الجمهورية الجزائرية الديمقراطية الشعبية
République algérienne démocratique et populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique
المركز الجامعي لعين تموشنت
Centre Universitaire Belhadj Bouchaib d'Ain-Temouchent
Institut des Sciences et de la Technologie
Département de Génie Electrique

Projet de fin d'études
Pour l'obtention du diplôme de Master en :
Domaine : SCIENCE ET TECHNOLOGIE
Filière : Electronique
Spécialité : génie des télécommunications
Thème

Application des registres LFSR dans les systèmes de communication mobiles.

Présenté Par :
1) Bahi walid
2) Hanafi abd el nadir

Devant les jurys composés de :

Dr.Ayache Choukria (née Sayah)	MCA	C.U.B.B (Ain Temouchent)	Président
Mr.Benazza Baghdadi	MAA	C.U.B.B (Ain Temouchent)	Encadreur
Mr.Krim Mohammed	MAA	C.U.B.B (Ain Temouchent)	Co-Encadreur
Melle.boutkhil Malika	MCA	C.U.B.B (Ain Temouchent)	Examinateur

Année universitaire 2014/2015

REMERCIEMENTS

Tout d'abord, nous aimerons remercier le Seigneur de nous avoir toujours donné la force de mener à bien la réalisation de ce travail de mémoire de fin d'études.

Nous remercions Monsieur Benazza Baghdadi, Enseignant et Chef du Département génie électrique.

Nous tenons à exprimer notre profonde et très sincère reconnaissance à Monsieur Krim Mohammed pour nous avoir encadré et qui n'a cessé de nous prodiguer de précieux conseils, nous le remercions pour la confiance qu'il nous a témoigné et pour nous avoir fait bénéficier de ses compétences et de ses conseils.

Nous tenons aussi à remercier Docteur Ayache Choukria (née Sayah), Enseignant au sein du Département Génie électrique, qui nous a fait l'honneur de présider les membres du Jury de ce mémoire.

Nous exprimons également toute notre gratitude à Melle Boutkhil Malika, Enseignant au sein du Département génie électrique, pour nous avoir guidées dans les grandes lignes du travail accompli et d'avoir acceptés d'être parmi les membres du jury.

Nous remercions également tous les Enseignants du centre universitaire Belhadj Bouchaib, qui nous ont formés durant ces cinq années d'études.

Nous exprimons notre très grande gratitude à nos familles, en particulier nos mères et nos pères pour nous avoir soutenus tout au long de nos études. Nous reconnaissons les sacrifices que ces longues années ont représentés et nous les remercions d'avoir appuyé nos choix et d'avoir toujours su nous encourager.

Et pour toute personne qui nous a aidé de près ou de loin à l'élaboration de ce mémoire, nous vous somme très reconnaissant et que la grâce de Dieu vous inonde.

Résumé :

Code Division Multiple Access (CDMA) est dominant technique d'interface radio utilisé pour des communications sans fil pour "3G" et des systèmes "4G". Multi-porteuse "CDMA" est devenu le centre des intérêts de recherche actuels en matière de communication numérique sans fil. Multi support "CDMA", Orthogonal Frequency Division Multiplexing (OFDM) techniques utilisées pour la production des systèmes de réseau sans fil $3^{ème}$ et $4^{ème}$ génération permettre la transmission à haut débit de données. Rapides variations temporelles du canal sans fil ont un effet sur la performance des systèmes "CDMA". L'objectif du mémoire est de fournir une étude sur les techniques de transmission "CDMA" pour 3G et 4G systèmes et analyse des performances des multi-porteuse "CDMA" modèle de système pour différentes séquences d'étalement comme codes PN et Gold code mises en œuvre sur Rayleigh canal et additif canal White Noise gaussien (AWGN) en utilisant MATLAB.

Mots clés: CDMA, OFDM, LFSR, DSSS, ES, GOLD, PN séquence, AWNG, Rayleigh,

ملخص:

تقنية (CDMA) هي التكنولوجيا السائدة الاستخدام في الاتصالات اللاسلكية بالنسبة للأنظمة الخاصة بالجيل الثالث "3G" والرابع "4G". أصبحت "CDMA" محور الاهتمامات البحثية الحالية في مجال الاتصالات الرقمية اللاسلكية.

استخدام تقنيات "CDMA" والتردد المتعامد بالتقسيم (OFDM) تمكن من إنتاج أنظمة للشبكات اللاسلكية للجيل الثالث والرابع ذات سرعة عالية لإرسال البيانات. الاختلافات السريعة في الوقت للقناة اللاسلكية لها تأثير على أداء نظام "CDMA". والهدف من هذه المذكرة هو تقديم دراسة حول تقنية "CDMA" في نظام الجيل الثالث G3 و G4 وتحليل أداء "multicarrier CDMA" نموذج النظام إلى سلاسل مختلفة كرموز نشر PN-séquence وGold Code وتنفيذها على قناة Rayleigh وقناة AWNG باستخدام MATLAB.

Table Des Matières :

Liste des Figures :

Liste des tableaux :

I. Introduction générale :

La dernière décennie a vu de nombreuses avancées dans la théorie de la communication sans fil de la couche physique et de leur mise en œuvre dans les systèmes sans fil. « Les téléphones mobiles de première génération étaient basées dans la technologie analogique à modulation de fréquence. Ce système prend en charge que les données vocales. La technologie de deuxième génération est numérique et capable de recevoir des données en plus de la voix. Le mobile 3G est basé sur Code Division Multiple Access charge les communications vocales et le service de données des services de haute qualité et multimédia avec une plus grande capacité. 4G est basé sur Orthogonal Fréquence Division Modulation (OFDM) utilisé pour Digital Audio Broad casting (DAB) et Digital Vidéo Broad casting (DVB) "de IEEE 802.11a et IEEE 802.11g. 2.5G, 3G, 4G comparaison avec égards à différents paramètres son existence, ses développements, applications de la zone de couverture des capacités sont pris en compte dans Code Division Tableau I. Multiple Access (CDMA) est une technologie à étalement de spectre qui, avec le concept de récepteur en râteau permet de minimiser les erreurs de communication résultant des effets multiples. « La technologie à étalement de spectre a pour but de propager le signal d'information sur une large bande passante et à rendre brouillage interception plus difficile.

CDMA 2000 est un système sans fil qui fait partie de la spécification IMT-2000 et est une extension de la CDMA une des plates-formes sans fil utilisant les normes est-95A / B et JST-A-008. CDMA 2000 a été déployée dans le IS-95 système existant et exposera de nombreuses améliorations. Il permet à plusieurs utilisateurs de partager le même spectre, différents types de main-offs fournis« En raison de son récepteur de BW et le râteau de large, CDMA utilise les signaux à trajets multiples et les combine pour faire un signal plus fort au niveau du récepteur qui fournit une plus grande efficacité et d'immunité aux trajets multiples BW .

Wide-band Code Division Multiple Access (de WCDMA) a attiré le plus d'attention dans le développement de systèmes sans fil de troisième génération (International Mobile Télécommunications IMT-2000) en l'an 2000. Applications WCDMA incluent la messagerie, voix, web la navigation, la vidéoconférence, la surveillance vidéo, l'audio de haute qualité, et l'accès de base de données. Cependant, la performance de large bande CDMA est limitée par les interférences d'accès multiple (MAI) et l'interférence inter symbole (ISI) en présence de trajets multiples scénario décoloration qui se traduit par un évanouissement sélectif en fréquence possible. Pour lutter contre le problème de la propagation par trajets multiples et la fréquence de canal sélective pour les techniques de support ou de transmission multi porteuse

simples, une technique multi porteuse (MC) de transmission qui est également connu comme Orthogonal Fréquence Division Multiple Access (OFDMA) a été examiné. [4] "OFDM" a été introduite dans 60 la fin des années sur la base de techniques de modulation multi porteuse utilisés dans la haute fréquence de radio militaire en 1971.Einstein introduit l'idée d'utiliser une transformée de Fourier discrète (DFT) pour la mise en œuvre de la génération et la réception de signaux OFDM, l'élimination de la nécessité pour les banques d'oscillateurs de sous-porteuse analogique.

L'OFDM élimine Inter Symbole interférences (ISI), interférence Inter Carrier (ICI) par l'utilisation de préfixe cyclique. Les avantages d'OFDM sont la résistance à l'évanouissement par trajets multiples, des interférences de canal transversal réduit, la réduction de la quantité d'augmentation du spectre de fréquences dans la capacité du système, l'utilisation efficace de la bande passante et au-dessus de toutes les sous-porteuses orthogonales peuvent parfaitement se chevaucher. Toutefois, OFDM est plus sensible au décalage de fréquence et de bruit de phase. OFDM a relativement grand rapport pic de puissance moyenne (PAPR), qui tend à réduire l'efficacité de la puissance de l'amplificateur RF. Mais il n'est pas idéal pour les communications mobiles.

Tableau 1. Sommaire de Mobile Génération

	2.5G	**3G**	**4G**
Type of transmission	**Digital Packet switching**	**Digital Packet switching**	**Digital Packet switching**
Year of évolutions	**1993-1998**	**1996-2005**	**2006**
Multiple Access multiple	**CDMA**	**CDMA & OFDM**	**FHMA & OFDM & MC-CDMA**
Channel BW	**1.25 MHZ**	**3 X 1.25MHZ**	**40MHZ**
Modulation	**BPSK**	**BPSK, QPSK, OFDM**	**BPSK, QPSK, 16&64 QAM,OFDM**
Supports number of users	**20 users**	**40 users**	**High spectral efficiency, higher data rates, multiple service, 100modes/users.**

Data rates	**115.2 kbps**	**144 kbps for high mobility Outdoor-384 kbps Indoor-2 kbps**	**1 – 100 Mbps for high mobility and 2Gbps for low mobility**
Application	**Voice, data**	**Voice, data, vidéos, Internet, multimédia**	**IP telephony Ultra broadband internet access, HDTV**
Security and efficiency	**More Secure**	**Higher**	**higher**
Network standards	**CDMA-one IS-95**	**WCDMA-2000, WCDMA**	**WIFI, WLAN, WIMAX**
Coverage area	**Global**	**Global**	**Metropolitan area**
Capacity	**Higher than 2G**	**Higher than 2.5G**	**Higher than 3G**

Au cours des dernières années, MC-CDMA a reçu des intérêts largement répandus pour les futures communications sans fil en combinant modulation OFDM et CDMA . un nouveau régime est développé qui récolte les avantages des deux techniques tels que l'efficacité spectrale élevée, la capacité d'accès multiple, la robustesse en cas de canaux sélectifs en fréquence.

Cependant, le signal OFDM a le grand pic de rapport de puissance moyenne (PAPR) qui limite sévèrement son application, aussi longtemps que le fonctionnement de base du MC-CDMA est identique au système de OFDM. Au cours des dernières années, il y a eu des efforts considérables dans les activités de recherche liés à la diffusion des techniques de spectre, CDMA, DS-CDMA, OFDM, MC-CDMA techniques de transmission qui ont été éprouvées pour augmenter les débits d'application de communications sans fil. MC-CDMA et OFDM émergent des technologies clés pour les systèmes sans fil 3G et 4G. La demande croissante pour les services multimédias nécessite des débits de données élevés pour la transmission, mais cette condition est considérablement limitée par Inter Symbole interférences (ISI) en raison de l'existence de trajets multiples. La combinaison de modulation multi porteuse (OFDM) et les techniques CDMA est utilisé pour lutter contre ce problème. La recherche dans ce domaine en pleine expansion du domaine des communications sans fil s'effectue à partir des deux dernières décennies.

II. Chaine de transmission

1. L'information :

L'information est au cœur de nos sociétés modernes : presse, téléphonie, données météorologiques, Internet… De nombreux vecteurs concourent à nous transmettre les messages porteurs de ces informations. Les machines associées à des outils informatiques sont elles aussi soumises à un flux de données provenant de capteurs susceptibles d'améliorer leur performance et leur sécurité. Les flux d'information sont ainsi omniprésents dans notre quotidien.

Au-delà du traitement qui est fait de ces informations tant par l'humain que par la machine, il importe avant tout que celle-ci soit communiquée en toute fidélité à son destinataire. En d'autres termes, il faut impérativement que le message reçu soit l'exacte réplique du message émis ! Il ne s'agit pas dans cet article de réécrire la théorie de l'information pour laquelle de nombreux documents sont disponibles sur Internet mais de présenter succinctement les éléments liés à une chaîne de transmission de l'information.

En préalable, il faut avoir présent à l'esprit que l'information est avant tout un événement aléatoire [1].

2. Chaine de transmission :

La chaîne de transmission de l'information, dans sa structure fonctionnelle la plus simple, est constituée :

- D'un émetteur.
- D'un canal de transmission.
- D'un récepteur.

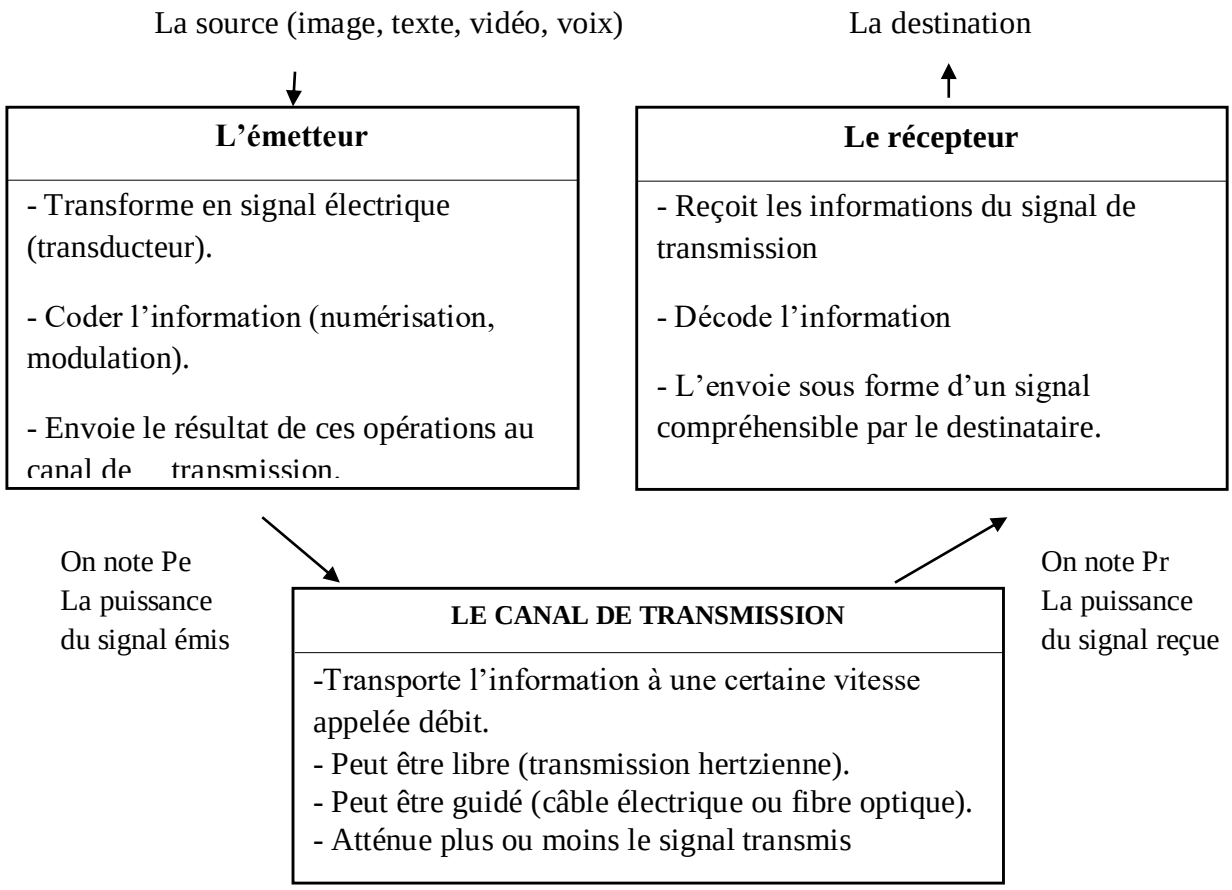


Figure 1. Schéma de principe d'une chaine de transmission [5], [6].

2.1. Transducteur à l'émission :

Le transducteur à l'émission permet de convertir le signal original (voix, image,…) en un signal électrique utile pour l'émetteur. Certains utilisent le terme « encodeur » (codec dans le jargon informatique), cela peut induire une confusion avec le convertisseur utilisé dans le canal de transmission qui réalise la conversion de la nature du signal (pour la voix : de pression en tension avec un microphone).

Son choix doit être compatible avec les caractéristiques (amplitude, spectre) du signal à convertir.

2.2. L'émetteur :

L'émetteur a pour fonction d'adapter le signal issu du transducteur en vue de le transmettre au canal de transmission. Il peut simultanément remplir plusieurs fonctions :

- Coder le signal issu du transducteur (tension) en nombres, dans le cas d'une conversion analogique numérique ou/et de chiffrage ;
- Moduler ;
- Amplifier.

Cet émetteur peut être un émetteur analogique (Exemple : Emetteur Radio FM) ou encore un modem ADSL utilisé pour Internet dans le cadre d'une information numérique.

2.3. Le canal de transmission :

Le canal de transmission permet au récepteur de recevoir l'information émise par l'émetteur. De nombreux supports sont utilisés [10] :

- Les supports avec guide physique (câbles, fibres, ...) ;
- Les supports sans guide physique (ondes radio, ondes lumineuses).
- Ces différents supports sont choisis en prenant en compte :
- Le débit d'information à transmettre ;
- Les caractéristiques du signal (bande passante, codage…) ;
- La distance entre l'émetteur et le récepteur ;
- Les possibilités de mise en œuvre.
- Pour donner une idée de la qualité des supports, disons que :
- Les câbles électriques à paires torsadées sont les moins fiables, suivis par les câbles coaxiaux ;
- Les fibres optiques offrent actuellement le meilleur compromis fiabilité/performance.

2.4. Le récepteur :

Son rôle est à la fois de recevoir le signal émis ainsi que de le rendre compatible avec le transducteur (exemple : haut-parleur) servant à la réception. Les actions réalisées par le récepteur sont alors les suivantes :

- Filtrer le signal reçu (éliminer la partie inutile du signal reçu pour ne garder que l'information) ;
- Décoder :
- Soit en réalisant une conversion numérique analogique ;
- Soit un déchiffrage ;
- Démoduler ;
- Amplifier le signal pour le rendre utilisable par le transducteur de sortie.

Ce récepteur est par exemple un poste de radiophonie pour un signal analogique ou un modem ADSL pour les informations numériques [9].

2.5. Transducteur à la réception :

Son rôle est de fournir une information exploitable par le destinataire sous la forme d'un signal. Il ne faut pas confondre le terme transducteur avec celui de décodeur qui a pour but de déchiffrer un signal crypté en une information « claire »[3][4].

3. Modulation :

Quand est ce qu'on fait la modulation ?

La question de la modulation se pose lorsque :

- L'on veut faire passer plusieurs informations simultanément dans le même canal de transmission.
- L'on veut transmettre l'information à des distances importantes.
- L'on veut diminuer le bruit dont est victime l'information lors de sa transmission.

La modulation consiste alors à adapter l'information à transmettre à un canal de communication mais ce n'est pas une obligation.

Moduler, c'est le moyen de séparer des informations provenant de différentes sources et ayant le même spectre qui utilisent le même support de transmission de façon à permettre à différents émetteurs de retrouver l'information qui les concerne.

Plus précisément, une modulation numérique consiste à associer à chaque mot de n symboles binaire (a_1, a_2, …, a_n), un signal S(i) $1 < i < M$, de durée fini T.

La forme des signaux Si (t) détermine le type de modulation (modulation d'amplitude, de phase, de fréquence, d'amplitude sur deux porteuse en quadrature).

Lorsque nous souhaitons envoyer des symboles n bit (nous supposons que les bits ne peuvent prendre que les valeurs {0,1} par signal, ainsi plutôt que de coder chaque bit indépendamment, on les regroupe par bloc de n ($M= 2^n$).

A chaque symbole formé on fait correspondre une forme d'onde de la constellation. L'utilisation de constellation faisant correspondre à un symbole plusieurs bits permet d'améliorer l'efficacité spectrale (bits/sec/Hz). Les deux techniques les plus connues s'appellent M-QAM et M-PSK. La modulation M-aire peut être combinée au codage de canal pour donner des performances très intéressantes.

Chaque modulation est caractérisée par sa rapidité de modulation pour un débit numérique donné, par son taux d'erreur binaire TEB. Ou par son efficacité spectrale définie

comme le rapport entre le débit numérique (bits/sec) et la bande de fréquence occupée par le signal modulé (Hz) [2].

4. Transmission en bande de base :

La transmission en bande de base consiste à transmettre directement le signal sur le support sans transposition de fréquence.

Cela peut se faire par exemple pour des signaux numériques en utilisant un modem dit à bande de base. Celui-ci utilise directement des supports physiques de types métallique (paires torsadées ou câble coaxiaux) ou fibre optique.

Dans la plupart des cas, les harmoniques supérieures à un certain rang peuvent ne pas être transmises sans qu'on note une altération inacceptable du signal. Les harmoniques d'un signal transmis sur une ligne sont diversement atténués, suivant leur fréquence, par la bande passante de la ligne. Si l'ensemble des harmoniques utiles du signal à transmettre se situent dans la bande passante de la ligne que l'on souhaite utiliser, on peut appliquer ce signal directement à l'entrée de la ligne. Il sera transmis sans atténuation notable à l'autre extrémité.

Les inconvénients majeurs de ce mode de transmission sont :

- Sensibilité aux parasites (bruits en 1/f).
- Coût élevé pour la transmission sur fibre optique ou câble coaxial ;
- Impossibilité de partage direct d'un même canal par plusieurs sources (on ne peut pas suivre plusieurs conversations à la fois !) ;
- Impossibilité de transmission à l'air de signaux basse fréquences (exemple : le son dont les fréquences vont de 20 à 20 kHz soit des longueurs d'onde de 15 à 15000 km).

5. Transmission en bande transposée :

La transmission en bande transposée dite aussi modulation consiste à transmettre le signal de l'information en lui faisant subir une modification préalable de son spectre. La modulation utilise deux signaux :

- Le signal modulant de basse fréquence qui contient l'information et qui peut-être analogique (voix) ou numérique (données informatiques) ;
- Un signal porteur de haute fréquence dont l'un des paramètres (amplitude, fréquence, phase) varie en fonction des évolutions du signal modulant.

