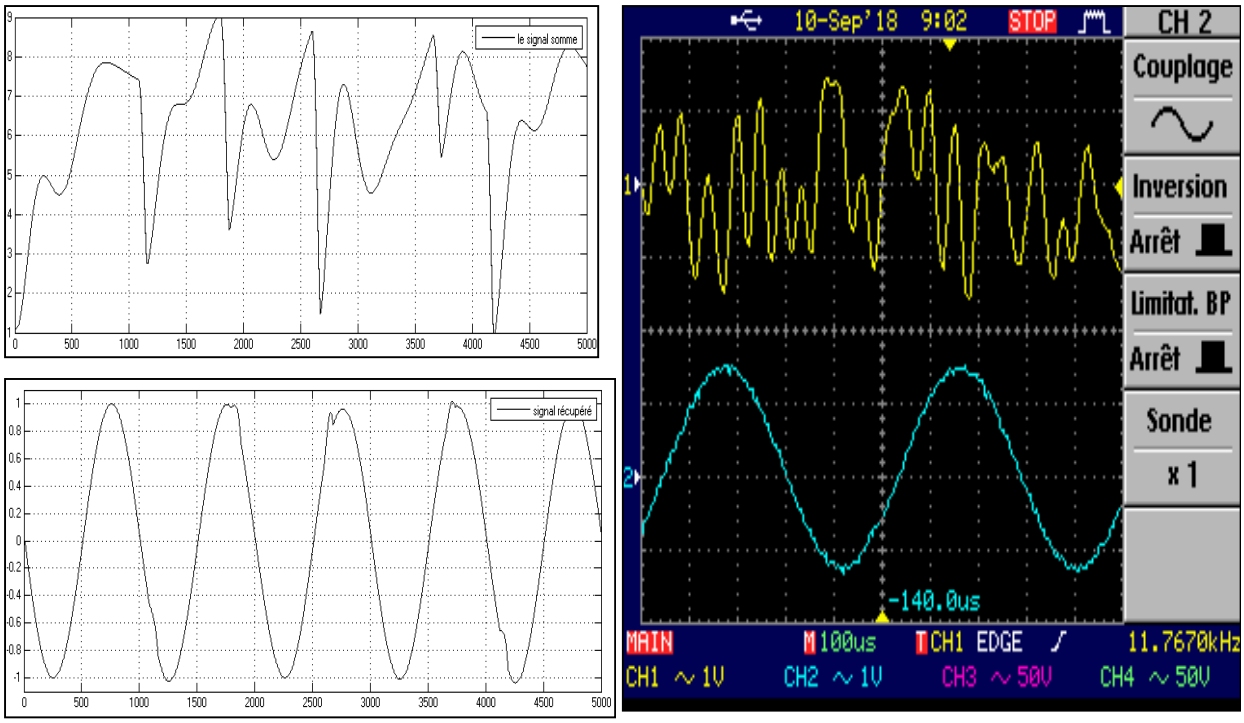


Figure 4.11. Implémentation de l'oscillateur de Colpitts sous System Generator.

Les signaux simulés sous System Generator sont affichés sur un oscilloscope numérique grâce au convertisseur numérique-analogique, et sont représentés sur la figure (4.13). On remarque que l'insertion du message n'a pas modifié le comportement du système chaotique validant ainsi le bon fonctionnement de l'émetteur chaotique.



(a) (b)

Figure 4.12. Les signaux crypté et décrypté : (a) simulés (b) expérimentaux.

Le plan de phase (Z ,Y) est représenté par la figure (4.13) ; on remarque que les résultats simulés et expérimentaux présentent une bonne concordance.