Il ne s'agit pas ici de décrire les principes de mise en œuvre de ces modulations mais de donner quelques informations succinctes pour comprendre le principe de la modulation.

Il existe différents modes de modulation qui peuvent consister à réaliser :

- soit une transposition plus ou moins directe du spectre du message vers les hautes fréquences (modulation d'amplitude, de fréquence) ;
- soit une modification radicale du signal lui-même en utilisant des moyens numériques, notamment l'échantillonnage (modulation par impulsions) ;
- soit une combinaison des deux techniques précédentes (Wide Band Code Division Multiple Access - W-CDMA).

L'usage de la modulation permet ainsi de :

- diminuer les longueurs d'onde de signaux transmis (exemple : une fréquence de 100
- MHz correspond à une longueur d'onde de 3,00 mètres) ;
- diminuer la présence de bruit lors de la transmission ;
- transmettre de signaux par voie hertzienne (exemple : la radio) ;
- transmettre simultanément sur le même support plusieurs informations sans « télescopage » par multiplexage fréquentiel.

Sa mise en œuvre est toutefois :

- plus complexe : risque d'augmentation de la dégradation du signal due aux équipements ;
- plus consommatrice de bande passante que pour le message d'origine. La bande de fréquences à l'émission est plus importante que celle du message d'origine (transposition vers les hautes fréquences) [4].

6. Milieu et les canaux de transmission :

Il assure la transmission des signaux générés par le codeur Maires ou par modulateur .Il apporte une atténuation de type aléatoire ou non, le signal reçue posséder en général un niveau comptable au bruit généré par les composants du circuit d'entrée du récepteur, ce bruit qui s'ajoute au signal reçu est généré d'une façon aléatoire et est une causes des erreurs de transmission.

Capacité d'un canal est une mesure de la quantité maximale d'information qui peut être transmission sur un canal puis reçue avec une probabilité d'erreur négligable.si l'on représente

l'entrée et la sortie d'un canal sans mémoire par les variables aléatoire X_k et Y_k respectivement la capacité d'un canal est définie comme le maximum de l'information mutuelle entre X_k et Y_k [4].

$$\boldsymbol{C = maxI(Xk\,;\,Yk)} \tag{1}$$

$$\boldsymbol{I(Xk\,;Yk) = H(Xk) - H(Xk/Yk)} \tag{2}$$

L'unité de capacité est le débit par symbole.

Avec $I(Xk\,;Yk)$: L'information transmise par le canal

$H(Xk)$: L'information de départ. [H : Entropie]

$H(Xk\,/\,Yk)$: Perte d'information lors de la transmission.

L'équation représente la différent entre l'incertitude à la sortie du canal quand on a aucune connaissance du message élémentaire émis moins celle que l'on a quand on connait le message élémentaire émis.

$$\boldsymbol{I(Xk\,;Yk) = 0} \qquad \text{Canal mauvais} \tag{3}$$

$$\boldsymbol{I(Xk\,;Yk) = H(Xk)} \qquad \text{Canal sans erreur} \tag{4}$$

Dans le cas d'un canal BBAG :

Le canal gaussien est un canal idéal purement théorique ou le bruit est reparti suivant une loi normale communément appelée loi gaussienne.

La formule de base de capacité est donnée par la relation suivante :

$$\boldsymbol{C = Blog_2(1 + A)} \quad \text{Avec} \quad \mathbf{A = \left(\frac{C}{B}\right).\left(\frac{E_b}{N_0}\right)} \tag{5}$$

OU : B : la bande passante du canal en (HZ)

N_0: la densité spectrale du bruit (Watt/Hz)

C : la capacité en bit/seconde.

E_b : l'énergie nécessaire pour la transmission d'un bit.

7. Les canaux de transmission :

7.1. Canal binaire symétrique :

Le canal binaire symétrique (CBS) est un canal discret dont les alphabets d'entrée et de sortie sont finis et égaux à 0 ou 1. On considère dans ce cas que le canal comprend tous les éléments de la chaîne comprise entre le codeur du canal et le décodeur correspondant (voir la figure 1.3) [11].

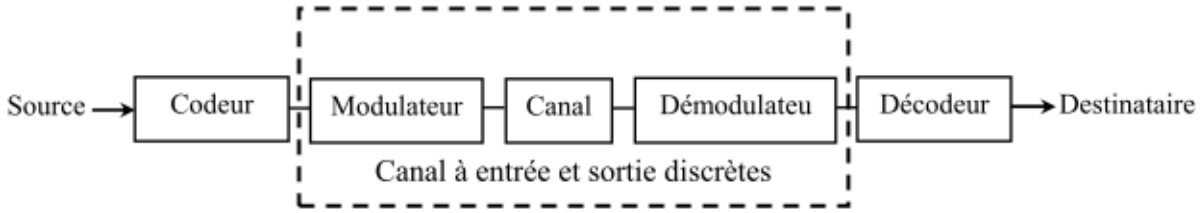


Figure 2. Description d'un canal binaire symétrique.

On note respectivement par *Xk* et *Yk* les éléments à l'entrée et à la sortie du CBS. Si le bruit et d'autres perturbations causent des erreurs statistiquement indépendantes dans la séquence binaire transmise avec une probabilité p, alors :

$$\boldsymbol{prob(Yk = 0|Xk = 1) = prob(Yk = 1|Xk = 0) = p} \quad (6)$$

$$\boldsymbol{prob(Yk = 0|Xk = 0) = prob(Yk = 1|Xk = 1) = 1 - p} \quad (7)$$

Le fonctionnement du CBS est résumé sous forme de diagramme dans la figure 1.4. Chaque élément binaire à la sortie du canal ne dépendant que de l'élément binaire entrant correspondant, dans ce cas le canal est dit « sans mémoire ».

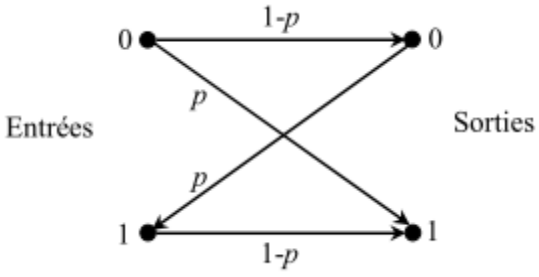


Figure 3. Diagramme du canal binaire symétrique.

7.2. Canal à bruit blanc Gaussien :

Le modèle de canal le plus fréquemment utilisé dans les transmissions numériques, qui est aussi un des plus faciles à générer et à analyser, est le canal à bruit blanc additif Gaussien. Ce bruit modélise à la fois les bruits d'origine interne (bruit thermique dû aux imperfections des équipements...) et le bruit d'origine externe (bruit d'antenne...). Ce modèle est toutefois plutôt associé à une transmission filaire, puisqu'il représente une transmission quasi-parfaite de l'émetteur au récepteur [7].

Le modèle du canal à bruit blanc Gaussien (Additive White Gaussien Noise : AWGN) est composé selon le principe de la Figure 1.5 d'un bruit blanc Gaussien ajouté à l'onde modulée s(t).

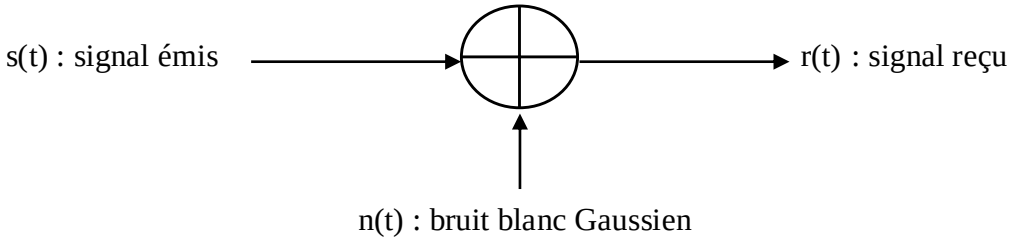


Figure 4. Modèle du canal AWGN.

Le signal reçu s'écrit alors :

$$\boldsymbol{r(t) = s(t) + n(t)} \tag{8}$$

Où n(t) représente le bruit, caractérisé par un processus aléatoire Gaussien de moyenne nulle, de variance σ_n^2 et de densité spectrale de puissance bilatérale notée$\emptyset_{nn} = \frac{N_0}{2}$.

7.3. Canal de Rayleigh :

Ce canal est donné par un model variable avec le temps qui est dû à un effet connu sous le nom de l'évanouissement, causé par l'inhomogénéité de la nature physique du canal [7].

Pour une transmission sur canal de Rayleigh, le rapport signal à bruit est une variable aléatoire dont la densité de probabilité est donnée par la relation :

$$\boldsymbol{P_\gamma(x) = \frac{1}{A} e^{-\frac{x}{A}}} \tag{9}$$

La capacité du canal de Rayleigh est donnée par l'équation :

$$\boldsymbol{C = Be^{\frac{1}{A}}(-E + ln + \frac{1}{A} - \frac{1}{4A^2} + \frac{1}{18A^3} - \frac{1}{96A^4})/ln_2} \qquad \text{Avec} \qquad \boldsymbol{A = \left(\frac{C}{A}\right).\left(\frac{E_b}{N_0}\right)} \qquad (9)$$

E : constante d'Euler dont la valeur approximation est : 0.5772157

8. Démodulation :

Lorsque l'on reçoit un signal modulé, il faut en extraire le signal utile, cette opération s'appelle démodulation, elle représentera donc le message présent à son entrée sous forme de symboles compatibles au décodeur de canal [8].

9. Conclusion :

Ce premier chapitre a été consacré à donner des généralités concernant les différents blocs constituant une chaine de transmission numérique.

Dans le chapitre suivant nous allons abordes en détail les registres à décalage à rétroaction linéaire appelée LFSR et leurs application dans les systèmes de communication mobiles.

III. Registre à décalage à rétroaction linéaire

1. Introduction :

Un registre à décalage à rétroaction linéaire ou LFSR (Linear Feedback Shift Register) a habituellement la rétroaction pour lui permettre d'effectuer des opérations plus avancées qui pourraient exiger d'une fonction spécifique de modeler le comportement d'état.

La nature du circuit de rétroaction, plus lequel l'endroit de registre dans le registre à décalage qu'elle est reliée détermine la fonction du LFSR. Ceci mène à un circuit flexible, particulièrement si une conception reconfigurable est employée, qui peut être employée dans beaucoup d'applications selon quelle fonction elle est nécessaire pour mettre en application. Ces applications incluent le générateur de nombre pseudo-aléatoire, le générateur et l'analyseur de modèle aléatoire, le chiffrage/déchiffrage et le spectre de diffusion par m-séquence pour le traitement numérique du signal [1]. LFSR dans la définition la plus simple sont employés en tant que générateurs de nombre pseudo-aléatoire. Quand correctement configuré pour des ordres de longueur maximum, chaque état sera atteint seulement une fois jusqu'à ce que chaque état ait été atteint. Une fois que chaque état a été atteint, l'ordre sera répété.

Ce chapitre discutera les deux réalisations principales du réseau de rétroaction, comment configurer le LFSR pour des ordres de longueur maximum, et présente quelques applications de LFSRs.

2. Registres à décalage à rétroaction linéaire :

Des LFSR en général sont construits avec le *D*-type bascules dans le chemin vers l'avant et la logique linéaire de *XOR* ou de *XNOR* dans le chemin de rétroaction. La valeur initiale du registre à décalage, les robinets de registre à décalage et la logique de rétroaction déterminent l'ordre de rendement [2].

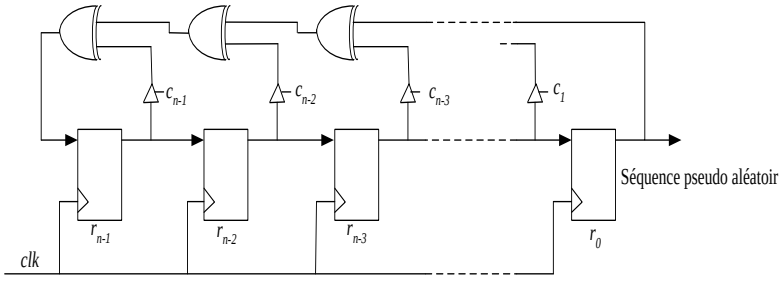
- Si des portes de *XOR* sont utilisées dans le chemin de rétroaction, le *LFSR* ne changera pas des états si l'état actuel est chacun des *0s*.
- De même, si des portes de *XNOR* sont utilisées, le *LFSR* ne changera pas des états si l'état actuel est chacun des *1s* [3].

2.1. Configurations de rétroaction :

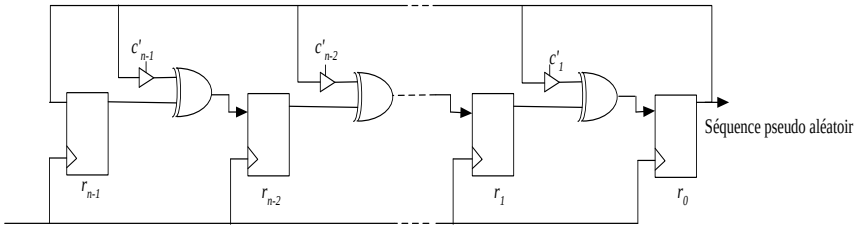
Dans cette section sont présentés les principes et les fondements mathématiques d'une structure couramment utilisée dans les architectures permettant le traitement de codes correcteurs d'erreur, ou plus généralement pour la production de séquences pseudo-aléatoires.

Les générateurs pseudo-aléatoires de type *LFSR*, sont des registres à décalages complétés par des boucles de rétroaction à base de portes *« ou-exclusif »*.

La forme générale des *LFSRs* est représentée sur la figure 1. Deux architectures de *LFSR* sont couramment utilisés : une dite de type 1 à portes *« ou-exclusif »* externes (figure 1.a) et une dite de type 2 à portes *« ou-exclusif »* internes (figure 1.b) [4].



(a)" many- to- one "



(b)" one -to- many "

Figure 5. Les deux architectures de LFSR.

Un registre est contrôlé par une horloge qui lui est externe. Dans notre cas, il s'agira de l'horloge système du circuit sur lequel cette architecture est implantée. Ces registres ont des propriétés particulièrement intéressantes, qui permettent entre autre d'envisager leur utilisation en tant que compteurs programmables. Les deux types d'architectures permettant de réaliser des ***LFSR*** sont présentées sur la figure 1.

Un choix judicieux des coefficients ***{ci} 1≤ i <n et {c'i} 1≤ i <n*** permet d'obtenir de ces deux architectures un comportement équivalent, mais l'architecture de la figure 1.b est la plus adaptée à l'implantation sur circuit numérique **[5].**

La fréquence maximale de fonctionnement d'un ***LFSR*** de type 1 est limitée par le chemin de rétroaction externe pouvant comporter un grand nombre de portes. Il s'intègre par contre facilement autour d'un registre à décalage préexistant.

La fréquence de fonctionnement du ***LFSR*** de type 2 est uniquement limitée par la durée de propagation des données au travers d'une porte « ou-exclusif » et d'une bascule mais il s'intégrera difficilement sur un registre à décalage du système.

- **Principe mathématique :**

L'ensemble des principes présentés dans cette section utilisent l'architecture *manyto- one* de la figure 1.a, car celle-ci permet une présentation plus simple des équations.

Les propriétés énoncées dans ce paragraphe peuvent également être appliquées à la forme *one-to-many* en utilisant les relations d'équivalence [**1**].

Le registre est initialisé avec la séquence $\boldsymbol{R_0 = (r_0, r_1, \ldots, r_{n-1})_0}$. À chaque itération, le contenu des cellules est décalé vers la droite, et celui de la cellule la plus à gauche, $\boldsymbol{r_{n-1}}$, est remplacé par une combinaison linéaire des contenus de certaines des cellules du registre.

Cette ***séquence est pseudo*** aléatoire car elle est en réalité périodique : elle se reproduit identique à elle-même au bout d'un certain temps lié à la longueur du registre à décalage.

Si le registre est initialisé avec tout à ***0***, alors la sortie sera toujours nulle. A l'inverse on montre que si au moins une bite ***1*** est injecté dans l'une des bascules, le registre prendra tous les états possibles sauf l'état tout à ***0***. Cette séquence ne sera pas obtenu pour tous les polynômes de degré ***n***, mais seulement pour une certaine classe d'entre eux appelés **« *polynômes primitifs* ».**

En conservant les notations présentées sur la figure 1.a, il est possible d'écrire l'état $\boldsymbol{R_k}$ des cellules d'un LFSR après ***k*** itérations en utilisant le système d'équations récurrentes suivant :

$$\begin{cases} \mathbf{r_{k+1,i} = r_{k,i+1}, \text{ pour } i \leq 0 \leq n-2} \\ \mathbf{r_{k+1,0} = \sum_{j=1}^{n-1} c_j \cdot r_{j,0}} \end{cases} \quad (1)$$

Ce système peut également être représenté sous la forme matricielle équivalente : $R_{k+1} = T \cdot R_k$

$$\begin{bmatrix} r_{k+1,0} \\ r_{k+1,1} \\ \vdots \\ r_{k+1,n-2} \\ r_{k+1,n-1} \end{bmatrix} = \begin{bmatrix} 1 & c_1 & \dots & c_{n-2} & c_{n-1} \\ 0 & 0 & \dots & 0 & 1 \\ \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} r_{k,0} \\ r_{k,1} \\ \vdots \\ r_{k,n-2} \\ r_{k,n-1} \end{bmatrix} .$$

Avec cette notation les *k* itérations effectuées sur le vecteur R_0 contenant les valeurs initiales du ***LFSR*** se traduisent par l'opération matricielle :

$$R_k\, T^k = \cdot R_0. \qquad (2)$$

Théorème 1 :

Si l'état initial d'un ***LFSR*** est $r_0=r_1=\dots=r_{i-2}=0$ et $r_{i-1}=1$, alors la séquence ***{ci}*** du LFSR est périodique avec une période égale au plus petit entier *k* tel que ***P(x)*** divise $(1-x^k)$.

2.2. Périodicité, polynôme minimal et polynôme primitif :

Les vecteurs ***Ri,*** dans le cas d'une implantation sur circuit numérique, prennent leurs valeurs dans le corps de Galois $GF(2^n)$, où ***n*** est la longueur du registre utilisé. Il s'agit d'un ***corps fini*** et les opérations récurrentes sur cet ensemble sont périodiques **[6].**

- Plus particulièrement l'opération réalisée par le ***LFSR*** est périodique, et il existe par conséquent une valeur $m \in N$ telle que $Rm = R_0$, où ***m*** définit la période du ***LFSR***.

Il est possible de garantir que cette période soit maximale **[7].**

À cet effet, on définit un polynôme ***P(X)*** sur ce corps, appelé **« *polynôme caractéristique* »** d'un LFSR de la façon suivante :

$$\mathbf{P(X) = X^n + \sum_{i=0}^{n-1} c_i . X^i} \qquad (3)$$

Les caractéristiques de la séquence $\{Ri\}\ i \geq 0$ dépendent de celles de ***P(X).***

En particulier, la période de cette séquence est maximale dans le cas où ***P*** est un polynôme primitif sur **GF(2).** Cela signifie que ***P*** est de degré minimal (en l'occurrence ***n***) et qu'il est irréductible (il n'a aucun autre diviseur que l'unité et lui-même) **[8].**

- La période maximale d'une telle séquence vaut alors : qu'il est irréductible (il n'a aucun autre diviseur que l'unité et lui-même) **[8].**

Par définition **[10],** la longueur maximale d'une séquence générée par un LFSR à n étages, est de 2^n-1. Le polynôme caractéristique associé à une séquence de longueur maximale est appelé polynôme primitif.

- La période maximale d'une telle séquence vaut alors : $Mmax = 2^{n-1}$.
- Si le registre est piloté par une horloge de période T, la durée de la séquence est donc : $(2n-1)T$.

- Le plus petit polynôme caractéristique, et donc le plus petit **LFSR**, permettant de générer la suite de $\{Ri\}\ 0 \leq i < m$ peuvent être calculés si au moins n éléments r_i consécutifs sont connus.

- Un tel polynôme est dit irréductible s'il n'est divisible par aucun autre polynôme de ce type de degré supérieur à zéro.

Théorème 2 :

Un polynôme irréductible satisfait les deux conditions suivantes :

1. Il a un nombre impair de termes (le terme 1 inclus)
2. S'il est de degrés supérieur à 3 alors $P(x)$ doit se devise en $(1+x^k)$, avec $k=2^n-1$.

Théorème 3 :

Un polynôme primitif est irréductible si le plus petit entier positif k qui permit le polynôme de se diviseur en $(1+x^k)$ est tel que $k=2^n-1$ avec le degré du polynôme.

Ces polynômes donnent des périodes maximales. Les LFSR ont les caractéristiques suivantes :

- La sortie est le bit le moins significatif.
- La période est la longueur de séquence produite avant qu'elle ne commence à se répéter.
- La fonction de rétroaction étant simplement une opération de « ou exclusif » de certains des bits du registre, la liste de ces bits est appelée « **la séquence de dérivation** ». Elle est obtenue à partir du polynôme choisi.
- Ils sont faciles à réaliser en matériel.

2.3. Recherche Des Polynômes Primitifs :

La recherche des polynômes primitifs de très grands poids, c'est-à-dire de degré supérieur est une étape algorithmique importante, pour les ingénieurs concepteurs des applications de communications moderne.

- **Théorèmes et définitions :**

L'anneau des polynômes :

On appelle polynôme une expression de la forme :

$$\mathbf{P(x) = c_0 + c_1 x + c_2 x^2 + \cdots . + c_n x^n} \quad (4)$$

- Dans laquelle les coefficients ***c0, c1,…...*** appartiennent à un corps de Galois ***GF(2).***
- On vérifier facilement que les polynômes ont une structure d'anneau de variable x.
- Le polynôme est dit normalisé si le coefficient du terme de plus haut degré est 1.
- Le degré d'un polynôme est la puissance la plus élevée de x à coefficient non nul.

Un message de n bites étant représenté par une suite binaire lue de gauche à droite, on convient de lui associer un polynôme en x de degré ***(n-1).*** **[9].**

a) Polynôme irréductible :

Soit ***GF(2) [x]*** l'ensemble des polynômes en x à coefficient dans ***GF(2),*** un polynôme ***g(x)*** de ***GF(2)[x]*** est dite irréductible sur ***GF(p)*** ,s'il ne se décompose pas en un produit de polynôme non triviaux ,c'est-à-dire polynômes de degré strictement positifs de *GF(p) [x]*

Exemple :

1. Le polynôme $P(x)= 1+ x+ x^2$ est irréductible sur *GF(2),*
2. Le polynôme $F(x)=x+x^3$ n'est pas irréductible sur *GF(2)* car $F(x)=x\,(1+x)$.

Période d'un polynôme :

- Tout polynôme à un période, est la période d'un polynôme irréductible de degré n est 2^n-1
- Tous polynômes irréductible **[24]** sur ***GF(2)*** de degré m divise x^k+1 avec $k=2^m-1$.

Exemple :

- x^3+x+1 divise x^7+1 on effet $2^3-1=7$
- $x^7+1=(x4+ x^2+x+1)\,(x3+x+1)$

b) polynôme primitif :

Un polynôme *P(x)* de degré m est dit primitif [26], si le plus petite entier *n* pour que :
g(x) divise x^n+1 *et* $n=2^m-1$.

- **Idéal sur un anneau de polynôme [10,11] :**

Un semple de polynômes sure ***GF(2)*** est un idéal soit et seulement s'il contient tous les multiples d'un polynôme donné ***g(x).***

- **Déféminisations polynômes primitifs :**

Ces polynômes générations sont déterminés en factorisant le polynôme x^n+1 un produit de polynômes irréductibles, il suit trois étapes :

1. Recherche des polynômes diviseurs de x^n+1.

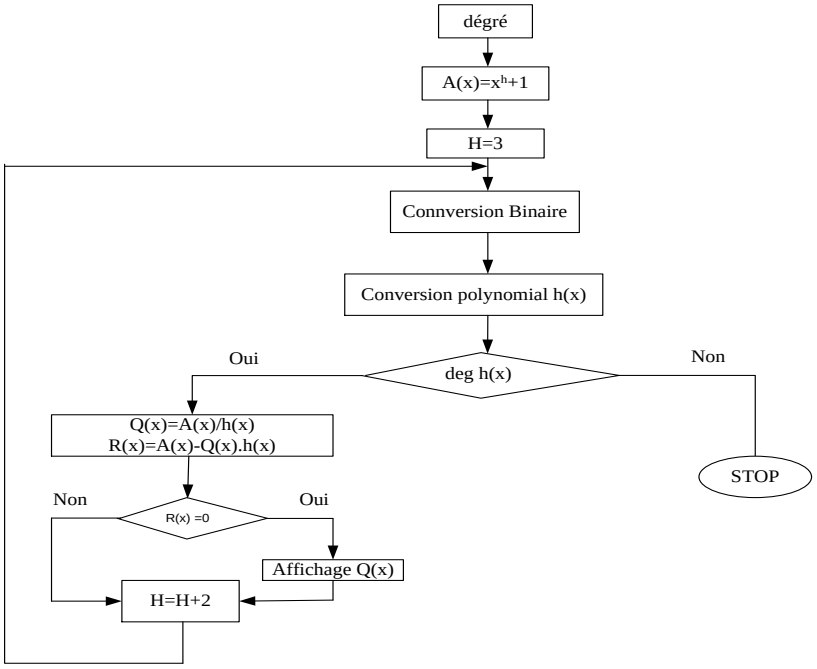


Figure 6. Organigramme pour la recherche des polynômes diviseur

2. Parmi ces polynômes diviseurs, recherche des polynômes irréductibles.

Un polynôme ***g(x)*** est dit irréductible s'il ne possède aucuns diviseurs de degré supérieur à zéro.

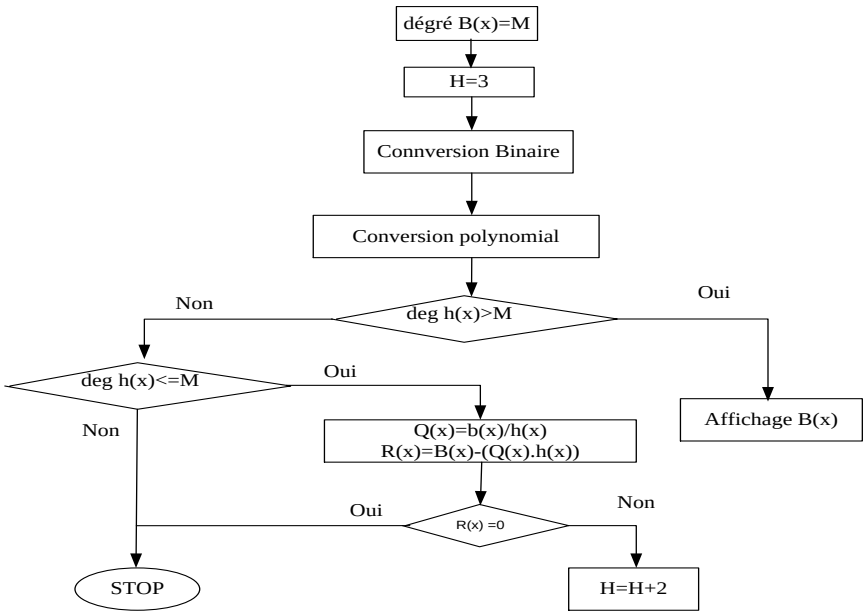


Figure 7. Organigramme pour la recherche de polynômes irréductible.

3. Parmi ces polynômes irréductibles, on recherche des polynômes primitifs. On appelle période ou ordre d'un polynôme ***g(x)*** le plus petite entier u tel que ***g(x)*** divise x^u+1.

Si un polynôme ***g(x)*** de degré r est irréductible, on peut montrer que la période de g (x***)*** divise 2^r-1.

Lorsque la période de ***g(x)*** est égale à 2^r-1., le polynôme irréductible ***g(x)*** est appelé primitif.

Théorème : Un polynôme primitif est irréductible et satisfait les deux conductions suivant :

- Il a un nombre impair de termes (le terme 1 inclus).
- S'il est de degré supérieur à 3 alors ***p(x)*** doit se diviser e

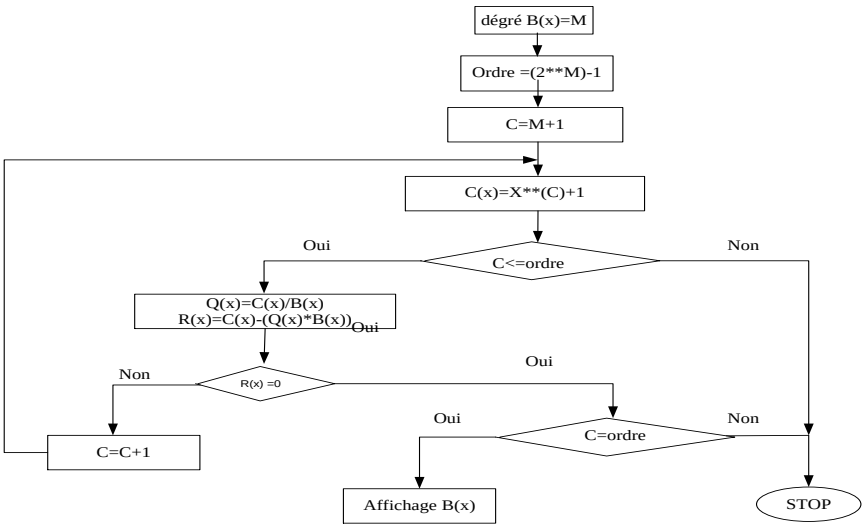


Figure 8. Organigramme pour la recherche des polynômes primitifs.

Exemple : Recherche les polynômes générateurs issus de $x^n+1= x^7+1$.

1. ***1ère étape :*** **Recherche des polynômes diviseurs.**

   polynômes diviseurs de x^7+1

   $x+1$ x^3+x+1 $x^3+ x^2+1$ $x^4+ x^2+x+1$ $x^4+ x^3+ x^2+1$

2. ***2ème étape :*** **Recherche des polynômes irréductibles.**

   polynômes irréductibles

   $x+1$ x^3+x+1 $x^3+ x^2+1$

3. 3ème étape : **Rechercher** *des polynômes primitifs.*

polynômes primitifs

x^3+x+1 $x^3+ x^2+1$

- Nous allons procéder à la recherche de ces polynômes générateurs qui sont déterminés en factorisant le polynôme x^n+1en un produit de polynômes irréductibles, et voilà quelques résultats obtenus :

Tableau 2. Recherche de ces polynômes générateurs.

Degré (n)	Longueur (2^n-1)	polynômes générateurs
2	3	[1,2]
3	7	[2,3],[1,3]
4	15	[3,4],[1,4]
5	31	[2,5],[3,5],[2,3,5],[1,2,3,5],[2,3,4,5],[1,3,4,5]
6	63	[1,6],[1,3,4,6] ,[1,2,5,6],[1,2,3,5,6]
7	127	[1,7],[1,3,7] [4,7],[1,2,3,7],[1,2,5,7],[3,4,5,7],[1,2,3,4,5,7]
8	255	,[2,3,4,8],[3,4,5,8] ,[1,2,3,4,5,8],[2,3,6,8] ,[1,2,3,4,6,8]
9	511	,[4,9],[1,3,4,9],[5,9],[2,3,5,9],[1,4,5,9]
10	1023	[1,2,3,10],[3,10],[1,3,4,10][1,2,3,4,10]
11	2047	[2,11],[1,2,4,11],[1,3,5,11],[1,2,6,11],[1,5,6,11],[1,2,5,6,11]
12	4095	[3,12],[1,2,3,12], [1,2,4,12],[5,12],[1,4,5,12], [2,4,5,12],
13	8195	[1,3,4,13], [1,4,5,13], [1,2,4,5,13], [1,4,6,13],,[2,5,6,13], [1,2,3,5,6,13],
14	16383	[1,6,10,14],[1,3,4,6,7,9,10,14],[4,5,6,7,8,9,12,14][1,6,8,14],[5,6,9,10,11,12,13,14]
15	32767	[1,15] [1,5,10,15] [1,3,12,15],[1,2,4,5,10,15],[1,2,6,7,11,15],[1,2,3,6,7,15]

16	65535	[1,3,12,16],[1,3,6,7,11,12,13,16],[2,3,4,6,7,8,9,16],[7,10,12,13,14,16][1,2,4,6,8,9,16]
17	131071	[3,17],[1,2,3,17] ,[3,4,8,17]
18	262143	[7,18],[5,7,10,18],[7,8,9,10,15,16,17,18]
19	524287	[1,2,5,19],[3,4,5,8,13,19],[3,7,9,10,12,19]
20	1048575	[3,20],[3,5,9,20],[2,3,6,8,11,20]
21	2097151	[2,21], [2, 7,,14,21],[2,5,13,21]
22	4194303	[1,22],[1,5,9,22],[1,4,7,10,13,16,19,22]
23	8388607	[5,23], [5, 11, 17,23]
24	16777215	[1,2,7,24],[4,5,7,8,9,11,14,16,18,20,22,24][1,4,5,9,10,13,14,15,16,17,18,19,21,24]
25	33554431	[3,25], [1, 2, 3,25], [3, 4,12,25]

On remarque que :

1. Tous les polynômes générateurs sont issus de la division de x^n+1, avec $n=2^k-1$(k entier).
2. Soit $n_1=2^k-1$(k entier),$\forall\ m$ un entier, le que $n=m\ *n_1$, les polynômes générateurs issus de la division x^n+1 sont les mêmes que ceux issus de la division x^n+1.
3. Si n n'est pas un multiple de $n=2^k-1$(k entier), alors tous les polynômes diviseur de x^n+1 ne sont pas des polynômes générateurs.

Enfin, on peut constater que pour la recherche des polynômes générateurs pour un n donné, il faut :

- Décomposer n en un produit de facteurs de la forme $n=2^k-1$(k entier),
- Les polynômes générateurs issus de x^n+1 sont la somme des polynômes générateurs issus du différent facteur.

Exemple : Pour $n=1023=33*$31 générateurs de degré 10 .Donc, les polynômes générateurs de $x^{1023}+1$ sont la somme des polynômes générateurs de 33 et 31 plus les générateurs de degré 5.

- x^5+x+1, $x5+ x^2+1$, $x5+ x^3+ 1$, $x5 + x^3+ x^2+x+1$, $x15+x^4+ x^3+ x+1$, $x10+x^4+ x^3+ x^2+1$

2.4. Sécurité des LFSR :

Pour assurer une meilleure sécurité, on doit respecter 3 caractéristiques :

- La période doit être la plus longue possible.
- Le flux de sortie doit être le plus aléatoire possible.
- La clé *K* servant d'initialisation doit être la plus longue possible (au moins 128 bits) et rester secrète.

Une attaque très commune porte le nom d'attaque par corrélation. Le principe est de trouver un LFSR dont la sortie est corrélée avec la sortie des LFSR utilisés.

3. Conclusion :

Les registres à décalage à rétroaction linéaire LFSR permettent en particulier de remplacer avantageusement les compteurs dans les architectures numériques dans lesquelles ils sont utilisés. De plus, s'ils sont présentés sous leur forme «one-to-many», ils correspondent très bien à la structure interne dans un circuit programmable FPGA. La connaissance des structures algébriques ainsi que les propriétés des polynômes primitifs permettent d'établir la construction pratique des codes détecteurs et correcteurs d'erreurs et, des générateurs pseudos aléatoires. La recherche des polynômes primitifs de très grands poids, et de degré supérieur est une étape algorithmique importante pour les ingénieurs concepteur des applications de télécommunication au centre de nombreuses applications importantes en télécommunications : l'étalement spectral, brouillage, chiffrement continu et des générateurs de nombre pseudo-aléatoire….et

IV. Application Des LFSR Dans Les Systèmes De Communication Mobile

1. Introduction :

Depuis les années 1980, le secteur des communications à distance connait une croissance fulgurante grâce aux progrès technologiques réalisés dans plusieurs domaines scientifiques. Cette évolution est particulièrement frappante pour les communications radio-mobiles avec l'apparition des différentes générations de téléphonie mobile. Parallèlement, les applications pouvant bénéficié de cette évolution technologique n'ont cessé de se diversifier.

Ainsi, nous assistons actuellement à l'avènement de la visiophonie et du visionnage de signaux audiovisuels sur des appareils de téléphonie mobile. Ces nouvelles fonctionnalités nécessitent des transmissions de plus en plus rapides garantissant à la fois une nécessaire flexibilité et une impérieuse efficacité au niveau de la qualité de service. Pour ce faire, les nouveaux réseaux de télécommunications doivent permettre l'accès simultané d'utilisateurs toujours plus nombreux aux multiples services proposés par les différents opérateurs de téléphonie mobile. Les bandes de fréquences de transmission étant limitées, l'efficacité de l'utilisation des ressources de transmission s'avère primordiale. [2]

Plusieurs techniques de multiplexage ont successivement été proposées dans le but d'utiliser à bon escient la bande de fréquence disponible. La technique d'accès multiple à répartition en fréquence, ou plus communément FDMA (*Frequency Division Multiple Access*) est la méthode de partage de ressource spectrale la plus ancienne. Elle consiste à allouer à chaque utilisateur une bande de fréquence différente pour permettre des transmissions simultanées. Un autre procédé permet à tous les utilisateurs d'émettre sur l'ensemble de la bande de fréquence mais successivement dans le temps. Il s'agit de la technique d'accès multiple à répartition en temps, appelée plus communément TDMA (*Time Division Multiple Access*). Généralement, les techniques FDMA et TDMA sont combinées pour une meilleure exploitation de la bande de fréquence. En effet, le principal inconvénient de ces deux techniques est qu'il est difficile de gérer l'ensemble de la bande de fréquence de façon optimale. D'une part, avec la technique FDMA, si au cours du temps un utilisateur n'émet pas de signal, alors la bande de fréquence qui lui est allouée n'est pas utilisée. D'autre part, avec la technique TDMA, si un utilisateur n'émet pas durant l'instant qui lui attribué, alors l'intervalle de temps qui lui correspond n'est pas utilisé. La combinaison des deux techniques rend l'allocation de ressources plus flexible. Cependant, ces deux techniques

conservent une certaine rigidité qui nuit à l'efficacité de l'utilisation optimale des ressources de transmission. C'est pourquoi, une autre technique a fait son apparition dans les standards de télécommunication. [2]

Il s'agit de la technique d'accés multiple à répartition en code, appelée plus communément CDMA (*Code Division Multiple Access*). Cette technique permet à tous les utilisateurs de transmettre simultanément dans une même bande de fréquence au cours du temps. Ainsi, toutes les ressources disponibles sont exploitées de manière optimale. Par contre, la difficulté réside dans la séparation des signaux de chaque utilisateur. Pour ce faire, un code d'étalement spécifique est alloué à chaque utilisateur. Lors de la réception, ces codes servent à la distinction des signaux émis par les différents utilisateurs. Cette technique de multiplexage est désormais privilégiée par les nouveaux standards de téléphonie mobile. Ainsi, des normes radio-mobiles récentes telles que la norme américaine CDMA 2000 et la norme européenne UMTS (*Universal Mobile Télécommunications System*), l'ont retenu comme technique d'accès.

Au niveau technologique, les performances optimales d'un système mono-utilisateur sont atteintes par des systèmes Multi-utilisateurs de type CDMA en assignant aux différents utilisateurs des codes orthogonaux entre eux. Les codes de Hadamard qui ont cette propriété d'orthogonalité sont généralement utilisés pour des transmissions synchrones. Ce type de transmission est représentatif d'une communication sur la voie descendante d'un réseau de télécommunication mobile ou la station de base émet vers les différents terminaux mobiles. A l'inverse, lors d'une transmission sur la voie montante, pour laquelle les différents terminaux mobiles émettent indépendamment vers la même station de base, la transmission est dite asynchrone. Dans ce second cas, des codes non orthogonaux ayant des inter-corrélations très faibles peuvent être utilisés. Néanmoins, cette propriété d'orthogonalité nécessaire à la séparation des signaux dans les systèmes CDMA constitue l'une des contraintes majeures de la technique CDMA. [2]

2. Techniques d'accès multiple :

Pour tout système mobile, il est nécessaire de définir et d'optimiser la façon dont les ressources radio disponibles sont allouées entre plusieurs utilisateurs. C'est à dire il faut définir la technologie d'accès qui permet une gestion plus efficace de l'interface radio.

Il existe trois méthodes classiques : le FDMA, LE TDMA, le CDMA.

❖ FDMA (Frequency Division Multiple Access) :

Est la méthode d'accès multiple la plus utilisée. Elle permet de différencier les utilisateurs par une simple différenciation fréquentielle. En effet, pour écouter l'utilisateur N, le récepteur ne considère que la fréquence f_N associée. L'implémentation de cette technique est assez simple. [3]

Avantage :

- Faible complexité du terminal mobile : pas d'égalisation ou de tramage complexe et de synchronisation.
- Transmission et synchronisation continue possible.

Inconvénients :

- Coûts des équipements fixes élevés et plus d'équipement au niveau de la station de base.
- Nécessité d'un duplexeur contre les interférences entre l'émetteur et le récepteur du mobile ce qui entraîne des coûts supplémentaires.

❖ TDMA (Time Division Multiple Access):

A la différence de FDMA, une simple bande de fréquence est à la disposition d'un certain nombre d'abonnés avec TDMA. La bande de fréquence est divisée en trames de TDMA de longueur finie. Chaque trame est divisée en n time slots (TS). Chacun de ces n time slots de la trame peut être assignés à un abonné différent. De ce cette façon, une simple bande de fréquence peut contenir jusqu'à n abonnés. La transmission d'un seul abonné comporte différents time slots assignés cycliquement à l'abonné (généralement un TS par trame, de plus longs cycles sont également possible). Avec TDMA, chaque bande de fréquence est uniquement employée par un seul abonné à un moment particulier. Ceci empêche la production d'interférences entre différents abonnés. Le TDMA est surtout utilisé dans les systèmes de deuxième génération, tel que le GSM. [3]

Avantage :

- Coût réduit de la station de base.
- Souplesse de modification sur les débits transmis.

Inconvénients :

- Complexité au niveau du mobile et traitement numérique plus complexe.
- Ajout de bits de signalisation et de synchronisation.

❖ **CDMA (Code division Multiple Access) :**

Est la méthode d'accès la plus récente. Le premier système CDMA qui a été développé est la norme américaine TIA-EIA-IS-95-A/B

Dans le cas de l'accès multiple à répartition par les codes, tous les mobiles coexistent dans une même bande de fréquence et transmettent sur les mêmes intervalles temporels comme l'illustre la figure II.1, mais utilisant des techniques d'étalement de spectre pour lesquelles chaque utilisateur possède un code ou séquence unique dans la cellule qui détermine les fréquences et les puissances utilisées. Ces techniques consistent à redistribuer et étaler le signal sur une grande largeur de bande, jusqu'à le rendre invisible, idéalement, pour les autres utilisateurs de la même largeur de bande. L'émetteur lie l'information originale avec le code. L'information codée est alors transmise au travers de l'interface par radio. L'information originale est régénérée dans l'unité de récepteur en utilisant le même code de manière synchrone. En isolant les séquences provenant des autres utilisateurs (qui apparaissent comme un bruit), le signal original de l'utilisateur peut alors être extrait. [3]

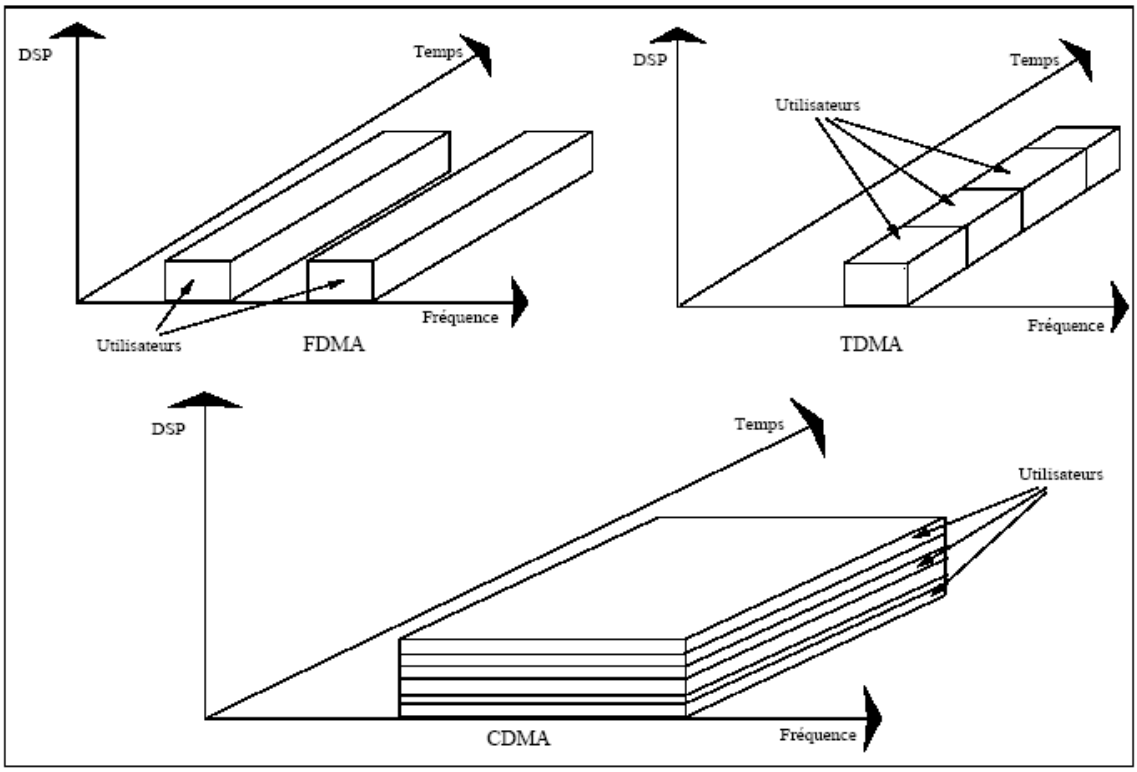


Figure 9. Techniques d'accès FDMA, TDMA, et CDMA.