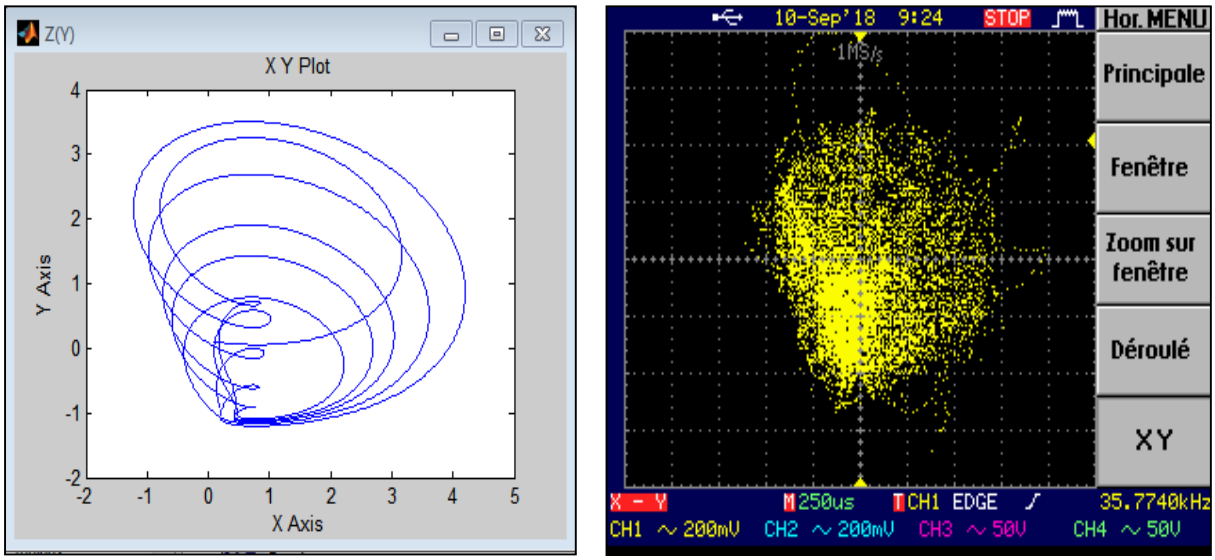


Figure 4.13. Plan de phase Z(Y).

4.5 Implémentation de la transmission chaotique sur FPGA :

Le système de transmission chaotique composé d'un émetteur chaotique (l'oscillateur de Colpitts incluant le signal utile) et d'un récepteur qui récupère l'information a été implanté sur la carte FPGA VIRTEX5 associée à une carte de conversion analogique-numérique et numérique-analogique (CODEC AC97). L'implémentation de l'émetteur et de récepteur sur FPGA est représentée sur la figure (4.14):

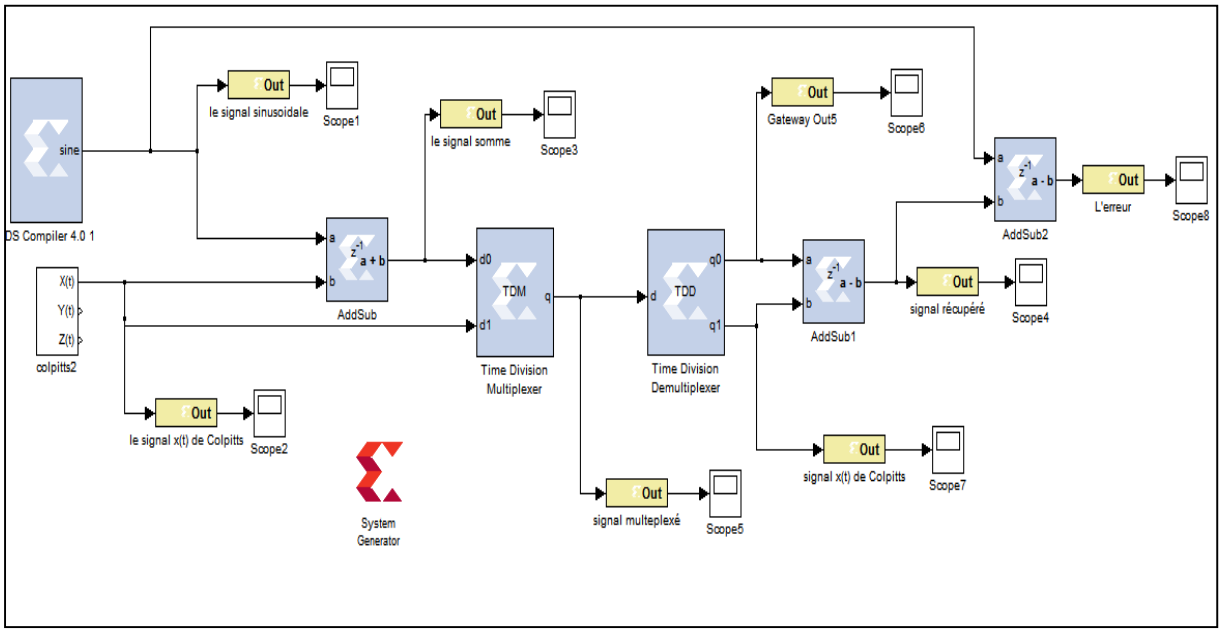
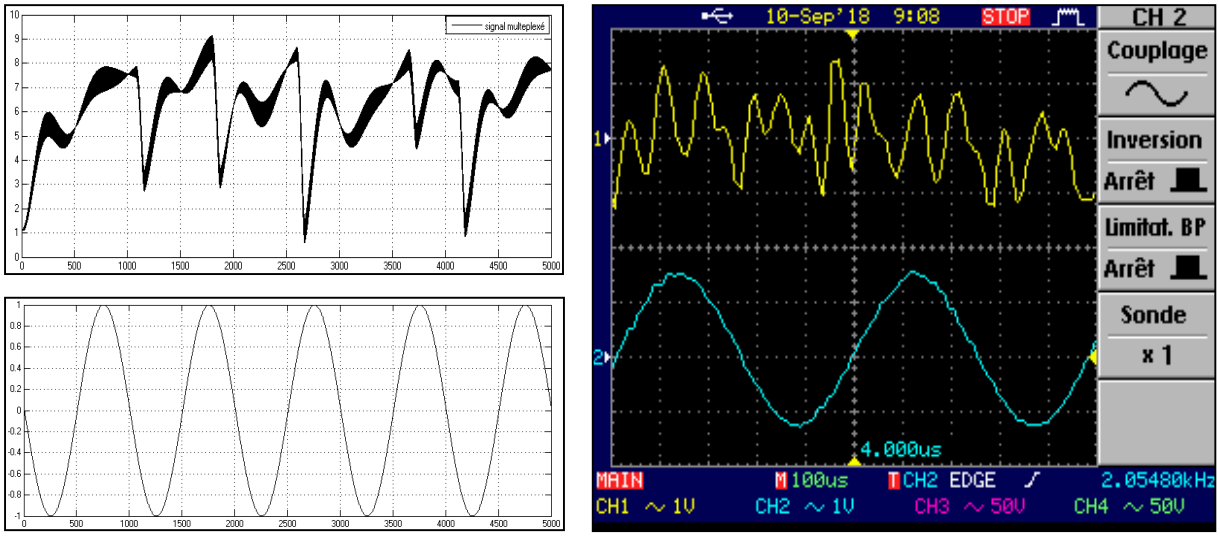


Figure 4.14. Implémentation du système de transmission chaotique.

Les différents oscillogrammes sont représentés sur les figures suivantes qui montrent le bon fonctionnement du schéma de cryptage et du codec, en utilisant le multiplexage et le démultiplexage temporel.

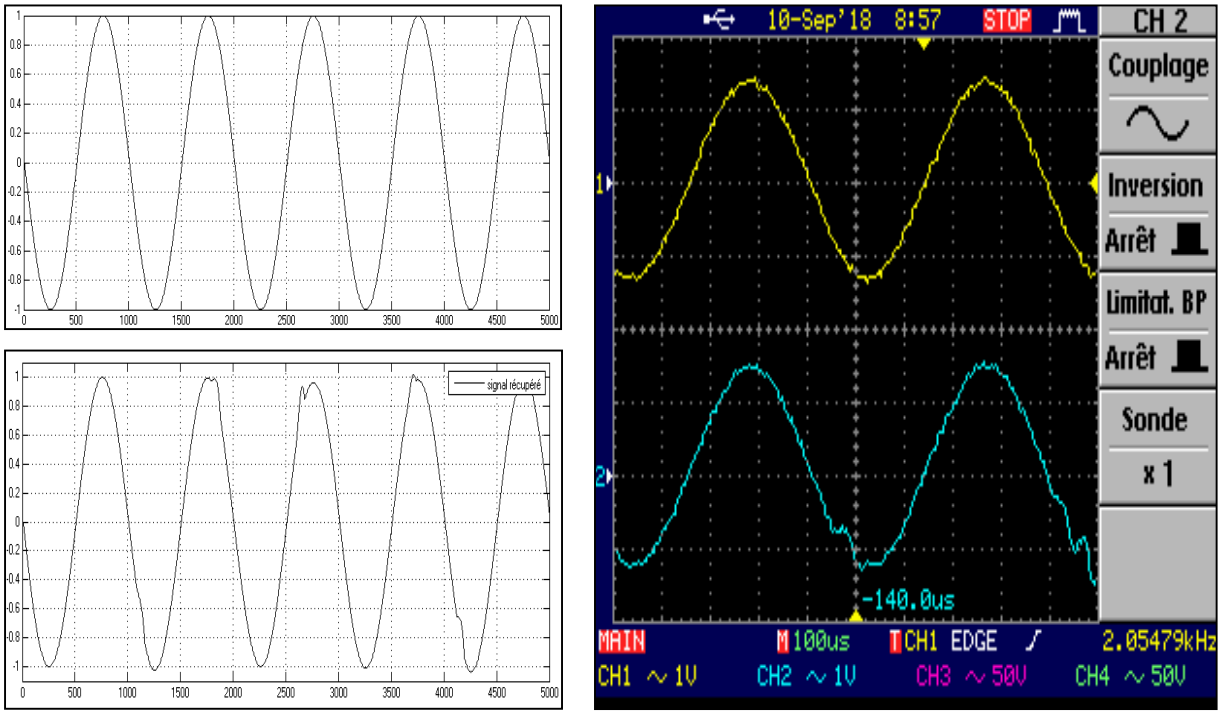
La visualisation des signaux nous permet de :