DSP (Densité Spectrale de Puissance).

Parmi les techniques d'étalement de spectre, on peut citer :

- TH-CDMA (Time Hopping CDMA).
- FH-CDMA (Frequency hopping CDMA).
- DS-CDMA (Direct-sequence CDMA).

La figure suivante montre les différents types de CDMA :

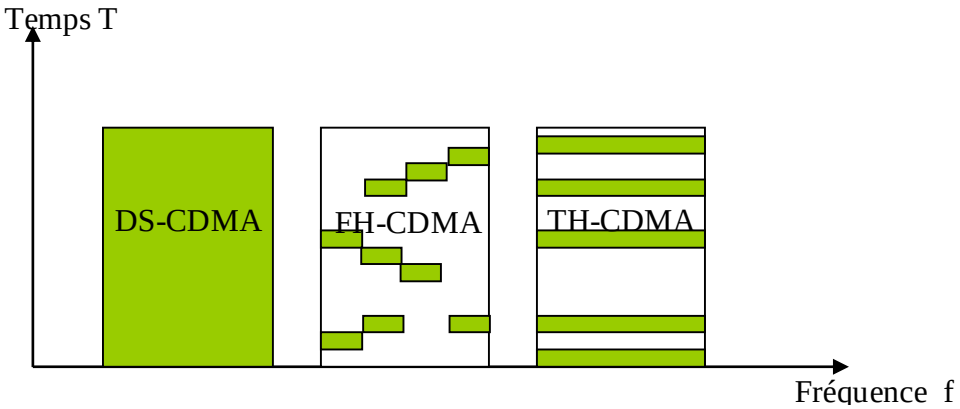


Figure 10. Type de CDMA.

Dans la méthode TH-CDMA (Time Hopping CDMA) on utilise le multiplex de temps. Le signal d'information est transféré par flashs. Le temps de transmission par rafales est indiqué par le code de propagation. Cette technique a été développée comme première méthode de CDMA.

Dans le protocole CDMA par saut de fréquence, la fréquence porteuse du signal d'information modulé n'est pas constante et change périodiquement. Pendant des intervalles de temps T, la porteuse reste la même, mais après chaque intervalle de temps, la porteuse saute vers une autre (ou éventuellement la même).

Un exemple de l'utilisation civile de FH-CDMA est la prétendue norme de Bluetooth. Le Bluetooth permet la transmission d'information aux débits élevés pour de petites distances dans l'intervalle de fréquence autour de 2.4 GHz sans licences.

Dans le protocole DS-CDMA (Direct Séquence CDMA), l'information d'un usager est étalée directement en joignant un code d'étalement.

Ceci a comme conséquence la transmission continue du signal (contrairement à TH-CDMA) à bande large dans la bande de fréquence entière (contrairement à FH-CDMA). DS-CDMA est utilisé par exemple pour IS-95 et pour le système par satellite Global START. Le système 3G UMTS est basé sur DS-CDMA. Dans l'émetteur l'information binaire de l'usager est jointe avec le code d'étalement produit par générateur de code. Ce processus se nomme le spreading (étalement).

Avantage :

Le principe CDMA possède beaucoup de points qui peuvent avoir des effets positifs pour la transmission d'informations.

- La transmission codée et la faible concentration en information des signaux CDMA étaient particulièrement importantes pour les applications militaires. Un signal transmis peut être désétaler, et les données sont régénérées seulement si le récepteur a le code d'expansion correct. La basse concentration de l'information permet à l'information d'être transmise discrètement. Les signaux utiles sont cachés dans le bruit de fond.
- Le niveau élevé de la stabilité de la transmission d'informations à large bande (contre les effets du bruit de fond à bande étroite) est extrêmement important pour l'utilisation militaire et civile.

Inconvénients :

- Effet Near-Far nécessite de contrôler la puissance du récepteur pour chaque utilisateur.
- Affaiblissement de la performance aux canaux à trajet multiple.

❖ **SDMA (Space division Multiple Access) :**

Si on considère les trois techniques actuelles d'accès multiple (par répartition fréquentielle, par répartition temporelle et par répartition de code), on constate que seule la dimension spatiale n'est pas prise en compte, du moins explicitement. En effet, l'agencement cellulaire, voire la sectorisation des antennes de certaines stations de base, est en fait une manière, primitive certes, de faire de l'accès multiple par répartition spatiale SDMA.

Le problème posé par le SDMA peut s'énoncer de la manière suivante : "*Nous voulons séparer plusieurs utilisateurs émettant à la même fréquence, en même temps et sans étalement de spectre, en fonction de l'endroit où ils se trouvent.*" L'objectif du SDMA étant clairement d'augmenter la capacité du réseau radio mobile en investissant au mieux la dimension spatiale. Le schéma de la figure II.3 montre trois utilisateurs servis par SDMA à l'aide du même canal dans la cellule [3].

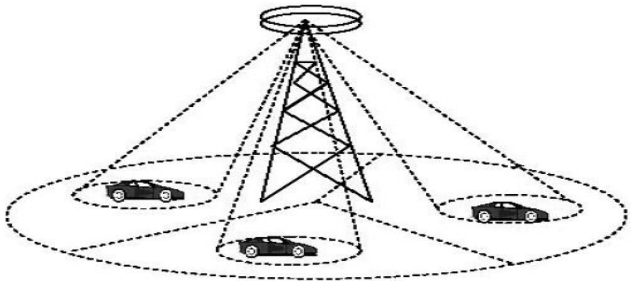


Figure 11. Technique d'accès multiple SDMA.

3. L'étalement de spectre :

3.1. Principe de l'étalement de spectre :

L'étalement de spectre est une technique qui permet de transmettre un signal d'information sur une largeur de bande plusieurs fois supérieure à la largeur de la bande du signal transmettre à demande.

Dans un système à étalement de spectre, le signal transmis est étalé à partir d'un code indépendant du message d'information. Après s'être synchronisé avec l'émetteur, le récepteur doit utiliser ce même code pour désétaler le signal et pouvoir par la suite récupérer le message d'information [4].

3.2. Principe du désétalement :

Le principe de désétalement est similaire à celui de l'étalement. Pour récupérer le signal en bande, il suffit de multiplier le signal reçu par le code qui a été précédemment utilisé pour l'étalement.

En multipliant le signal reçu par le code, on étale les brouilleurs dus au canal, non corrélés au signal utile. Ceci permet de diminuer le niveau du bruit du signal en bande de base [4].

3.3. Etalement du spectre à séquence directe (DS) :

3.3.1. Modèle de base :

L'étalement de spectre en séquence directe se fait par la multiplication de l'information à transmettre de débit Rb par un code pseudo-aléatoire, aussi appelé signature, ayant un débit Rc. On a : N = Rc /Rb = Tb/Tc

Où $Tb = 1/Rb$ est la durée d'un bit d'information et $Tc = 1/Rc$ est la durée d'une impulsion rectangulaire du code, appelée chip. N est habituellement un entier, supérieur à 1 puisqu'il mesure l'étalement du spectre et représente le nombre de chips par bit d'information.

On appelle également ce rapport gain de traitement (*processing gain*). En ce sens, il représente une mesure de la résistance à l'interférence et au brouillage intentionnel obtenue en augmentant la largeur de bande du signal transmis. La figure 4 présente un schéma général d'un système à étalement de spectre en séquence directe.

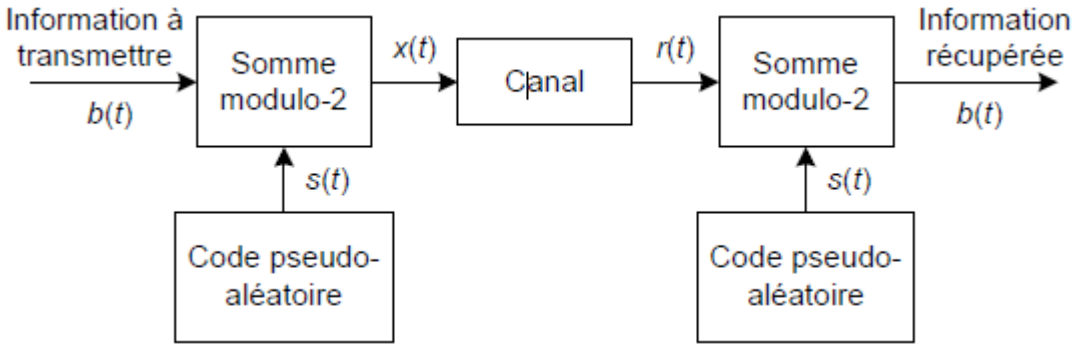


Figure 12. Schéma général d'un système à étalement de spectre en séquence directe.

La figure 5 montre un exemple de signaux *b*(*t*), *s*(*t*) et *x*(*t*) en bande de base tels que définis à la figure 3 et permet d'illustrer le principe d'étalement de spectre et de produit des signaux lorsque *b*(*t*) est modulé par déplacement de phase bivalente (BPSK). On peut remarquer que le signal transmis *x*(*t*) est égal au code *s*(*t*) lorsque *b*(*t*) vaut +1 alors qu'il est égal à -*s*(*t*) lorsque *b*(*t*) vaut -1.

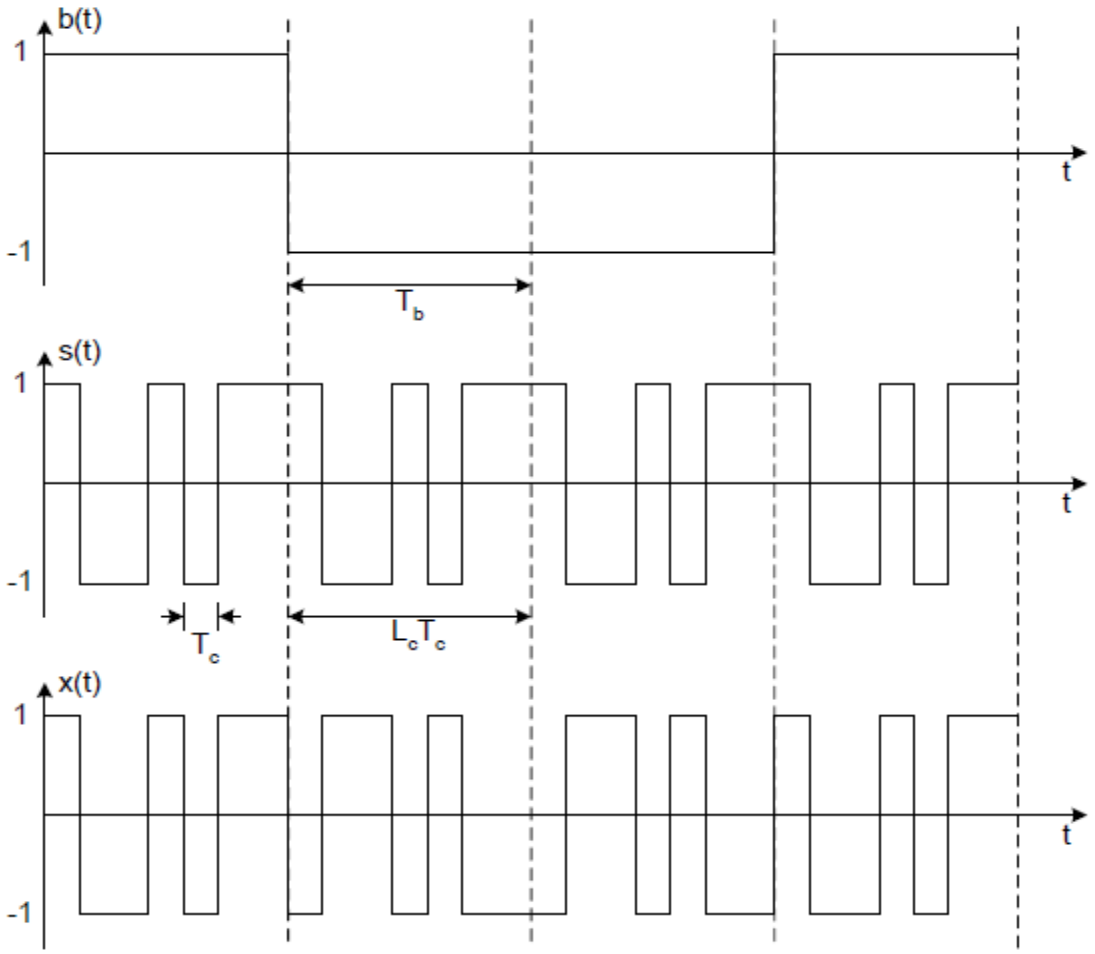


Figure 13. Exemple de signaux b(t), s(t) et x(t).

3.3.2. Principe spectral :

Du point de vue spectral, la multiplication des données avec la séquence de code produit un étalement du spectre du signal transmis, Figure 15a. Si on suppose un canal simple ne comportant que du bruit thermique et une source d'interférence à bande étroite, le signal reçu par le récepteur sera donc composé de trois éléments, Figure 15b, soit le signal transmis étalé (en bleu), le bruit thermique (en vert) et l'interférence à bande étroite (en rouge). En multipliant une nouvelle fois par le code lors de la réception, le signal désiré est désétalé. Le spectre du bruit thermique demeure intouché par la multiplication par le code, c'est-à-dire qu'il n'est ni étalé ni comprimé.

L'interférence à bande étroite, par contre, subit une première multiplication par le code lors de la réception, ce qui cause un étalement et réduit considérablement son impact sur le signal désiré, voir Figure 15c.

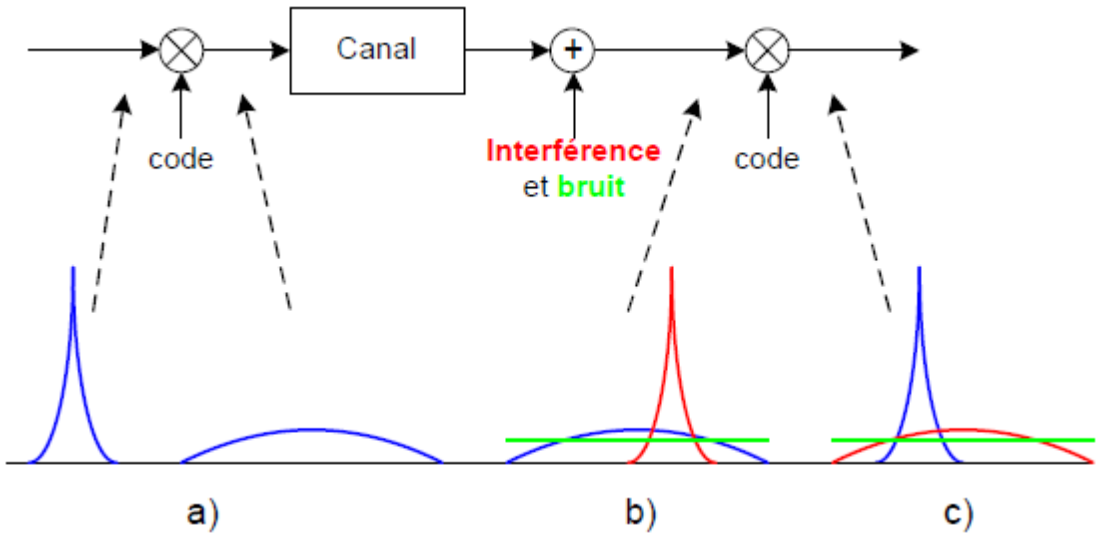


Figure 14. Représentation fréquentielle du principe d'étalement spectral.

3.4. Avantage et inconvénient :

Comme nous l'avons vu, la technique de l'étalement de spectre consiste à moduler le signal contenant l'information puis a l'étaler de manière à ce que le spectre du signal émis occupe une bande de fréquence très supérieure à celle nécessaire à la transmission de l'information. L'étalement de spectre, par rapport aux modulations a bande étroite, présente de nombreux avantages :

- bonne résistance aux perturbations bande étroite :

Lors de l'émission des perturbations bande étroite peuvent s'ajouter au signal étalé. Le récepteur réalise l'opération inverse de l'étalement. Le signal étalé est ainsi transforme en signal bande étroite alors que les perturbations a bande étroite sont étalées. De cette façon, la puissance des perturbations devient négligeable devant celle du signal utile reconstitue, voir Figure (5).

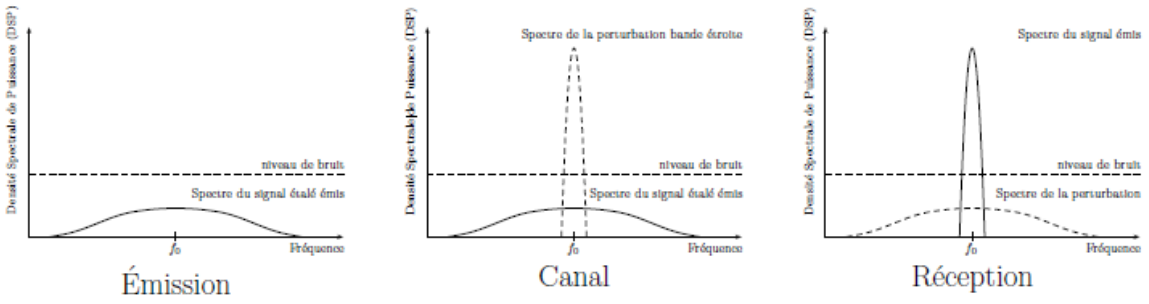


Figure 15. Exemple d'émission avec une perturbation bande étroite.

- faible brouillage des émissions classiques a bande étroite :

Les signaux a bande étroite peuvent cohabiter sur la même bande de fréquence que ceux génères par un système a étalements de spectre, sans perturber de façon importante un système par rapport à l'autre. La puissance de ces signaux est étalée sur une bande de fréquence importante. Leur densité spectrale de puissance est donc très faible comparée à celle des signaux a bande étroite.

- insensibilité aux effets des trajets multiples :

Contrairement aux transmissions bande étroite, l'étalement de spectre permet de lutter efficacement contre l'effet des trajets multiples de propagation. Les creux de Fading [26] résultant de ces trajets multiples peuvent absorber complétement le spectre d'une modulation bande étroite. Dans le cas d'une modulation large bande, sous réserve que cette bande soit supérieure a la bande de cohérence du canal radio, seule une partie du signal disparait.

- faible probabilité d'interception :

Le signal ayant les caractéristiques d'un bruit aléatoire dont le niveau peut être inférieur à celui du bruit thermique, la communication est difficilement détectable. De plus, si le signal était détecte, seuls les récepteurs possédant les paramètres de la séquence d'étalements pourront accéder à l'information.

- multiplexage et adressage sélectif :

Plusieurs émissions peuvent cohabiter dans la même bande de fréquence dans la mesure où les codes d'étalements relatifs à chacun des signaux sont orthogonaux, c'est à dire dans la mesure où ils présentent un inter corrélation voisine de zéro (code de Hadamard, code de Walsh, code de Gold). La séquence d'étalements à effectuer à chaque signal constitue sa clé de codage. Ce signal ne peut être exploite que si le récepteur possède la même clé de codage. Cette propriété se nomme l'Accès Multiple à Répartition par les séquences d'étalements, appellation que l'on trouve dans la littérature anglo-saxonne sous le terme CDMA (Code Division Multiple Access).

Quelques inconvénients sont liés à cette technique :

- encombrement spectral important qui rend souvent l'attribution de fréquences difficile. En effet, le signal a toujours la même puissance mais celle-ci est repartie différemment.
- complexité accrue des systèmes qui rend leur coût plus élevé par rapport à celui des systèmes bande étroite.
- nécessite d'avoir de bonnes méthodes de synchronisation permettant, à la réception, de reconstruire le signal émis.

Ce type d'émetteur-récepteur, utilisant l'étalement de spectre, est principalement utilise dans les systèmes CDMA, c'est à dire dans un environnement multi-utilisateurs. Il se distingue aussi d'autres systèmes, comme le MBOK Mary Bi-Orthogonal Keying) et le CCK (Complementary Code Keying), qui sont contraints de fonctionner simplement en mono-utilisateur pour avoir des performances optimales.

4. Les codes d'étalement :

Le choix des codes d'étalement est directement influencé par leurs propriétés d'autocorrélation et d'inter corrélation. Dans un contexte d'accès multiple, les codes doivent posséder des propriétés particulières :

- pour éviter les interférences causées par les trajets multiples, ils doivent être le plus faiblement auto corrélés.

$$\mathbf{R_{Ci}(\tau) = \sum_{k=0}^{M-1-\tau} Ci(k).\, Ci(k+\tau) = 0} \qquad \text{Pour } \tau \neq 0 \qquad (1)$$

- Afin d'assurer la sécurité et éviter le brouillage des sources entre elles, les codes doivent être le plus faiblement inter corrélés.

$$\mathbf{R_{Ci,Cj}(\tau) = \sum_{k=0}^{M-1-\tau} Ci(k).\, Cj(k+\tau) = 0} \qquad \text{Pour tout } \tau \qquad (2)$$

- Enfin, pour permettre la synchronisation, ils doivent posséder un pic d'autocorrélation le plus étroit possible.

$$\mathbf{R_{Ci}(0) = M} \qquad \text{(M: longueur du code)} \qquad (3)$$

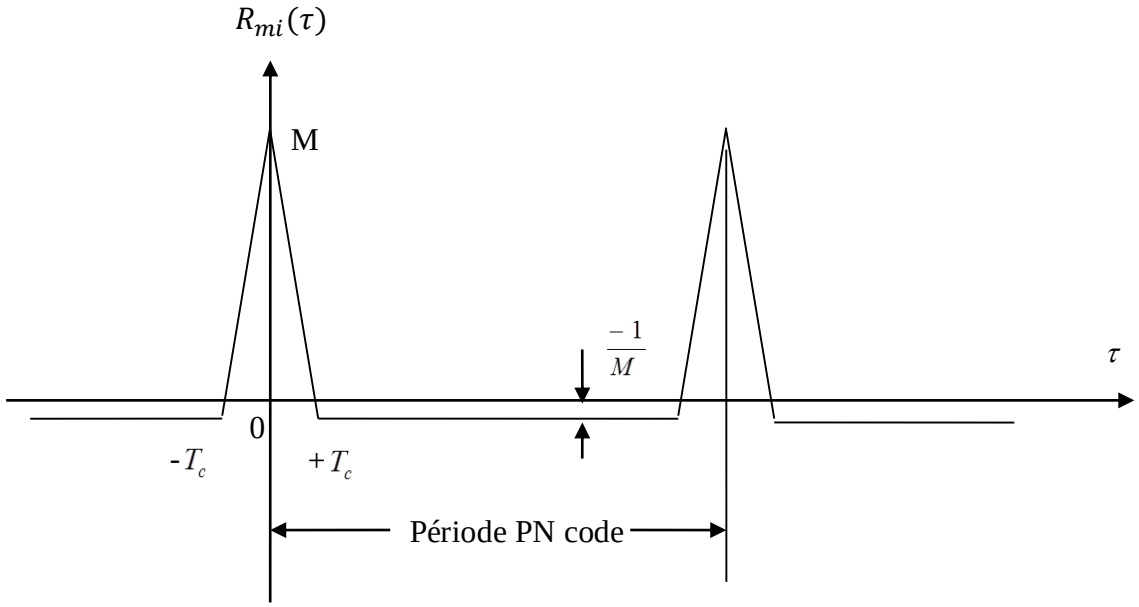


Figure 16. Fonction d'autocorrélation de code d'étalement.

Dans la plus part des systèmes de radiocommunication avec les mobiles fondés sur le DS-CDMA, les codes utilisés pour effectuer l'étalement sont de deux types : codes de Walsh-Hadamard ou orthogonaux et les codes pseudo-aléatoires. [4]

4.1. Codes de Walsh-Hadamard :

Les codes orthogonaux utilisés en DS-CDMA sont choisis d'après les fonctions de Walsh. La manière la plus courante de générer ces codes est d'utiliser les matrices de Hadamard. Ces dernières sont toujours carrées et peuvent être générées de manière récursive.

Il existe plusieurs manières de générer les séquences de Walsh. La génération par des matrices de Hadamard est l'une des plus courantes. Les matrices de Hadamard sont toujours carré et pouvant être générées de manière récursive suivante :

$$\mathbf{H_{2M}} = \begin{bmatrix} \mathbf{H_M} & \mathbf{H_M} \\ \mathbf{H_M} & \mathbf{-H_M} \end{bmatrix} \qquad \text{Avec} \qquad \mathbf{H_1 = [0]} \qquad (4)$$

$$\mathbf{H_2} = \begin{bmatrix} \mathbf{+1} & \mathbf{+1} \\ \mathbf{+1} & \mathbf{-1} \end{bmatrix} \qquad \text{M est une puissance de 2} \qquad (5)$$

Un code de Walsh-Hadamard C_i possède les propriétés suivantes :

- le premier élément de C_i est toujours +1, pour tout i ;
- C_i possède le même nombre de +1 et -1 (excepté C_i) ;
- la fonction d'inter corrélation de deux codes distincts satisfait :

$$\mathbf{R_{Ci,Cj}(\tau) = \sum_{k=0}^{M-1-\tau} Ci(k).Cj(k+\tau) = 0} \qquad \forall\ i \neq j \qquad (7)$$

- la fonction d'autocorrélation $R_{ci}(0)$ du code C_i satisfait :

$$\mathbf{R_{Ci}(0) = \sum_{k=0}^{M-1} Ci(k).Cj(k) = M} \qquad (8)$$

4.2. Codes orthogonaux de longueur variable (OVSF) :

Ils viennent d'une famille de codes orthogonaux au sens de la corrélation. Ils peuvent être définis par un arbre générateur tel qu'une racine engendre deux branches.

Le code d'une branche est composé par le code de la racine et de son complémentaire.

N détermine simultanément la longueur du code mais également le nombre de codes disponibles pour un étalement donné.

Pour l'utilisation de ces codes il faut respecter certaines règles. Au sein d'une même cellule, les codes OVSF de la figure II.6 ne peuvent pas être utilisés simultanément car ils ne sont pas tous orthogonaux entre eux. En effet, le code d'une branche est fortement lié à celui de sa racine. Une règle d'utilisation de ces codes est définie :

Lorsqu'un code est alloué, tous les codes issus de ces branches ne peuvent être utilisés.

Cette règle apporte une contrainte forte sur la disponibilité dans les canaux à haut débit [4].

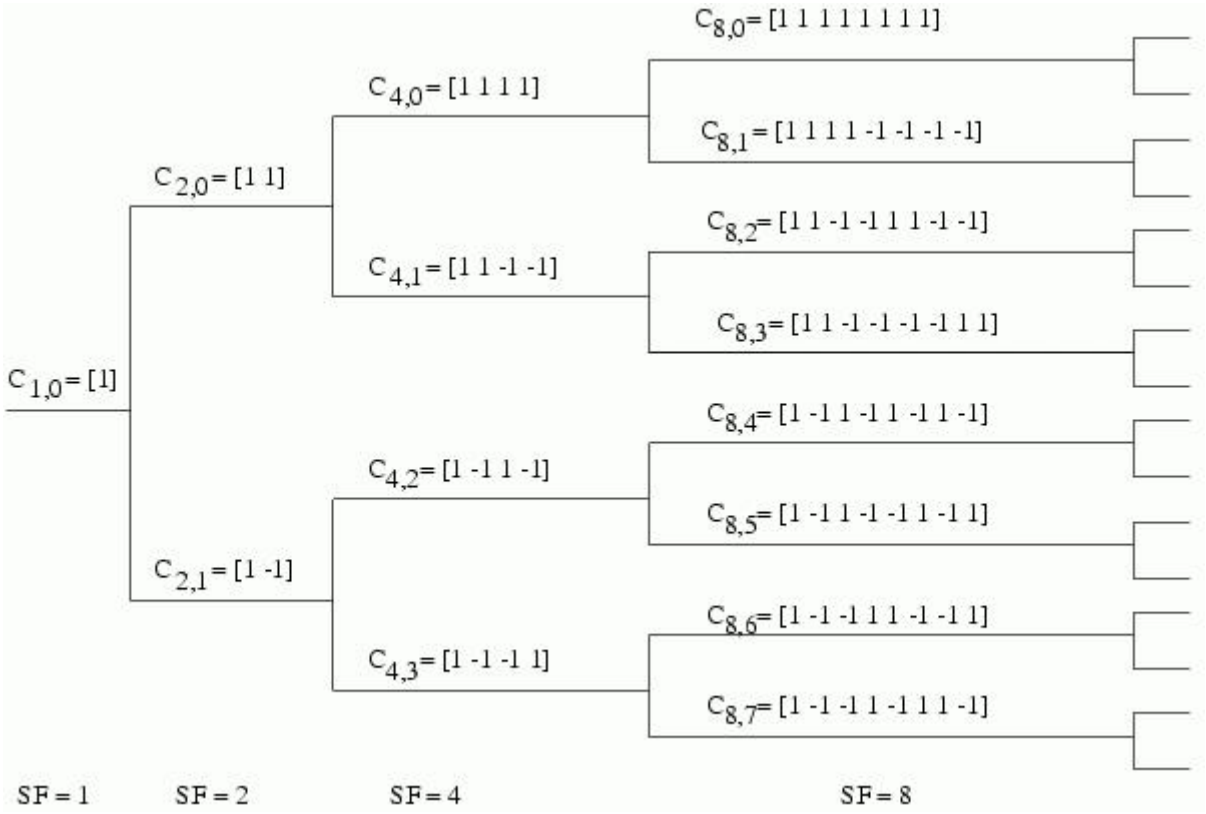


Figure 17. Le code OVSF.

4.3. Séquences de longueur maximale (m-séquence) :

LFSR générateurs produisent ce qu'on appelle des suites récurrentes linéaires (LRS), car toutes les opérations sont linéaires. D'une manière générale, la longueur de la séquence avant la répétition se produit dépend de deux facteurs, les robinets de rétroaction et l'état initial. Un LFSR de toute taille m donné (nombre de registres) est capable de produire chaque état possible pendant la période N = 2m-1 changements, mais ne le fera que si les robinets de rétroaction appropriés ont été choisis. Par exemple, une telle LFSR stade huit contiendra toutes les combinaisons possibles de uns et de zéros après 255 quarts de travail. Une telle séquence est appelée une séquence maximale de longueur, séquence maximale, ou, moins fréquemment, séquence de longueur maximale. Il est souvent abrégé en séquence m.

Dans certaines industries séquences m sont désignés comme pseudo bruit (PN) ou pseudo séquences, en raison de leurs caractéristiques optimales de type bruit. (Officieusement, même des séquences non maximales sont souvent appelés pseudo aléatoires ou pseudo aléatoires séquences.)

Techniquement parlant, les générateurs de longueur maximale peuvent réellement produire deux séquences. La première celle trivial a une longueur d'un, et se produit lorsque l'état initial du générateur est réglé à zéro. (Le générateur reste simplement dans l'état zéro

indéfiniment.) L'autre l'une utile a une longueur de 2m1. Ensemble, ces deux séquences représentent tous deux m états d'un registre de m bits Etat.

Lorsque les robinets de rétroaction d'un LFSR sont non maximaux, la longueur de la séquence générée dépend de l'état initial du LFSR. Un générateur non maximal est capable de produire deux ou plusieurs séquences uniques (plus trivial tout à zéro une), à l'état initial de déterminer qui est produite. Chacune de ces séquences est appelé un espace d'état du générateur. Ensemble, chaque séquence non maximale du générateur peut produire des comptes pour tous les 2 m états d'un registre de m bits Etat.

Les propriétés des séquences non maximales sont généralement inférieures à celles des séquences maximum. Ainsi, l'utilisation de séquences Non-maximaux dans les systèmes réels est généralement évitée en faveur de leurs homologues de longueur maximale.

4.3.1. Propriétés des m-séquence :

Il résulte de leur définition que les m-séquences présentent les propriétés suivantes :

- La période de la séquence est égale à : N=2R-1.
- Le OU EXCLUSIF (équivalent à une somme modulo 2) entre une M-séquence avec une version décalée de celle-ci (0 < décalage < N) donne une autre version de cette même M-séquence.

Soit par exemple le registre à décalage de la figure suivante :

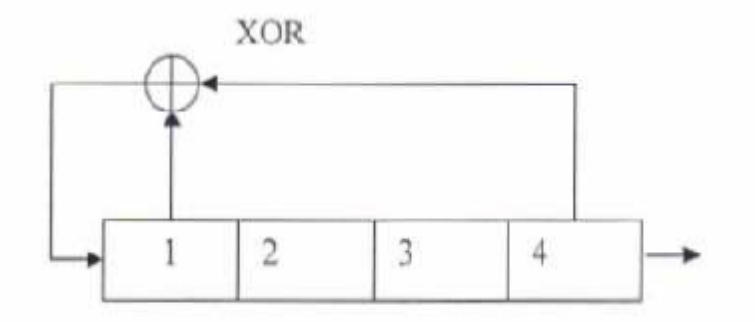


Figure 18. Registre à décalage LSFR [4 1].

Période : N =15. Décalage = 6

La séquence générée s'écrit : $b(n)$: 111101011001000

La séquence décalée s'écrit : $b\ (n+6)$: 011001000111101

La nouvelle séquence s'écrit : $b(n)$ XOR $b(n+6)$: 100100011110101

Cette nouvelle séquence est bien une autre version de la séquence $b(n)$.

- Une séquence à longueur maximale comporte $(N-1)/2$ fois la valeur "0" et $(N+1)/2$ fois la valeur "1". I1 y a donc un "1" de plus que de "0".
- Si un registre à décalage génère une ML séquence, le registre inverse génère lui aussi une M-séquence qui est inversée, c'est-à-dire que si le registre à R étages comporte des prises de retour sur les étages R, P, Q et génère une séquence. *bi, bi-1, bi-2*, … alors le registre inverse doit posséder des prises de retour sur 1es étages R, P, Q et la séquence générée devient … *bi-2, bi-1, bi.*

Exemple avec R=5 :

[5,2] : 00110100100001010111011000111111

[5,3] : 11111000110111010100001001011100

- Le registre décalage passe par toutes les combinaisons possibles de "1" et de "0" sauf la combinaison [00000…0000] qui est interdite car c'est une combinaison de blocage.
- Le nombre de prises doit être pair. C'est à dire que le nombre de coefficients *hk* égaux à 1 doit être pair. Si le nombre de prises est impair, la combinaison [11…11] est interdite car c'est une combinaison de blocage.

4.3.2. Propriétés de distribution des m-séquences :

Dans cette section, nous étudions la distribution des états des m-séquences, c'est à dire le nombre d'apparition des déférents bits constituant la séquence et leur disposition.

Une séquence pseudo-aléatoire doit à la fois paraître aléatoire tout en obéissant à des propriétés très fortes sur la distribution de ses bits. C'est un paradoxe exigé par les applications des séquences aux déférents domaines scientifiques et techniques (simulation informatique, intégration de Monte Carlo, radar, cryptographie. . .). Golomb a posé trois grands postulats d'altérité :

- la propriété de l'équilibre (balanced property),
- la propriété des séries (run properties) et
- une autocorrélation idéale.

Ces trois postulats paraissent minimes et pourtant il est étonnant de constater que rares sont les familles de séquences vérifiant ces trois postulats. Les m-séquences font parties des familles de séquences vérifiant les trois grands postulats de Golomb.

Les séquences d'étalement construites à partir de séquences à longueur maximale possèdent une fonction d'autocorrélation qui présente un fort pic de corrélation. Cette propriété est utilisée dans les démodulateurs pour assurer des fonctions de synchronisation.

4.4. Les codes de Gold :

Il est souhaitable d'obtenir un ensemble plus important de séquences de longueur N = 2n-1 et dont les niveaux d'inter-corrélation ne dépassent pas t(n)=1+2[(n+2)/2] où [α] désigne la partie entière du réel α. Les codes de Gold sont une catégorie importante de séquences générant un ensemble de codes ayant de bonnes propriétés d'inter-corrélation.

Les séquences de Gold sont une famille de codes qui découle des séquences PN. Elles sont particulièrement employées dans les structures CDMA dites "non-orthogonales" compte tenu de leurs propriétés de corrélation.

- Principe de génération des codes de Gold

Soit t(n)=1+2[(n+2)/2, avec [α] indiquant la partie entière du réel α. Si *n≠0 mod4*, il existe des paires de *m*-séquences qui ne possèdent que trois pics d'inter-corrélation de valeur -1, *-t(n)* et *t(n)-2*. Les paires de *m*-séquences vérifiant ce critère sont dites "*m*-séquences préférées".

Un ensemble de séquences de Gold de période $N = 2n-1$ consiste en $N+2$ séquences dont les corrélations *AC* et *CC* sont égales à *t(n)*. Cet ensemble peut être construit à partir de m-séquences dites "préférées".

Soit $u = \{ui\}$ et $v = \{vi\}$ deux *m*-séquences "préférées" de longueur *N=2n-1*. L'ensemble des codes de Gold issues de ces deux séquences est alors :

$$\mathbf{G(u,v) = u, v, u \oplus v, u \oplus Tv, v \oplus T^2 v \ldots, u \oplus \tau^{N-1} v} \qquad (9)$$

où *T* est un opérateur de décalage tel que u=(a0,a1,a2,……,aN-1), Tu=(a1,a2,…...aN-1a0), T2u=(a2,…,aN-1 a0 a1)

G (u.v.) contient *N+2 = 2 n +1* séquences de période *N*.

Soit *f(x) = h(x)h'(x)* où *h(x) et h'(x)* n'ont aucun facteur en commun et où le plus grand commun diviseur (PGCD) vaut 1. L'ensemble des séquences générées *par f(x)* est de forme *a*E*b* où *a* est une séquence générée par *h(x)* et *b* une séquence générée par *h'(x).* Dans le cas où *a* et *b* sont des m-séquences "préférées".

Les codes de Gold *G (u.v.)* peuvent aussi être générés en additionnant modulo 2, terme à terme, les sorties des registres à décalage correspondant à *h(x) et h'(x).*

L'exemple qui suit montre comment un ensemble de séquences de Gold est généré :

$$\begin{cases} h(x) = X3 + X + 1 \\ h'X = X3 + X2 + 1 \end{cases}$$

Avec des états initiaux 100 et 111, les séquences *h(x)* et *h'(x)* génèrent respectivement les *m-séquences* "préférées» :

$$\begin{cases} 0011101 \\ 1110010 \end{cases}$$

En configurant le générateur de séquences de Gold, comme le montre la *Figure 8*, il en résulte les séquences données par le Tableau 3.

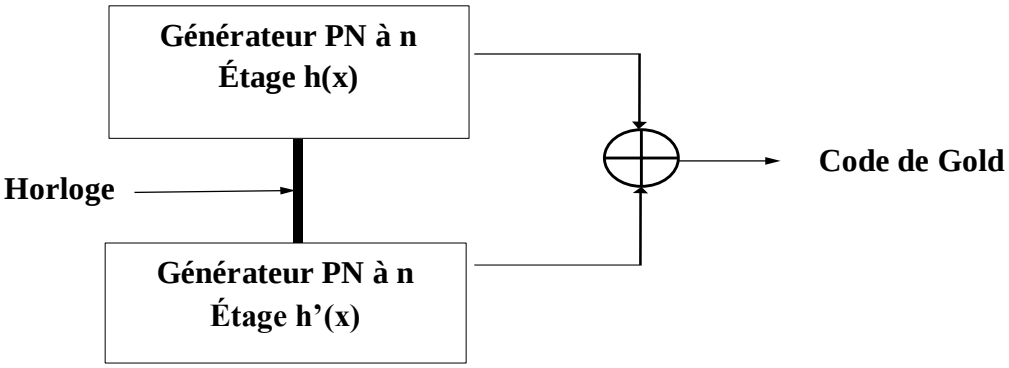


Figure 19. Générateur de séquences de Gold.

Tableau 3. Exemple de 9 codes de Gold.

G1= 0011101	G2= 1110010
G3= 1101111	G4= 0100100
G5= 1000001	G6= 0110011
G7= 0001011	G8= 1010110
G9= 1111000	

Le tableau ci-dessous montre une liste de paires préférées :

Tableau 4. Exemple de liste des paires préférées.

n	N	Polynôme préféré 1	Polynôme préféré 2
5	31	$x^5 + x^2 + 1$	$x^5 + x^4 + x^3 + x^2 + 1$
6	63	$x^6 + x + 1$	$x^6 + x^5 + x^2 + x + 1$
7	127	$x^7 + x^3 + 1$	$x^7 + x^3 + x^2 + x + 1$
9	511	$x^9 + x^4 + 1$	$x^9 + x^6 + x^4 + x^3 + 1$
10	1023	$x^{10} + x^3 + 1$	$x^{10} + x^8 + x^3 + x^2 + 1$
11	2047	$x^{11} + x^2 + 1$	$x^{11} + x^8 + x^5 + x^2 + 1$

Ces couples sont appelées des "paires préférées". Pour générer des séquences de Gold, la recherche de ces paires préférées est indispensable.

Voici une caractéristique des séquences de Gold :

Tableau 5. Paires préférées et valeur maximale de l'inter-corrélation.

R (registre)	3	4	5	6	7	8	9	10	11	12	13	14
N (période)	7	15	31	63	127	255	511	1023	2047	4095	8191	16383
Nombre des paires préférés	2	0	3	2	6	-	2	3	4	-	4	3

Nombres des séquences de Gold	18	0	99	130	774	-	1026	3075	8196	-	32772	49155
Inter corrélation	5	9	9	17	17	33	33	65	65	129	129	257

Gold a aussi montré que l'inter-corrélation entre deux séquences peut prendre trois valeurs possibles avec une certaine probabilité connue.

Tableau 6. Propriétés des codes de Gold.

R (longueur du registre)	L (longueur du code)	Valeur de l'inter corrélation normalisée	Fréquence d'occurrence
R Impair	$2^R - 1$	$-1/L$ $-(2(R+1)/2 + 1)/L$ $-(2(R+1)/2 - 1)/L$	Voisine de 0.5 Voisine de 0.25 Voisine de 0.25
R pair non divisible par 4	$2^R - 1$	$-1/L$ $-(2(R+1)/2 + 1)/L$ $-(2(R+1)/2 - 1)/L$	Voisine de 0.75 Voisine de 0.125 Voisine de 0.125

5. Domaine d'application des LFSR :

Il est évidemment impossible d'utiliser la suite produite par un LFSR comme suite chiffrant dans un chiffrement à flot. En effet, si les coefficients du LFSR sont publics (ce qui est généralement le cas quand le LFSR est implémenté sous forme d'un circuit électronique), il suffit à un attaquant qui connaît L bits consécutifs de la suite d'appliquer la relation de récurrence pour retrouver tous les bits suivants. Dans le cas où les coefficients de rétroaction sont secrets, l'algorithme de Berlekamp-Massey permet de les reconstituer, ainsi que l'état initial, à partir de 2L bits de suite chiffrant.

Toutefois, les LFSR sont des dispositifs extrêmement rapides et d'implémentation peu coûteuse pour engendrer des suites ayant de bonnes qualités statistiques, notamment une période élevée. C'est pour cette raison qu'ils sont souvent utilisés comme module de base dans les générateurs pseudo-aléatoires dédiés, mais au sein d'un dispositif plus complexe.