- ✓ Montrer le bon fonctionnement de la méthode de cryptage par addition (Figure 4.12).
- ✓ Assurer la sécurité du signal crypté au cours du canal de transmission par le multiplexage des signaux (Figure 4.15).
- ✓ Vérifier la synchronisation entre l'émetteur et le récepteur (Figure 4.16).
- ✓ Récupérer le signal message avec un léger chattering (Figure 4.16).



(a) (b)

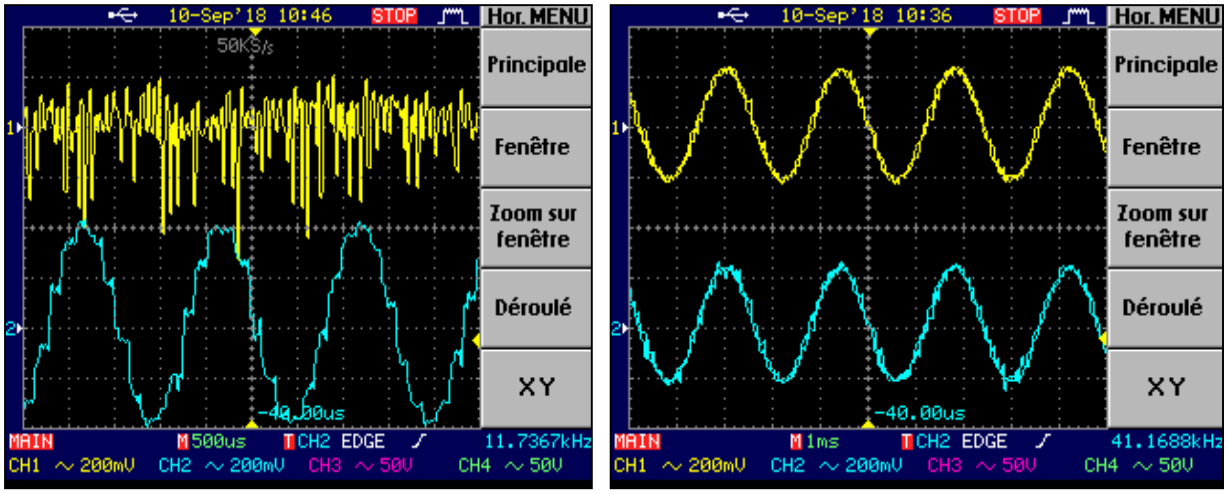
Figure 4.15. Signal multiplexé et décrypté (a) simulés (b) expérimentaux..



(a) (b)

Figure 4.16. Signaux message original et décrypté : (a) simulés (b) expérimentaux.

Pour rapprocher plus de pratique, on a ramené un générateur de tension et on a envoyé le signal de l'extérieur de la carte, on a visualisé les mêmes signaux et sont représentés dans les figures suivantes :



(a) Signal crypté et signal récupéré (b) Signal original et signal récupéré

Figure 4.17. Signaux obtenus dans le cas d'un signal sinusoïdal injecté à l'entrée du codec AC97.

On a réalisé un montage électronique pour générer le signal ECG, en utilisant un amplificateur d'instrumentation à base du circuit TL084A contenant quatre amplificateurs opérationnels dont trois sont utilisés dans notre manipulation.

La visualisation du signal ECG sur l'oscilloscope numérique est représentée par la figure suivante :

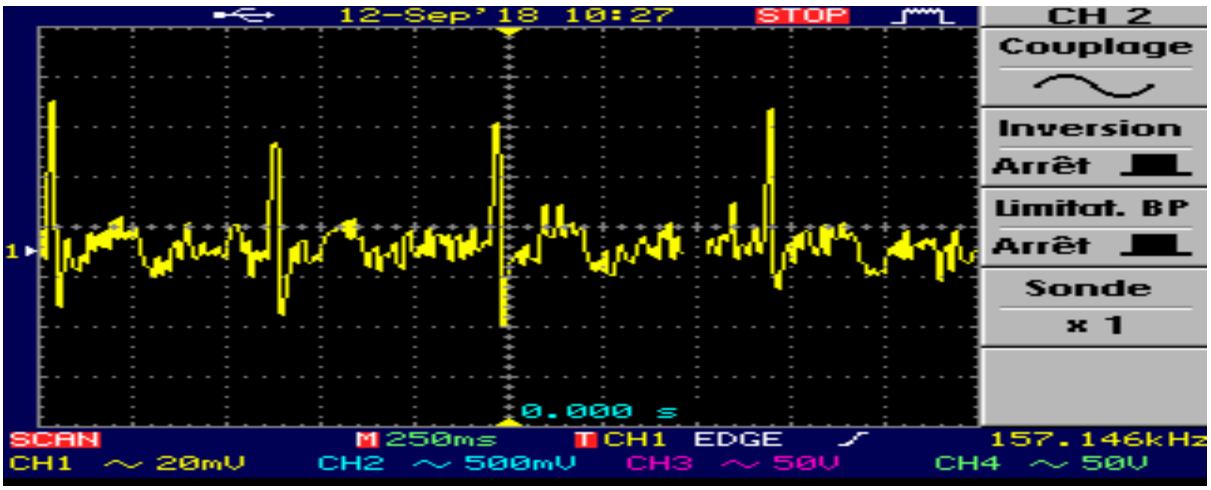


Figure 4.18. Signal d'ECG transmis.

La figure (4.19) montre la récupération du signal ECG après le cryptage chaotique. On remarque que le signal a bien été récupéré montrant ainsi le bon fonctionnement du schéma de cryptage et de décryptage ainsi du codec audio AC97 :

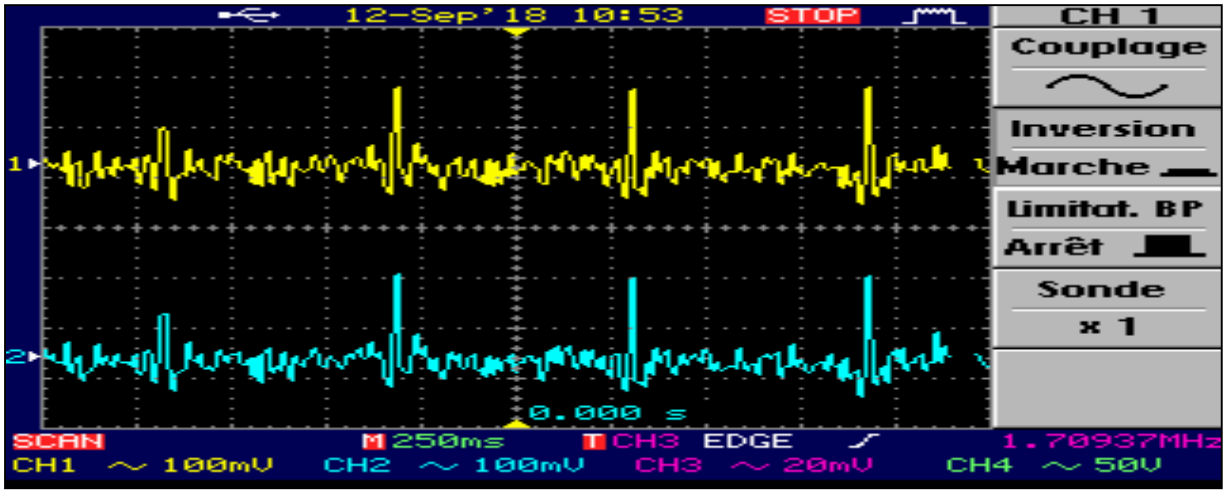


Figure 4.19. Signal ECG transmis et décrypté.