Un problème fondamental en cryptologie est la production de suites de bits « aussi aléatoires que possible ». Un exemple évident étant la génération des clefs de chiffrement (symétrique ou asymétrique).

Ce problème se décompose en fait en deux parties :

- La génération de bits par des procédés physiques, dans le cas d'un ordinateur des mesures liées à l'activité de la machine (températures interne, déplacement de la souris, etc.)
- L'expansion d'une courte suite aléatoire de bits en une suite éventuellement beaucoup plus grande ; Dans ce dernier cas, on parle de suite pseudo-aléatoire.

6. conclusion :

Nous avons présenté dans ce chapitre les différentes techniques des méthodes d'accès multiple en particulier celle utilisant l'étalement de spectre par séquence directe DSSS (Direct Séquence Spread Spectrum), puis nous justifions l'emploi du DSSS dans les systèmes d'accès CDMA.

Dans le chapitre suivant on fait une comparaison de la technique DS-CDMA avec la technique MC-CDMA été présentée sous forme tableau qui donne les caractéristiques principales de différents concepts de DS-CDMA et MC-CDMA et récapitule les avantages principaux et les inconvénients de différents arrangements.

Nous donnons quelques modèles de canaux de transmission qu'on peut rencontrer dans la réalité. Enfin, et pour terminer nous donnerons un aperçu sur quelque principaux travaux publié dans la littérature qui traitent le problème de l'acquisition du codes PN et Gold code

V. Simulation sur Matlab

1. Introduction :

Les programmes informatiques avancés (tels que MATLAB) fournissent des maniéré utile de simuler des systèmes de technologie. Dans notre projet nous avons employée MATLAB pour faire quelque résultat sur le système de DS-CDMA. Pour des systèmes de communication moderne, taux d'erreur sur les bits BER est le paramètre le plus important qui décrit l'exécution du système.

2. Environnement de programmation :

Notre logiciel est implémenté sous un langage de programmation évolué, récent, conçu par la firme MATHWORKS, il s'agit du Matlab version 7.10.0.499(R2010a).

MATLAB pour Matrix Laboratoire, est une application qui a été conçue afin de fournir un environnement de calcul matriciel simple, efficace, interactif, permettant la mise en œuvre des algorithmes développes dans le cadre des projets linpack et eispack. MATLAB est constitué d'un noyau relativement réduit, capable d'interpréter puis d'évaluer les expressions numériques matricielles qui lui sont adressées :

- soit directement au clavier depuis une fenêtre de commande ;
- soit sous forme de séquences d'expressions ou **scripts** enregistrées dans des fichiers texte appelées m-files et exécutées depuis la fenêtre de commande ;
- soit plus rarement sous forme de fichiers binaires appelées mex-files ou fichiers .mex-générés à partir d'un compilateur C ou fortran.

Les simulations ont été réalisées à l'aide de logiciel Matlab et les résultats sont présentés sous forme de graphiques.

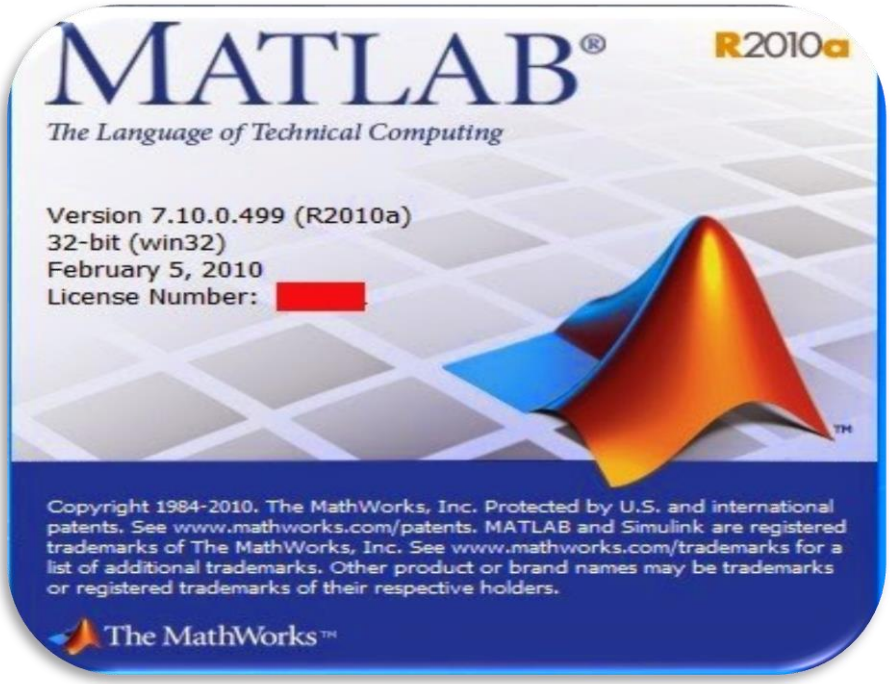


Figure 20. MATLAB R2010a

3. Technique DS-SS (Etalement de Spectre a Séquence Direct) :

3.1. Bloc d'émetteur :

La partie d'Émetteur du programme de Matlab avait trois blocs de base suivant :

1. la Génération du signal de message utilisant la fonction ronde de Matlab qui produit un tableau aléatoire de numéros et les stocke dans une matrice de dimension généreuse.

2. La Génération de Code Gold a l'aide de deux PN (Pseudo Noise) séquence PN1 et PN2.

3. La modulation du signal de message produit dans le bloc 1, avec le Code Gold produit dans le bloc 2 cela pour produire la Bande de Base du signal modulé.

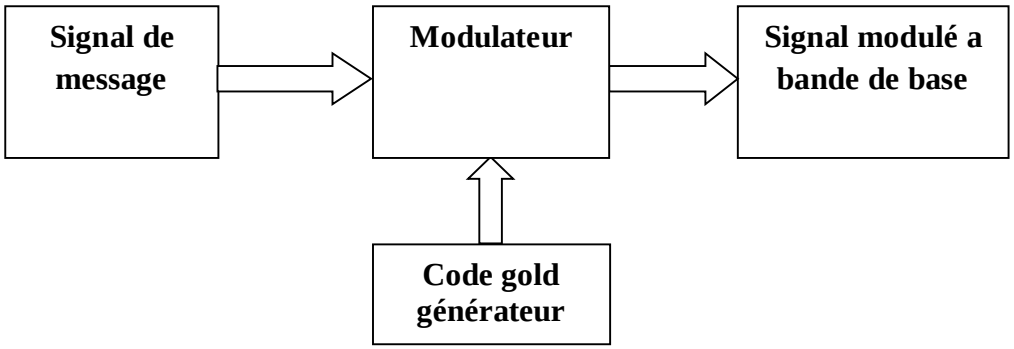


Figure 21. Diagramme Bloc de Transmetteur

3.2. La génération de séquence code Gold :

Les mesures qui ont été suivies pour générer le gold code sont les suivants :

Deux générations de séquences de code gold.

Les mesures qui ont été suivies pour générer le gold code sont les suivants :

Deux PN séquences PN1 et PN2 sont produites, chacun des 5 bits long par XOR spécifique suivant un modèle prescrit et déplaçant chacun d'eux en permanence.

- Pour le modèle de PN1 opération ou exclusif bit est en prenant PN1= [1, 4] ;
- Pour le modèle de PN2 opération ou exclusif bit est en prenant PN2 = [3 4] ;

Chaque bit de sortie des deux séquences ont été XOR et stocke dans un tableau appelé code gold.

3.3. La modulation du signal de Message avec Gold Code :

l'idée de base derrière la modulation était que nous devons remplacer chaque 0 dans le signal de message de 4 bits avec le Code Gold Original et chaque 1 dans le signal de message avec les 4 bits Inversé de Code Gold convertissant ainsi le signal de message de 4 bits dans des 16 (4 x 4) le signal de diffusion bit.

Signal de message :

1 1 0 1

Gold Code :

1 0 0 0

Signal étalé :

0 0 1 0 1 1 0 1 1 1 0 1 1 1 0 1

3.4.Bloc du Récepteur :

Ce que nous faisons dans le récepteur (destinataire) est que nous démodulons simplement le signal étalé reçu avec le Gold Code pour produire le signal de message original. Les étapes pour la Démodulation sont :

- Depuis tous les deux signaux du message original aussi bien que le code gold est 20 bits de longueur, nous XORons chaque 5 bits successifs du signal étalé reçu avec les 5 bits de code gold et stocker le résultat dans un tableau.
- Depuis chaque bloc de 5 de bits des signaux de message consiste en code de Gold ou en code Gold inversé, XORé avec le code de Gold nous donnera un résultat de 0 ou 1.
- Si le résultat est 0, donc nous stockons 0 dans un tableau appelé despreaded_signal et si le résultat est 1, nous stockons 1.
- Le processus est répété pour chaque ensemble de 5 bits jusqu'a que tous les 25 bits du signal reçu soient couverts.
- Le tableau du despreaded_signal nous donne en fin le signal de message original

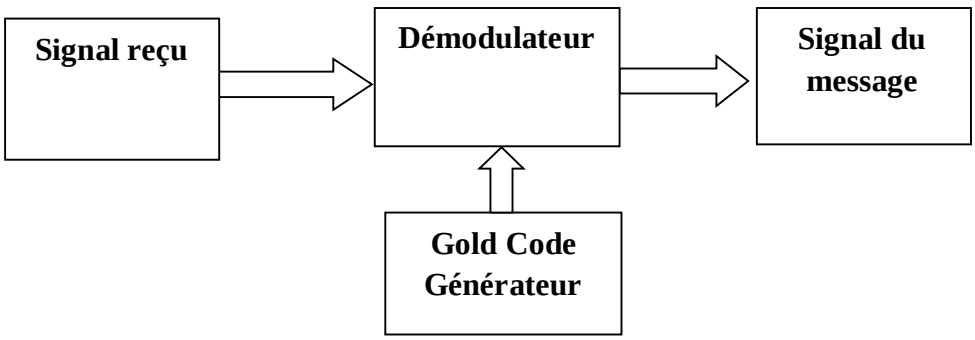


Figure 22. Diagramme Bloc de Récepteur

3.5. Résultat de simulation émetteur et récepteur DSSS :

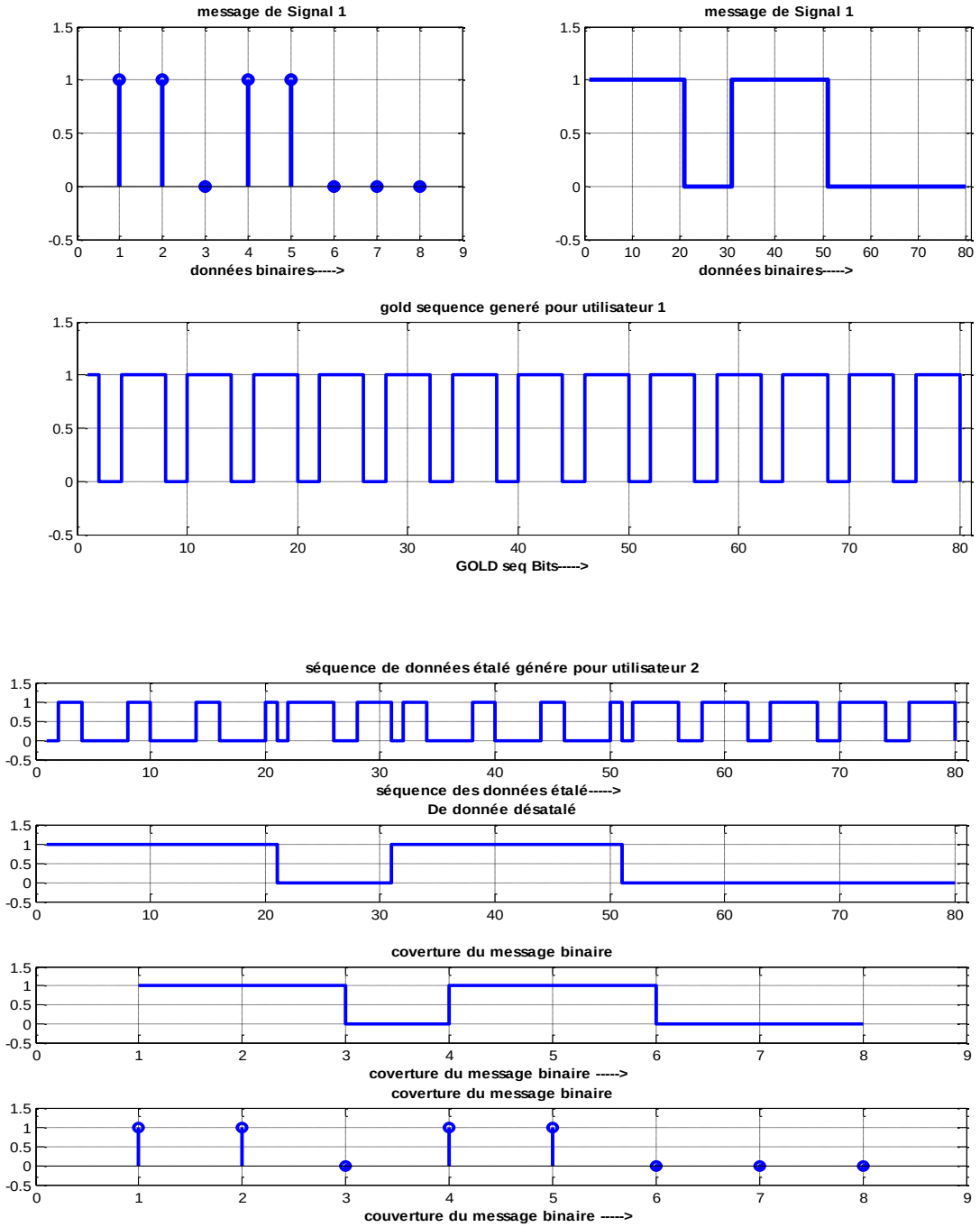


Figure 23. Résultats de simulation émetteur/ récepteur DSSS

(avec gold code de l'ordre 4).

4. Propriété autocréation et inter corrélation :

Corrélation et autocorrélation du Code GOLD et les séquences PN1 et PN2 :

Le tableau énumère la grandeur maximale Rmax pour la corrélation croisée périodiquement entre les paires de m-séquence pour $4<m<5$. Egalement énuméré dans le tableau, est le nombre de m-séquence de la longueur $L=2^m-1$ pour $4<m<5$.

Nous observons que le nombre de ***m-séquence*** de la longueur L augment rapidement avec *m* bits et ainsi nous observons également que pour la plupart des séquences , l'importance maximale Rmax de la fonction de corrélation croisée est un grand pourcentage de la valeur de crête de la fonction d'autocréation (FAC) par conséquent , les m-séquences conviennent aux système de communication CDMA.

Bien qu'il soit possible de choisir un petit sous –ensemble de m-séquence qui ont des valeur de crête de corrélation croisée relativement plus petite que Rmax le nombre de séquence dans l'ensemble est habituellement trop petit pour l'application de CDMA [41].

La méthode pour produire des séquences de PN avec de meilleures propretés périodiques de corrélation croisée que des m-séquences ont été développées par le « Gold ».

Exemples :

m- séquence :

- 1 ère générateur **LFSR** /p(x) $=x^4+x^2+1$
- 2ème générateur **LFSR** /p(x) $= x^4+x^3+1$
- 3ème générateur **LFSR** /p(x) $= x^4+ x + 1$

Séquence de Gold Code :

Les codes Gold sont générés à partir de deux séquences maximales obtenues à partir de *n* bascules, tel que montré à la figure. Ils sont composes de deux générateurs de séquences a longueur maximale qui forment une paire préférée.

- 1 ère générateur LFSR /p(x) $= x^4 + x + 1$
- 2ème générateur LFSR /p(x) $= x^4+x^3+1$

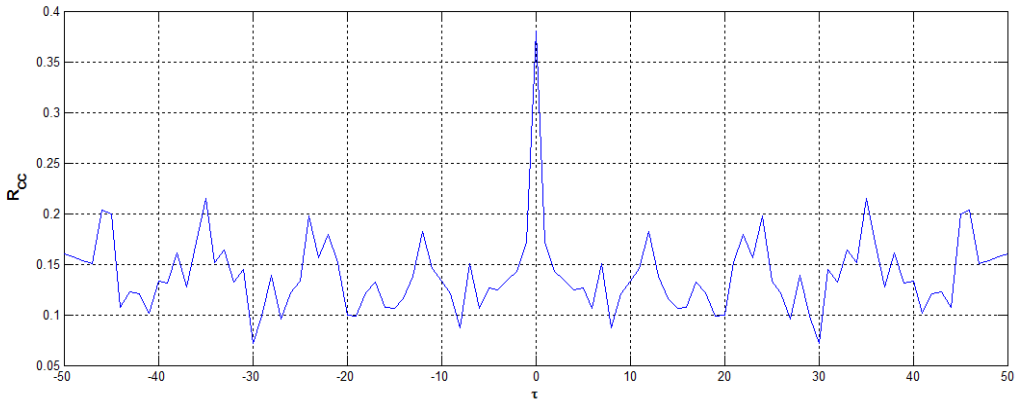


Figure 24. FCC gold code [2 5] et [2 3 4 5]

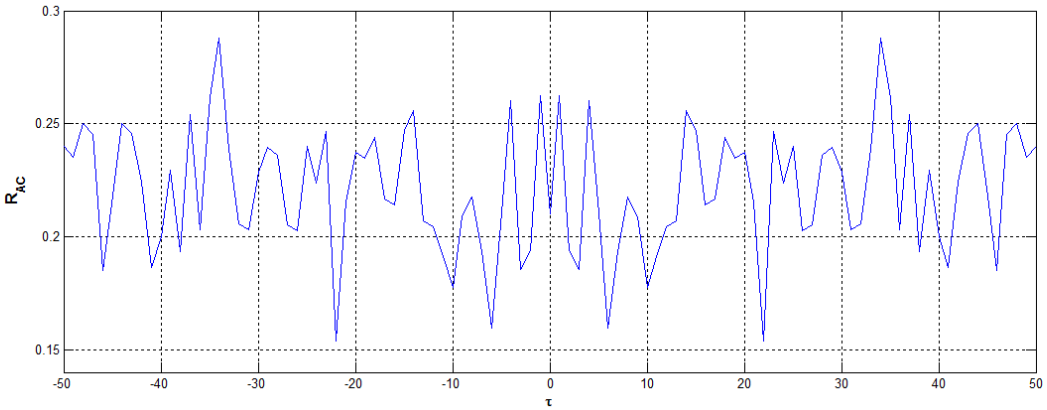


Figure 25. FCC PN code [2 5]

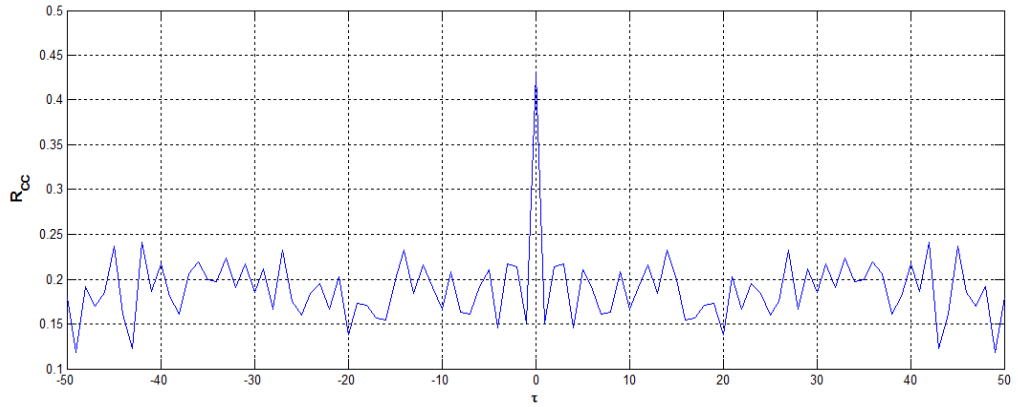


Figure 26. FAC PN code [2 5]

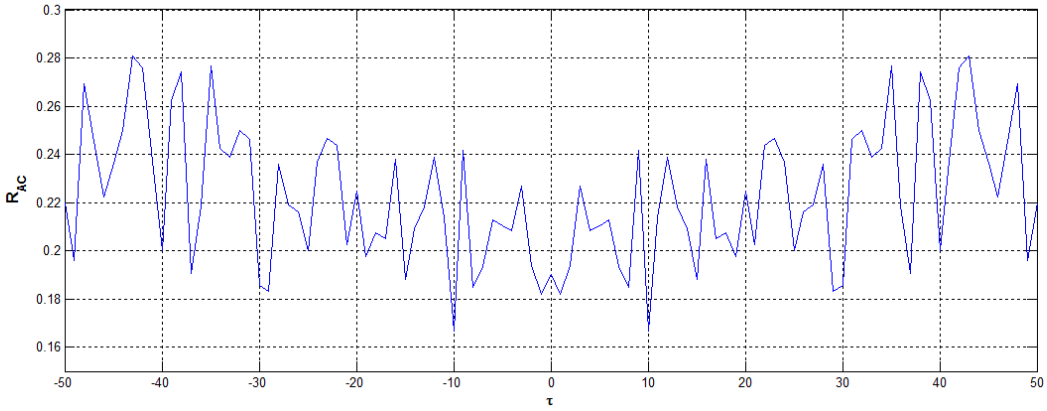


Figure 27. FAC gold code [2 5] and [2 3 4 5]

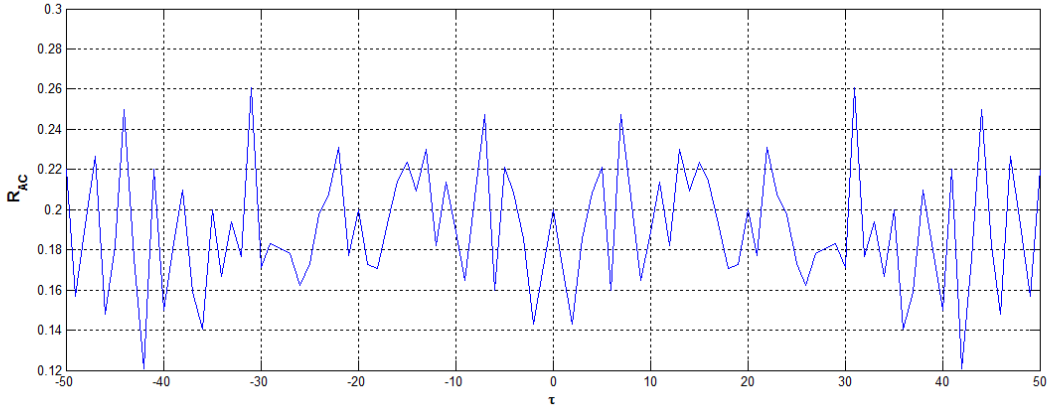


Figure 28. FAC gold code [1 4] and [3 4]

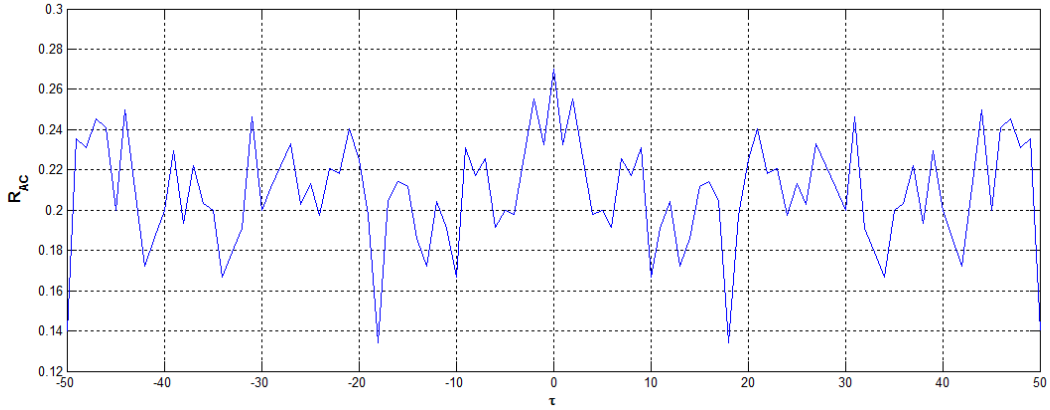


Figure 29. FAC PN code [1 4]

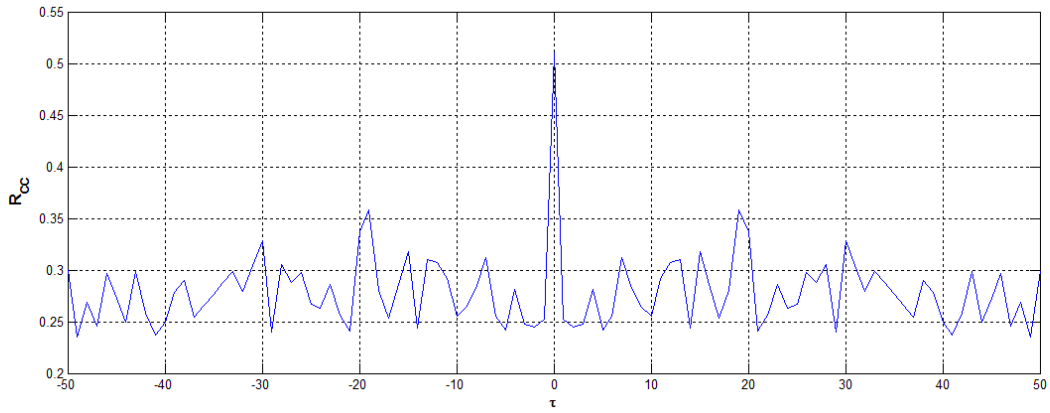


Figure 30. FCC PN code [1 4] [3 4]

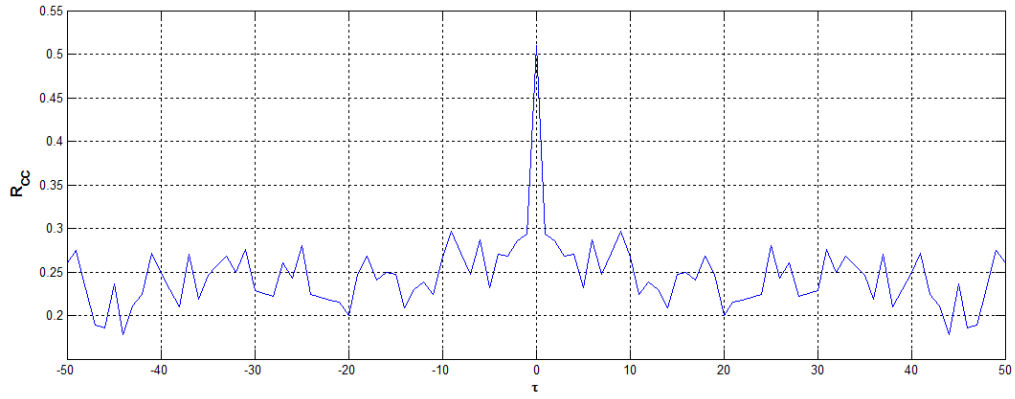


Figure 31. FCC PN code [1 4]

Dans la séquence de propagation la forme d'onde de bande de base du spectre Direct est XORé par séquence PN afin de diffuser le signal. Après la diffusion, le signal est modulé en utilisant binaire déplacement de phase puis transmis comme le montre la figure 13. Le signal émis est représenté par :

$$\mathbf{X(t)} = \left(\frac{\sqrt{\mathbf{2E_b}}}{\mathbf{T_S}}\right)\mathbf{[b(t).c(t)].cos(2\pi f_c + \theta)} \qquad (1)$$

Le démodulateur, le démodulateur BPSK premier signal, le même filtre puis se propage le signal filtré, pour obtenir les données d'origine comme représenté sur la figure 14. Le processus de données d'origine est représentée par : $b(t) = [x(t).\cos(2\pi f_c + \theta).c(t)]$

b(t) est une information binaire. c(t) est PN code d'étalement. fc est la fréquence porteuse. Ts est la durée de symbole de données. θ est la carrière d'angle de phase. Eb est transmise énergie par bit.

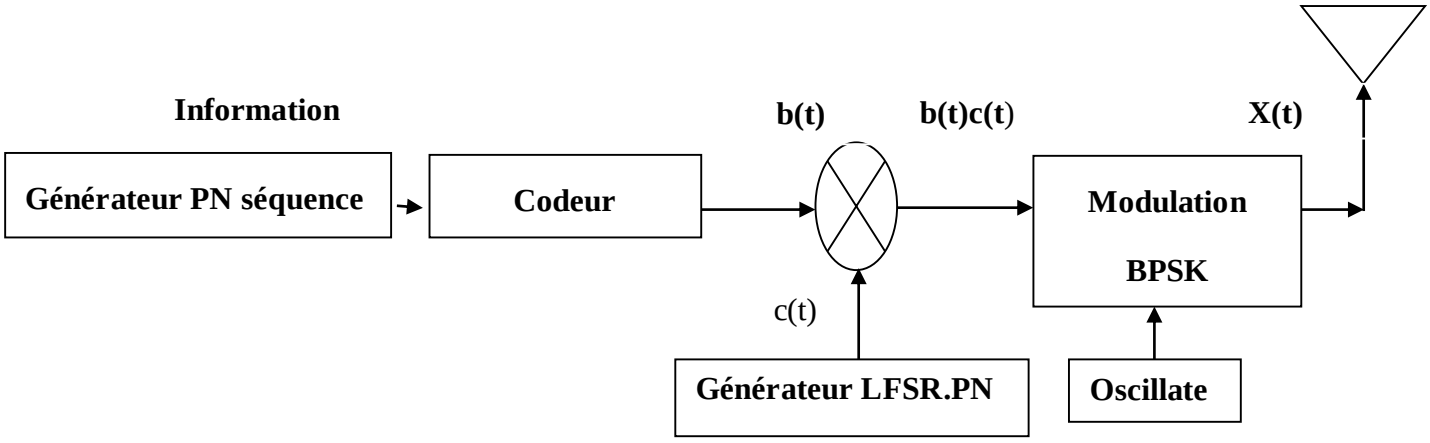


Figure 32. Schéma Emetteur DSSS.

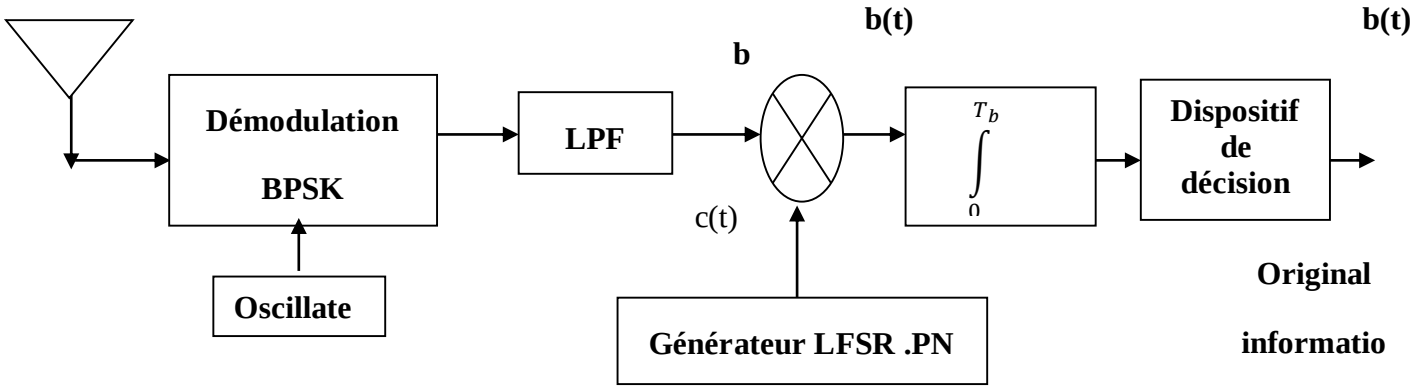


Figure 33. Schéma Récepteur DSSS.

Dans les systèmes CDMA tous les utilisateurs transmettent simultanément dans la même bande de fréquences. Par conséquent, si les utilisateurs "k" sont actifs. La bande de base reçue, le signal continu est une superposition de tous les signaux de k. Le signal de bande de base pour le mode k ème est [15] :

$$\mathbf{X_k(t)} = \sum_{\mathbf{i=0}}^{\infty} \mathbf{b_k(i).\, c_k(t).\, P_k(t - iT_k - \tau_c)} \quad (2)$$

$b_k(i)$ est le signal d'entrée pour l'i^{ième} et k^{ième} utilisateur

$c_k(t)$ est le gain réel de canal positif

$P_k(t)$ est la forme d'onde de signature contenant pour PN séquence

τ_c temp de transmission pour synchrone CDMA $\quad \tau_c = 0$

Signal reçu en bande de base :

$$\mathbf{y(t)} = \sum_{\mathbf{k=1}}^{\mathbf{k}} \mathbf{X_k(t)} + \mathbf{n(t)} \quad (3)$$

K est le nombre d'utilisateurs et n (t) est le complexe du bruit blanc gaussien additif (AWGN).

5. SYSTÈME OFDM :

Système de transmission OFDM est utilisée pour éliminer évanouissement par trajets multiples pour les systèmes de communication multimédia à large bande sans fil (WBMCS). OFDM est basé sur un système de transmission de données parallèle qui réduit les effets de trajets multiples et rend égaliseurs complexes inutiles [3]. En général, les systèmes OFDM sont mis en œuvre en utilisant une combinaison de transformée de Fourier rapide (FFT) et transformée de Fourier inverse (IFFT) blocs qui sont mathématiquement équivalentes des versions DFT et IDFT respectivement [3]. Le schéma de principe de l'émetteur, comme indiqué sur la figure 3.An système OFDM traite les symboles de source, comme se ils se trouvent dans le domaine fréquentiel.

Ces symboles sont transmis à un bloc IFFT qui amène le signal dans le domaine temporel. Si le nombre N de sous-porteuses sont choisies pour le système, les fonctions de base pour la IFFT sont N sinusoïdale de fréquence orthogonale distincte et IFFT recevoir N symboles à la fois. Chacun de n symboles à valeurs complexes d'entrée détermine à la fois l'amplitude et la phase de la sous-porteuse sinusoïdale pour que. La sortie d'IFFT est la somme de tous les n

sinusoïdale et constitue un seul symbole OFDM. La durée du symbole OFDM est NT, où T est la période de symbole d'entrée IFFT. Au bloc-diagramme du récepteur tel que représenté à la figure 4, le FFT schéma fonctionnel effectue le processus inverse sur le signal reçu et le ramène à domaine fréquentiel.

6. SYSTÈME MC CDMA :

En 1993, de nouveaux modèles d'accès multiple basés sur une combinaison de CDMA et multi-porteuse (OFDM) techniques sont proposés, comme multi-porteuse-CDMA (MC-CDMA). [16], [18], [19] Différents utilisateurs transmettent le même ensemble de sous-porteuses, mais avec un code d'étalement qui est orthogonal aux codes des autres usagers. Le signal résultant présente une structure de code orthogonal dans le domaine fréquentiel.

Système multi-porteuse CDMA comme une forme de spectre étalé avec étalement dans le domaine de fréquence que le code d'étalement est fixée au fil du temps en faisant varier la fréquence de sous porteuse. MC-CDMA est une forme de diversité de fréquence. Chaque transporteur a un sous déphasage constant qui forme le code aux utilisateurs distincts.

L'émetteur est essentiellement un système de OFDM avec étalement supplémentaire utilisé par une séquence d'étalement spécifique comme des codes de Walsh, codes Gold, codes PN sont principalement utilisés à l'entrée. Les symboles étalés sont modulés par **MC** modulation par transformée de Fourier rapide (IFFT) opération inverse comme indiqué dans Figure 15. [12], [13] Le récepteur est un récepteur OFDM avec une opération de combinaison supplémentaire pour isoler l'émetteur pour le mode d'intérêt comme le montre la figure 16. en utilisant un intervalle général ; le récepteur sélectionne la partie du signal qui est libre de "ISI". Cet est progressait par un bloc FFT pour démoduler les multiples accès.

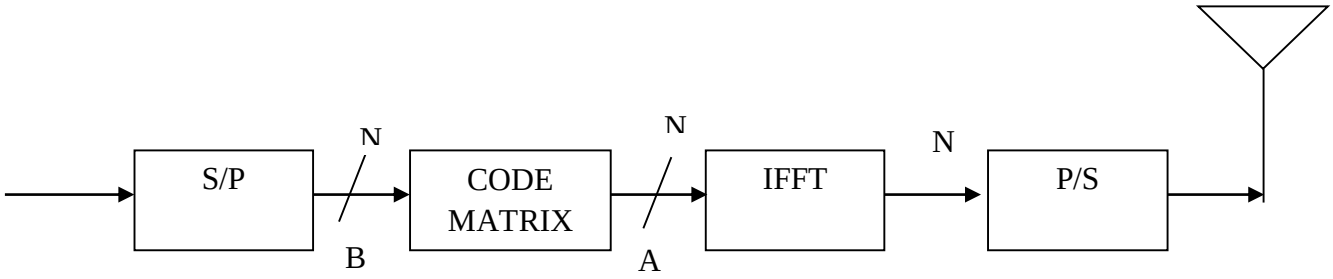


Figure 34. MC CDMA émetteur Schéma.

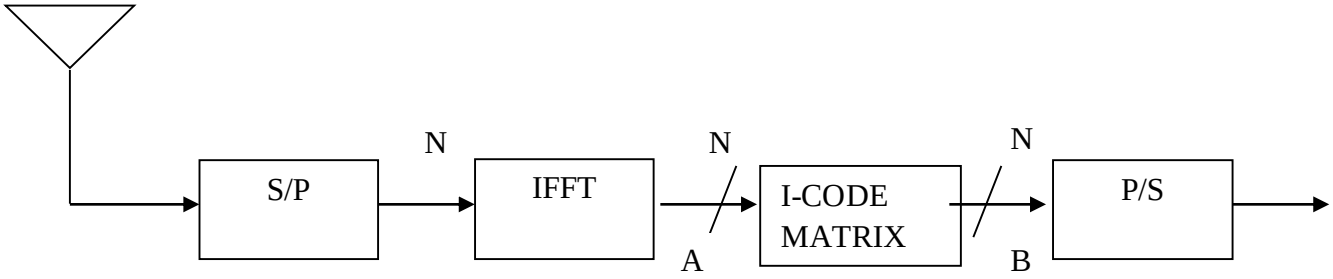


Figure 35. Schéma de bloc récepteur MC CDMA.

MC-CDMA combine les avantages de la technologie CDMA et OFDM contre trajets multiples et le bruit impulsif. [9], [20], [21] Les spécifications de systèmes CDMA différents sont rassemblées sous la forme d'une table, comme indiqué dans le tableau 1.

Tableau 7. SPECIFICATION OF CDMA SYSTEM.

	CDMA-2000/WCDMA	**OFDM**	**MCCDMA**
Receiver	**Rake + MUD**	**Multicarrier Receiver**	**Multiucarrier Receiver**
Chip rate MCPS	**1.024/4.096 8.192/16.384**		**1.2288/3.684**

Carrier Spacing (MHZ)	**1.25, 5, 10,20**	**20MHZ sub Carrier spacing 312.5 KHZ**	**20MHZ sub Carrier spacing 312.5 KHZ**
Frequency lenght ms	**10ms**	**10ms, 20ms,30ms**	**10ms, 20ms,30ms**
Channel coding	**Rate 1/2, 1/3 K=9CC optional RS outer code**	**1/2, 2/3, 3/4 CC**	**Rate 1/2, 1/3 K=9CC optional RS outer code**
Inter leaving	**10ms or more**	**Inter frame**	**Inter leaving Inter frame**
Data	**144Kbps 384Kbps 2Mbps 9.6Kbps**	**6, 9, 12, 18, 24, 32, 48,54 Mb/s**	**Up to 10mbps**
Modulation	**FL : QPSK RL : BQPSK**	**BPSK, QPSK 16QAM,64QAM**	**BPSK, QPSK 16QAM,64QAM**

7. SIMULATION et RÉSULTATS :

La performance Bit Error Rate (BER) du système multi porteuse CDMA en utilisant domaine fréquentiel propagation a été évaluée en utilisant MATLAB et les graphiques obtenus comme indiqué aux figures 7, 8 et 9. Le BER est calculé en fonction de la Signal to Noise (SNR) par bit savoir Eb /N_0, en utilisant les paramètres de *K*= 2 (Nombre d'utilisateurs). La performance des trois codes d'étalement pour savoir MC-CDMA. Codes de Walsh, Gold code et PN séquences de code pour déterminer le système avec le BER moins et interférence d'accès multiple minimum (AMI).

- **Description des paramètres :**

De divers paramètres sous la surveillance constante pendant les simulations sont décrits comme dans le tableau 2.

Tableau 8. Paramètres et descriptions de simulation.

Eb/N0 (dB)	0~20
Nombre des utilisateurs	Deux utilisateurs K=2
Codes d'étalements	Code walsh
	m-sequence : X4+X3+X2+1 ; X4+X2+1
	Gold code : X4+X3+X2+1 ET X4+X2+1
nombre de bit transmis	10^4 bits
Channel noise	AWNG ; Rayleigh
Modulation type	BPSK

- **1ier resultat de simulation pour deux séquenes de méme famille de generateur de l'ordre N=4 :**

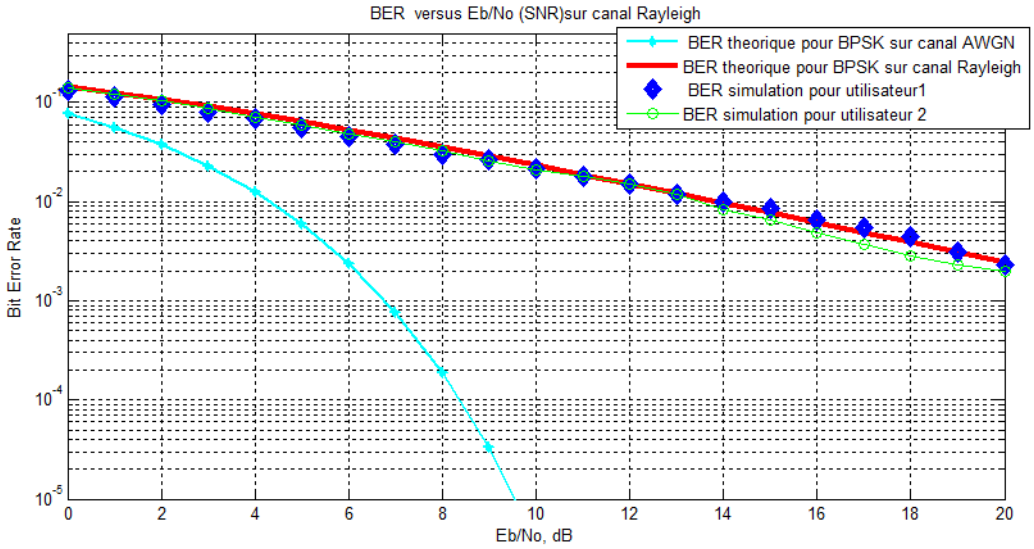


Figure 36. BER versus Eb/no performance CDMA sur canal Rayleigh

avec générateur Walsh code.