Un rapport d'implémentation est donné par l'environnement ISE sous forme d'un tableau contenant toutes les informations utiles liées au design. La (figure 4.18) montre toutes les ressources internes utilisées en nombre et en pourcentage .

mat123_cw Project Status			
Project File:	cryptage.xise	**Parser Errors:**	No Errors
Module Name:	mat123_cw	**Implementation State:**	Programming File Generated
Target Device:	xc5vlx50-1ff676	• **Errors:**	No Errors
Product Version:	ISE 14.2	• **Warnings:**	819 Warnings (818 new)
Design Goal:	Balanced	• **Routing Results:**	All Signals Completely Routed
Design Strategy:	Xilinx Default (unlocked)	• **Timing Constraints:**	All Constraints Met
Environment:	System Settings	• **Final Timing Score:**	0 (Timing Report)

Device Utilization Summary				[-]
Slice Logic Utilization	**Used**	**Available**	**Utilization**	**Note(s)**
Number of Slice Registers	713	28,800	2%	
Number used as Flip Flops	703			
Number used as Latch-thrus	10			
Number of Slice LUTs	1,332	28,800	4%	
Number used as logic	1,292	28,800	4%	
Number using O6 output only	1,107			
Number using O5 output only	129			
Number using O5 and O6	56			
Number used as exclusive route-thru	40			
Number of route-thrus	195			
Number using O6 output only	157			
Number using O5 output only	26			
Number using O5 and O6	12			
Number of occupied Slices	501	7,200	6%	
Number of LUT Flip Flop pairs used	1,614			
Number with an unused Flip Flop	901	1,614	55%	

Design Summary

Figure4.20. Ressources internes de l'implémentation.

Le routage et l'emplacement sur la carte VIRTEX5 sont donnés par la figure (4.19) :

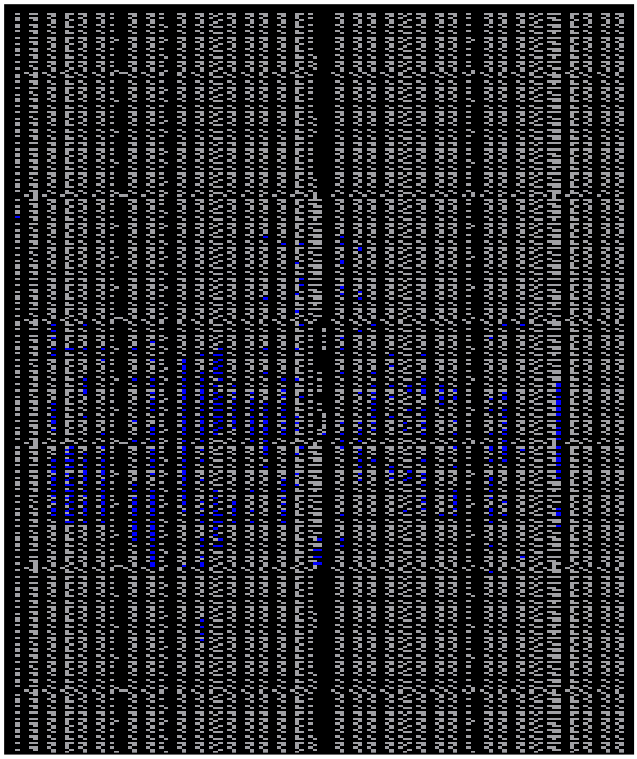


Figure 4.21. Circuit implémenté sur le FPGA VIRTEX5.

Ce chapitre a été consacré à l'implantation d'une transmission chaotique sécurisée sur une cible FPGA. L'émetteur chaotique constitué de l'oscillateur Colpitts et du signal utile (ECG) à crypter a été implémenté sur la carte FPGA VIRTEX 5. Les signaux obtenus par simulation et les signaux relevés de la carte ont été observés. En utilisant le multiplexage et le démultiplexage temporel, l'émetteur envoie le message crypté et le récepteur récupère ce dernier en minimisant la complexité du montage. L'implémentation du récepteur permet la récupération du signal crypté avec un chattering qui peut être minimisé par un filtrage adéquat. Nous avons par la suite, effectué une estimation des ressources utilisées par les différentes implémentations.

Conclusion générale

Dans ce mémoire, on a étudié et réalisé une implémentation sur FPGA d'un système de transmission sécurisée par chaos d'un signal ECG en utilisant le multiplexage et le démultiplexage temporel pour la récupération du signal utile (ECG).

On a consacré le premier chapitre à la présentation des généralités sur le système cardiovasculaire ainsi que l'électrocardiogramme en décrivant ses principales propriétés telles que l'étude fréquentielle. Dans le deuxième chapitre, la description détaillée des systèmes dynamiques chaotiques est présentée. Leurs caractéristiques ont été décrites en mettant en évidence l'intérêt du calcul des exposants de Lyapounov et les différents scénarios possibles de transition vers le chaos.

Ensuite, on a expliqué le principe de fonctionnement de l'oscillateur de Colpitts qui est utilisé comme générateur du signal chaotique appliqué au signal ECG pour son cryptage.

Ces études ont été mises en évidence à l'aide de simulations, en ajustant les différents paramètres de l'oscillateur de Colpitts pour obtenir un comportement chaotique.

Le troisième chapitre a été consacré à citer les différentes méthodes de cryptage chaotique telles que la méthode de cryptage par addition qu'on a utilisé dans notre projet. On a ainsi a montré que les systèmes de communication chaotiques sont basés sur la synchronisation entre l'émetteur et le récepteur. L'objectif du multiplexage et de démultiplexage temporel est de simplifier les méthodes de synchronisation du système chaotique au niveau d'émetteur et de récepteur apportant ainsi une souplesse dans le montage. Dans le dernier chapitre, une implémentation de la transmission chaotique a été réalisée sur circuit FPGA. Les différents signaux obtenus au niveau du récepteur ont été visualisés sur un oscilloscope numérique.

Le principe de notre travail a été l'implémentation d'une transmission sécurisée par chaos sur une cible FPGA et la récupération du message crypté au niveau du récepteur grâce au multiplexage et au démultiplexage temporel.

On a montré par simulation et par réalisation expérimentale, l'effet du multiplexage temporel pour transmettre le message utile et du démultiplexage temporel pour le récupérer. Nous avons par la suite validé le bon fonctionnement du codec audio AC97 (CAN et CNA) par la visualisation des différents signaux et leur comparaison avec ceux obtenus par simulation.

Après la réalisation de ce travail, on a remarqué que l'inconvénient majeur de la méthode de multiplexage temporel dans la transmission est la nécessité d'une horloge commune à tous les utilisateurs qui peut poser des problèmes de synchronisation.

Comme perspectives, nous envisageons d’associer au TDM une FDM (Frequency Division Multiplexing) c'est-à-dire un multiplexage fréquentiel associé au multiplexage temporel. Aussi, à la sortie de la carte FPGA, il faut ajouter un filtre audio passe bande pour éviter le bruit associé au signal informatif.

Références

01. Ben Safia. K, « Télésurveillance : transmission sans fil, par voie GSM, et traitement du signal électrocardiographie (ECG) ». Thèse de magister de l'université de Tizi-Ouzou.

02. Cours anatomie et physiologie, Dr Slimani, 2017.

03. Dassier.P, « ECG NORMAL ». HEGP2006.

04. Juan Sztajazel,« Introduction à l'électrocardigramme », service de cardiologie Hôpitaux universitaires Genève.

05. Malti A. et LANTRI H., «Transfert du signal ECG sur mobile pour la télésurveillance médicale ». Thèse de master de l'Université Abou Bakr Belkaïd de Tlemcen, 2013.

06. laid.Z et Daraoui.A. « FILTRAGE ADAPTATIF DU SIGNAL ELECTROCARDIOGRAMME (ECG**) ».** Thèse de master de l' Université Abou Bakr Belkaïd de Tlemcen,2014.