- **2ème resultat de semilation pour generateur gold code de lorde N=4 :**

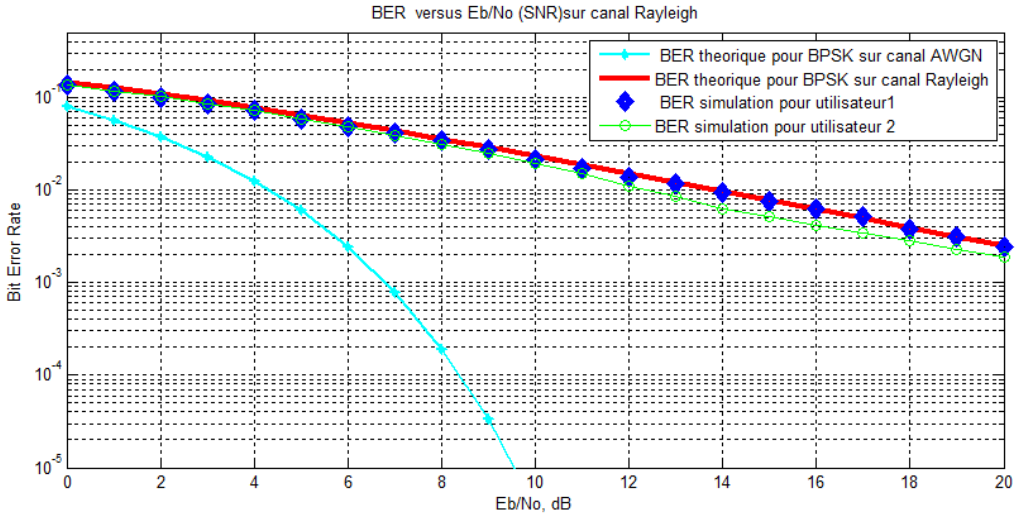


Figure 37. BER versus Eb/no performance CDMA sur canal Rayleigh

avec générateur LFSR de l'ordre 4, polynôme :

X4+X3+X2+1 avec état initial = [1 0 0 1] ;

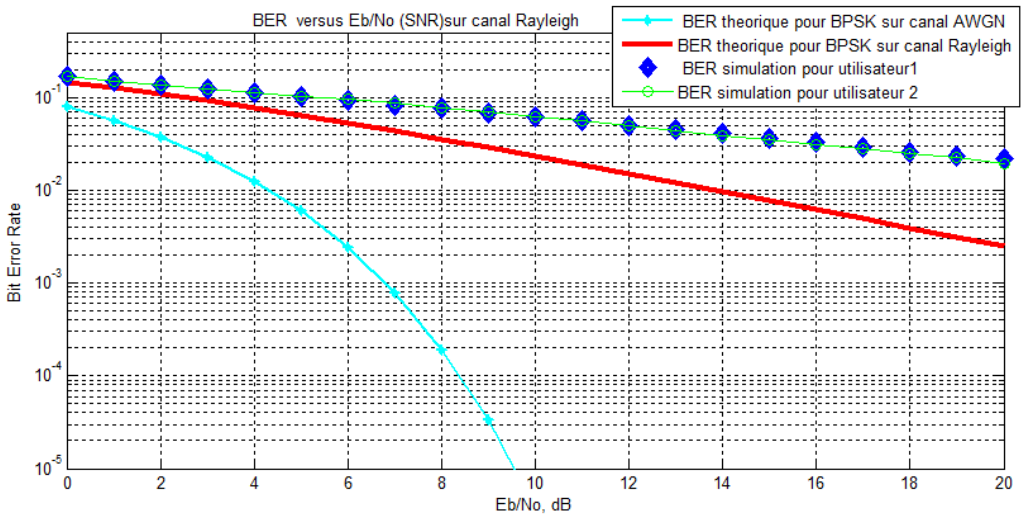


Figure 38. BER versus Eb/no performance CDMA sur canal Rayleigh avec générateur LFSR de l'ordre 4, polynôme : X4+X2+1 avec état initial = [1 0 0 1] ;

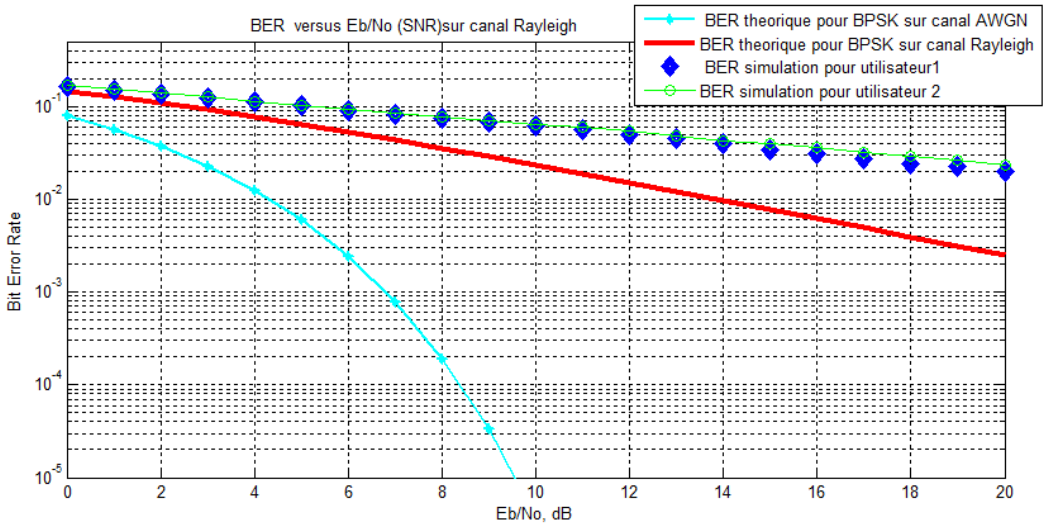


Figure 39. BER versus Eb/no performance CDMA sur canal Rayleigh. avec générateur gold code de l'ordre 4, deux générateur LFSER : X4+X3+X2+1 et X4+X2+1 avec état initial = [1 0 0 1] ;

L'étude du système de transmission MC-CDMA en utilisant canal de Rayleigh fading et le canal AWGN pour les utilisateurs K et trois séquences d'étalement a été réalisée avec succès.

Les codes de Walsh orthogonales dans MC-CDMA donnent de meilleurs résultats que les codes m-séquence PN et codes de Gold.

8. Conclusion :

Dans cette étude, un examen rapide a été fait sur les différents CDMA systèmes sans fil dans le domaine des communications mobiles. La performance de la même a été étudié et analysé. DSSS technique de transmission trouve ses applications dans les réseaux de communications personnelles. CDMA fournit une plus grande efficacité de la bande passante avec une augmentation de capacité correspondante, la vie privée de la parole, l'immunité d'évanouissement par trajets multiples, et souffre de multiples interférences d'accès (AMI) en raison de non étalement orthogonal. WCDMA offre facteur d'étalement variable et plusieurs codes pour utilisateur d'activer des fonctionnalités telles que des débits élevés et de multiples services pour la même connexion. MUD réduit l'effet de l'interférence et donc augmente la capacité du système. Dans les systèmes MC-CDMA l'interférence est considérablement réduite. On peut conclure que la technique MC-CDMA peut être utilisé pour transmettre et recevoir les données en particulier dans un environnement bruyant. Cette technique contrecarre les effets indésirables comme ISI, ICI, des erreurs en rafale, évanouissement par trajets multiples, etc., et les données peuvent être récupérées sans erreur. Nos principales conclusions sont les suivantes :

- La comparaison de la CDMA, CDMA-MUD et OFDM à MC-CDMA, montre que "MC-CDMA" donne de meilleurs résultats.
- La performance du code PN séquence et Code Walsh séquence d'étalement dans "MC-CDMA" est le meilleur que la séquences d'étalement (gold code)
- MC-CDMA système de transmission peut être prolongée pour une estimation de canal en faisant usage de filtres adaptatifs approprié

Annexe

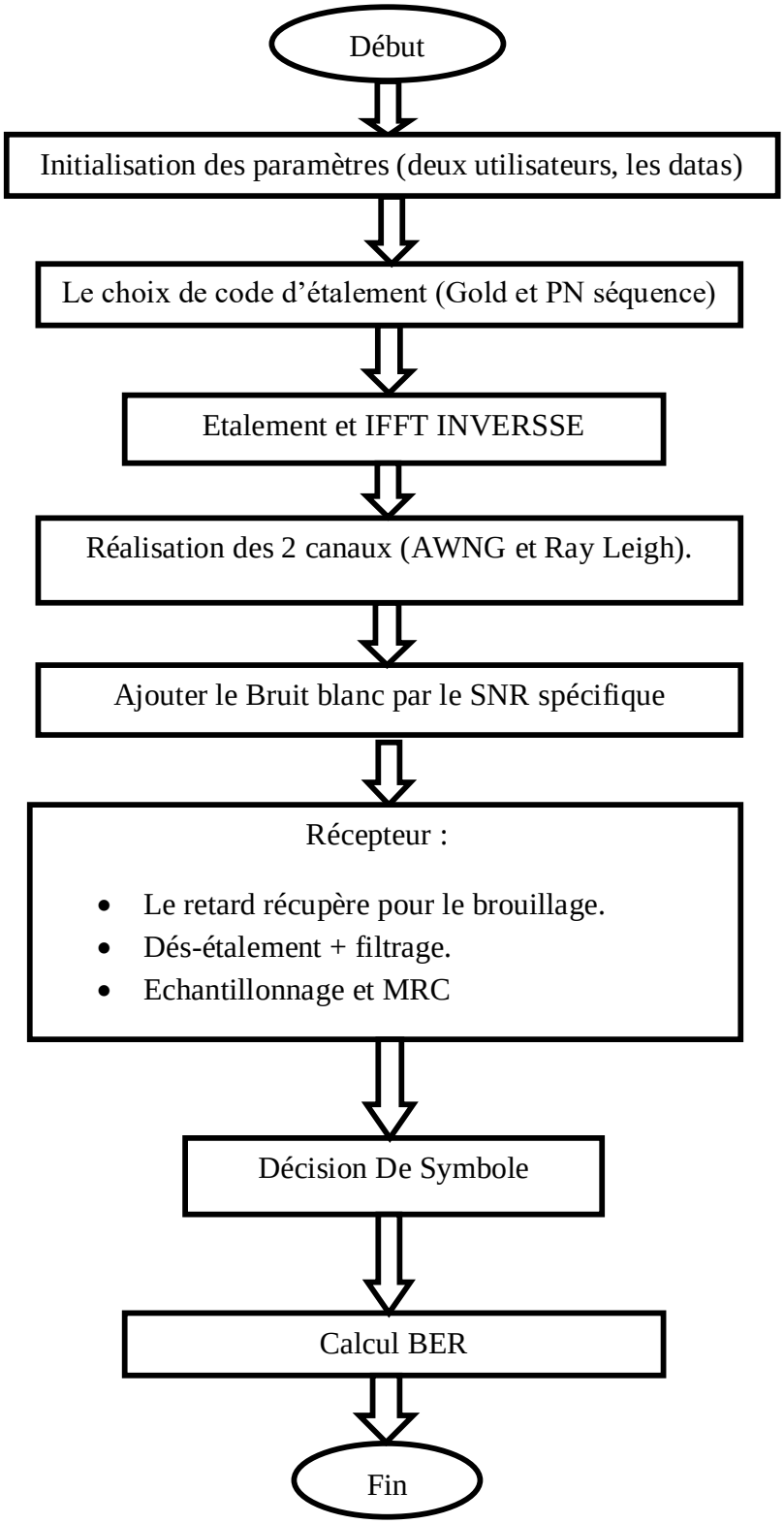


Figure 40. Organigramme de l'algorithme d'application de LFSR dans les systèmes de communication mobil

VI. Conclusion general:

Une communication multiutilisateur consiste en la transmission sur un même canal de transmission, des données provenant de plusieurs utilisateurs. Les divers utilisateurs doivent alors se partager ce canal de transmission. Dès lors, l'efficacité de l'occupation du canal par les différents utilisateurs s'avère primordiale. Plusieurs critères discriminants existent pour séparer les signaux provenant des différents utilisateurs. Parmi eux, le CDMA qui est une technique de multiplexage définie comme étalement de spectre. Cette technique est issue des programmes de recherches militaires qui avaient pour but de protéger les transmissions d'informations contre le brouillage, c'est-à-dire une forme d'interférence volontaire. Actuellement, le WCDMA qui n'est autre que la version de CDMA à large bande est déjà utilisé dans la téléphonie de troisième génération comme l'UMTS.

Pour le CDMA, l'utilisation des séquences d'étalement comme codes permettant de distinguer les différents utilisateurs donne l'avantage d'exploiter simultanément l'ensemble de la bande de fréquence et des intervalles de temps. Dans cette technique d'accès multiple, les utilisateurs partagent le même espace fréquentiel et transmettent sur les mêmes intervalles temporels. Il s'agit, dans ce cas, d'affecter à chaque émetteur un code, aussi appelé signature ou encore séquence de code. Il en résulte une meilleure gestion des ressources disponibles. Pour assurer la synchronisation des ces codes et pour séparer les canaux, il faut que la fonction d'autocorrélation soit maximale et que la fonction d'inter-corrélation soit minimale. Ces deux propriétés sont basées sur le principe d'orthogonalité des codes utilisés.

Ce mémoire nous a permis de savoir de plus près cette technique d'accès multiple et traite surtout les caractéristiques de ces codes. Walsh Hadamard possède une bonne propriété d'auto-corrélation mais l'inconvénient majeur que présente ce code est qu'il ne possède plus les mêmes propriétés d'orthogonalité dans le cas d'une émission asynchrone des différents utilisateurs. De plus les propriétés d'auto-corrélation des différentes séquences, pour une valeur non nulle de τ, sont, elles aussi, mauvaises, là où l'on constate la présence des pics. Pour cela grâce à leurs spécificités en termes de fonction de corrélation, les séquences de Gold peuvent être utilisées comme séquence de code dans les systèmes de transmission CDMA asynchrones. Le récepteur dans ce système peut se synchroniser en utilisant les propriétés d'auto-corrélation des séquences de Gold.

Bibliographie

Chapitre II :

[1] http://fr.wikipedia.org/wiki/Th%C3%A9orie_de_l%27information

[2] http://www.ref-union.org/index.php

[3] http://www.espaceferrie.fr/

[4] http://www.industrie.gouv.fr/tc2015/technologies-cles-2015-tic.pdf

[5] http://fr.wikipedia.org/wiki/Histoire_des_t%C3%A9l%C3%A9communications

[6] http://www.cnes.fr/web/CNES-fr/485-histoire-et-techniques-des-telecommunications.php

[7] http://www.udppc.asso.fr/national/

[8] http://www.lesite.tv/videotheque/0697.0022.00-internet

[9] http://www.samomoi.com/reseauxinformatiques/, http://hautrive.free.fr/reseaux/supports/,

[10] http://nicolas.baudru.perso.esil.univmed.fr, www.scribd.com/doc/30411489/Cours-Fibre Optique

Chapitre III :

[1] http://www.sss-mag.com/pdf/lfsr/pdf « Linear Feedback hift Rgister Megafunction » Version 1, Déc. 1996.

[2] M. George and P .Alfke , « Linear Feedback hift Rgister in Virtex Devices (application not) » http://www.xilinx.com/bvdocs/appnotes/xapp210.pdf

[3] J.Nyathi, J.G Delgado-frias and J.Lowe , « A High-Performmance, Hybrid Wave-Pipelined Linear feedback register with skew tolerant clocks, » 46th IEEE Midwest symposium on circuits and systèmes , Cairo ,Egypt ,in press, dec. 2003.

[4] Gérald arnould these de doctorat discipline : elctronique « etude et conception d'architectures haut-débit pour la modulation et la démodulation numériques » 8 Décembre 2006 page 75.

[5] M. Goresky and A.Klapper, « Fibonacci and Galios representation of feedback with carry shift register », IEEE Trans. Inform . Theory, vol 48, pp .2816-2836, Nov. 2002.

[6] R.Lidl and H.Niederreiter , Inroduction to finite fields and their application , :année 1986.

[7] Alfred J. Menezes ,Pall C.van Orschot ,scott A. Vanstone Handbook of applied cryptography 1997 by CRC presse LLC

[8] S. W. Golomb, shift Register Sequences, aegean park press, laguna Hills, CA, 1982.

[9] Coures Codages télécom réseaux octobre 2006 v1.3 PDF page 247.

[10] Ali pacha adda ; thése doctorat d'état « sécurité de l'information : algorithmes et synthèses » année 2004 ; chapitre 2 ; page 73-77

[11] Hadj SAID NAIMA ; thèse doctorat d'état « codes correcteurs d'erreurs entre la transmission de l'information et sa sécurité » année 2005 ; chapitre 3. Page 54-60.

Chapitre IV :

[1] Andreas Klein, *Linear Feedback Shift Registers*, 20 avril 2013 DOI10.1007/9781447150794(http://dx.doi.org/10.1007/9781447150794)),p. 1758

[2] A. Ahmad, Sameer AlBusaidi et Ahmed AlNaamany,*Measurement techniques of lfsr sequences*, mars 2003

[3] Abdelaziz Marjane, *Conception Vectorielle de Registre à rétroaction avec retenue sur les corps finis*, 8 juillet 2011(lire en ligne (http://tel.archivesouvertes.fr/docs/00/68/00/21/PDF/rapportthesemarjane2011halv2.pdf))

[4] T.K. Moon, *Error Correction Coding : Mathematical Methods and Algorithms*, 27 juin 2005(DOI 10.1002/0471739219.ch4 (http://dx.doi.org/10.1002/0471739219.ch4)), p. 154170, en particulier le chapitre 4, « Cyclic Codes, Rings, and Polynomials »

[5] Lauradoux, « From Hardware to Software Synthesis of Linear Feedback Shift Registers»,*Parallel and Distributed Processing Symposium, 2007. IPDPS 2007. IEEE International*, 2630 mars 2007, p. 18 (DOI 10.1109/IPDPS.2007.370643 (http://dx.doi.org/10.1109/IPDPS.2007.370643))

[6] M. Goresky et A.M. Klapper, « Fibonacci and Galois representations of feedbackwithcarry shift registers », *Information Theory, IEEE Transactions on*, novembre 2002, p. 28262836 (ISSN 00189448 (http://worldcat.org/issn/00189448&lang=fr),

DOI 10.1109/TIT.2002.804048 (http://dx.doi.org/10.1109/TIT.2002.804048))

[7] Antoine Joux et Pascal Delaunay, « Galois LFSR, Embedded Devices and Side Channel

Weaknesses », *Progress in Cryptology INDOCRYPT 2006*, 2006, p. 436451 (ISSN 03029743 (http://worldcat.org/issn/03029743&lang=fr), DOI 10.1007/11941378_31 (http://dx.doi.org/10.1007/11941378_31))

[8] Nadia Ben Atti, Gema M. Diaz–Toca et Henri Lombardi, « The BerlekampMassey Algorithm revisited », *Applicable Algebra in Engineering, Communication and Computing*, avril 2006, p. 7582 (ISSN 09381279 (http://worldcat.org/issn/09381279&lang=fr), DOI10.1007/s002000050190z (http://dx.doi.org/10.1007/s002000050190z))

[9] Circuits and Systems, Oct. 1989, pp. 1074 -1088, Circuits and Systems, July 2002 Page(s): 842 -851

Chapitre V :

[1] Pin Gan, s, 2002, CDMA detection guided rake receivers channel of information technology and electrical engineering. The University of Queensland PP 1-28.

[2] Fundamentals of wireless communication by David Tse and Pramod Viswanath.

[3] The enhanced performance of combined Multicarrier and CDMA Technologies in Multipath fading channels.

[4] Multi-carrier transmission techniques for wireless communication system. A servy by Haithan J Tuna and M.F.M Sallesh school of Electrical and Electronics Engineering, University Saia's Malaysia.

[5] Hara, S. Prasad Overview of multicarrier CDMA, IEEE communications Magazine. Dec 1997, Vol.35, no.12, PP 126 –133.

[6] Nobilet, S.Helard, J.Moltier D. spreading services in uplink and downlink MC-CDMA systems. PAPR an MAI minimization. European transactions in Telecommunications, 2002.

[7] Third Generation wireless networks by Nitin Desai, Madav Chinta.

[8] An overview of wireless data communications by Richard Perlman, Lucent technologies.

[9] Theodore S. Rappaport, Wireless communications principles and practice, second edition, Pearson Education, 2003.

[10] System-level performance analysis and design of RF receiver for WCDMA user equipment by Hyun Seob Shiz, Jai Hyungpark, Jihoon Kin & Hyuang Joun Yoo 2000, 2 nd International Conference on Microwaves.

[11] Design & Implementation of Configurable WCDMA Rake receiver architecture on GPGA by Mukesh Chugh, Dinesh Bhatia, University of Texas, Dallas.

[12] R.Prasad and S.Hara, "Overview of Multicarrier CDMA", proceeding of fourth International Symposium in Spread Spectrum Techniques.

[13] Effects of spreading sequences on the performance of MC CDMA System with non-linear models of HPA by P.Drotar, J.Gazela, P.Galaija, Radio Engineering, Vol.18, No.1, and April, 2009.

[14] Direct sequence spread spectrum technique with residue number system, M.I.Yousseb, A.E.Emam and M.Abdul Elghary, International Journal of Electrical and System Engineering, 2009.

[15] Design of 3 rd generation multirate CDMA system with multicarrier detection, MUD CDMA by Tero Ojanpera, Kari Rikkinen, Hannu Hakkinen, Kari Phehkoresh, Ari Haltimen and

Jarna Lillebery.

[16] Multi-carrier Transmission for wireless communication systems– A survey by Haitham J.Taher and M.F.M Salleh, School ofElectrical and Electronics Engineering, ISSN:1109-2742, University Sains Malaysia, Issue 5, Volume 08, May 2009.

[17] Implementation of Cordic based Architecture for WCDMA/ OFDM receiver by Srinivas Chaitanya.K, P.Muralidhar, C.B.Rama Rao, European Journal of Science & Research, and ISSN 1450-216 X, Vol. 36, pp 65-68, No.1-2009.

[18] Design and performance Analysis of the MC CDMA by Bang- Solee, Sin Chang Park,14 th IEEE International Symposium on Personal Indoor and mobile Radio Communication Proceedings, 2009.

[19] The Enhanced Performance of Combined Multicarrier and CDMA technique in Multipath Fading Channels by Rash S.EI- Khamy, Shawki E. Shaaban, Ibrahim A. Ghaleb and Hassan N. Kheirallah. 21 st National Radio Science Conference (NRSC2004) (NTI) March 16-18, 2004. [20] W-CDMA and CDMA2000 for 3G mobile networks by M.R. Karim M. Sarraf 2002, Lucent Technologies.

[21] Wideband multi-rate DS-CDMA for next generation mobile communication systems by F. Adachi and M. Sawahashi R&D Department, NTT Mobile Communication Network. 0-7803-4194- 5/97 @1997 IEEE.

[22] Chang, R. W., and R. A. Gibby, "A Theoretical study of the Performance of an Orthogonal Multiplexing Data Transmission Scheme". IEEE Tran. COM. Vol.Com.16, no.4, August 1968, PP.527-540.

[23] Performance analysis of MC-CDMA and OFDM in wireless Rayleigh channel by V.Jagan naveen, K Murali Krishna, K.RajaRajeswari.International journal of Advanced Science and Technology vol.25.December, 2010.

[24] Performance evaluation of MC-CDMA techniques for variable bit-rate transmission in LEO Satellite Networks by Claudio Sacchi, Gianluca Gera, Carlo S, Regazzoni.