07. Kligfield et al AHA Recommendations for the standardization ECG... Circ, 2007.

08. Garcia-Nebla.J et al. « Technical mistakes during the acquisition of the electrocardiogram ». Ann Noninvasive Electrocardiol, 2009.

09. Buendía-Fuentes F, et al. « High-Bandpass Filters in Electrocardiography: Source of Error in the Interpretation of the ST Segment ». ISRN Cardiol, 2012.

10. BTS,« Aquisition et traitement d'un électrocardiogramme », SYSTEMES ELECTRONIQUES EPREUVE U4.2-PHYSIQUE APPLIQUEE-2009.

11. Jérôme Dequeker - Paul-Henri Michel , « Mouvements chaotiques, étude du pendule double »

12. Huyen Dang V. et Claudine D., «Bifurcation et Chaos : Une introduction à la dynamique contemporaine», Ellipses, 2000.

13. Chikhi L., « Application des systèmes dynamiques chaotiques en transmission de données ». Thèse de magister de l'université de Blida 1, 2012.

14. Talbi I., « Systèmes dynamique non linaires et phénomène du chaos ». Thèse de magister en mathématique, Université Mantouri de Constantine, 2010.

15. ODEN J., « Le chaos dans les systèmes dynamiques »,2007.

16. Manneville P. « Dynamique non linéaire et Chaos », Laboratoire d'Hydrodynamique, Ecole polytechnique, Séminaire E2PHY, 2005.

17. Morel C., « Analyse et contrôle de dynamiques chaotiques, application à des circuits électroniques non linéaire », Thèse de Doctorat en automatique et informatique appliquée,2005.

18. L'Hernault, M., « Faisabilité d'un système d'émission-réception analogique pour les communications sécurisées par le chaos », Thèse de doctorat de l'université de Paris 6, 2007.
19. Guo-Hui Li, « CHAOS AND SYNCHRONIZATION OF COLPITTS OSCILLATORS ». Départment of Communication Engineering. Shanghai University,2003.
20. Gian Mario Maggio, *Student Member, IEEE*, Oscar De Feo, and Michael Peter Kennedy «Nonlinear Analysis of the Colpitts Oscillator and Applications to Design », *Fellow, IEEE.*
21. A. Baziliauskas, A. Tamaševičius, S. Bumelienė, and E.Lindberg. «Synchronization of Chaotic Colpitts Oscillators ».
22. Nijmeijer, H. and Van Der Schaft, A. J., "Nonlinear dynamical control systems",Springer, 1990.
23. Magherbi Ouerdia. « Etude et realisation d'un système sécurisé à base de systèmes chaotiques ». Mémoire de Magister, spécialité Automatique, Université MOULOUD Maammeri Tizi Ouzou.2013.
24. Pecora, L. M. and Caroll, T. L., "Synchronization in chaotic systems", Phys. Rev.Lett. 64, p. 821–824, 1990.
25. Kocarev, L., Shang, A. and Chua, L. O., "Transitions in dynamical regimes by driving : a unified method of control and synchronization of chaos", Chaos, Solitons and Fractales 24, p. 1025–1030, 2005.
26. Rubezic, V., Lutovac, B. and Ostojic, A., "Linear Generalized Synchronization of Two Chaotic Colpitts Oscillators", in Proceedings of ICECS, p. 223–225, 2001.
27. Mme Cherfa. A, Cours " Développement des FPGA", Université de Blida 1.2018
28. Pedroni V. A. , " Circuit dessign with VHDL", MIT Press, 2004.
29. Chu P. P. "FPGA Prototyping by verilog examples", Wiley, 2008.
30. Fabrice Aubépart. « Outil System Generator ».Département Geii – Marseille ,Colloque Geii Marseille,2007.
31. ML501 Evaluation,Platform*User Guide* UG226 (v1.4) August 24, 2009.
32. JOSÉ ROBERTO,"Implementing an AC97Audio Controller IP", Master of Science Thesis in Integrated Electronic System Design , University of Gothenburg ,2011.
33. A. BAZILIAUSKAS1,∗, R. KRIVICKAS1, and A. TAMAS˘EVIC˘ IUS2,"Coupled Chaotic Colpitts Oscillators:Identical and Mismatched Cases".Department of Signal Processing, 2005.