Embrouillage

PLAN

Utilité
Utilisation d'un code polynômiale
Construction de l'embrouilleur
Désembrouilleur
Générateurs de séquences aléatoires
    a) Générateurs congruentiels
    b) Générateur de Fibonacci décalé
    c) Registres à décalages à rétroactions linéaires
Problème de synchronisme
Exemples connus

Bibliographie

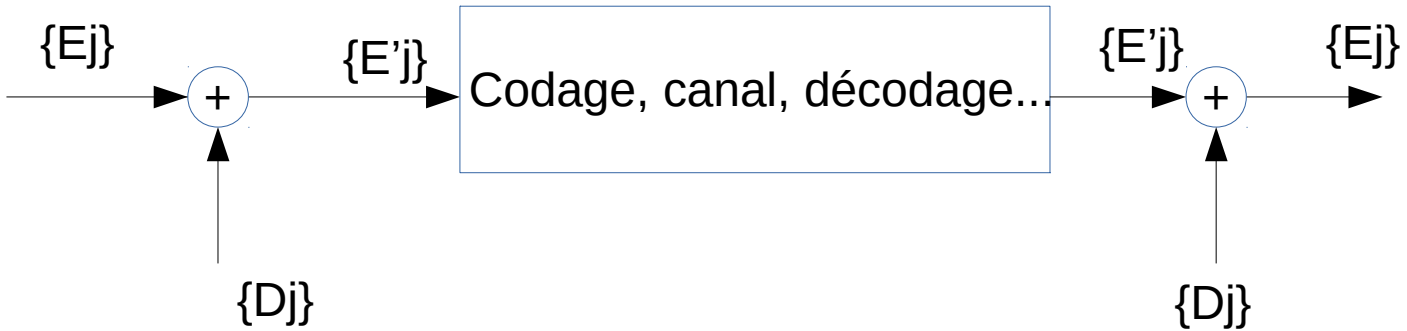
Utilité

- Rend les informations transmises difficilement piratables
- Permet de diminuer l'impact des erreurs en rafale

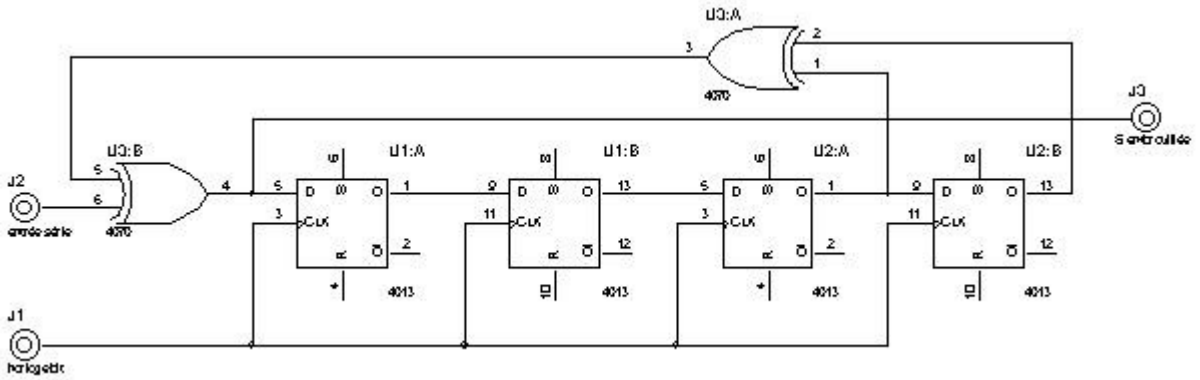
  ↳ les informations sont alors transmises de façon fiable

Utilisation d’un code polynômiale

Idée : utiliser le OU EXCLUSIF et une séquence pseudo-aléatoire générée par un code polynomiale



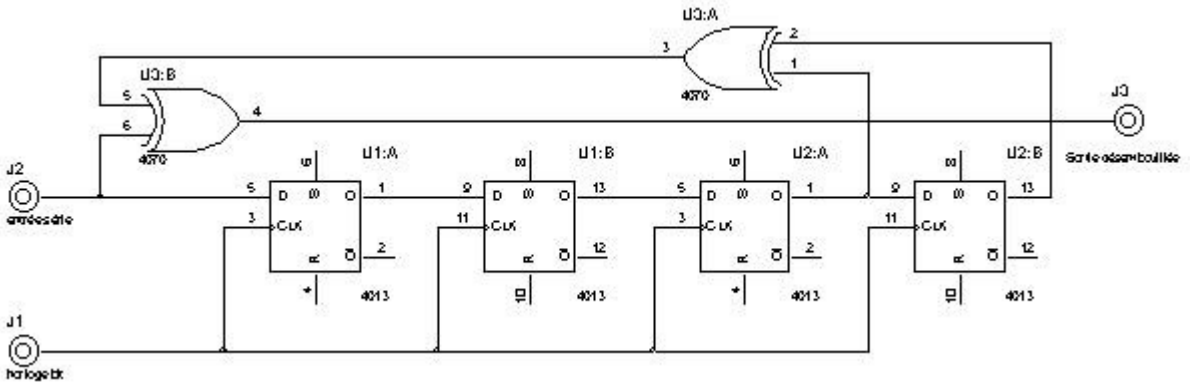
Construction de l’embrouilleur



Preuve : S(n) = E(n) ⊕ [Q3 ⊕ Q4]

(on observe bien la présence du OU EXCLUSIF)

Désembrouilleur



En J3, le signal S’(n) = S(n) ⊕ [Q3 ⊕ Q4] donc

S’(n) = [E(n) ⊕ [Q3 ⊕ Q4]] ⊕ [Q3 ⊕ Q4]

D’où S’(n) = E(n)

Générateurs de séquences aléatoires

- a) Générateurs congruentiels
- b) Générateur de Fibonacci décalé
- c) Registres à décalages à rétroactions linéaires

a) Générateurs congruentiels

Idée : créer une suite de nombres avec le moins de régularité possible

On choisit une valeur m qui sera le maximum des entiers considérés, le premier terme A_0 et deux entiers a et b pour poser $U_{n+1} = a.U_n + b$

a) Générateur congruentiels

1er cas : b = 0.

- Choisir a tel que les restes des divisions euclidiennes par m des puissances successives de a ne soient égales à a que le plus tard possible

2ème cas : b non nul.

- Il faut tout d'abord que m et b soient premiers entre eux. Ensuite a-1 doit être un multiple de p pour tout p diviseur premier de b et un multiple de q pour tout q diviseur premier de m.

Ainsi, de cette manière on obtient un générateur à une racine de période m, on peut alors choisir la racine au hasard entre 0 et m-1

Problème : il faut définir avant un m souvent trop grand !

b) Générateur de Fibonacci décalé

Au lieu de définir un rang suivant, on définit le rang n de la suite (Un) par les deux termes précédents :

$$U_n = a.U_{n-1} + b.U_{n-2} + c$$

$$U_n = U_{n-j} + U_{n-k}$$

Avec cette méthode, la série ne bouclera que si les deux valeurs au rang n-p et n-q se répètent simultanément. Ainsi, il n'est plus nécessaire de choisir un m grand puisqu'une suite pour laquelle Un est défini par U_{n-1} , U_{n-2}... jusque U_{n-k} aura une période maximale de $m^k - 1$

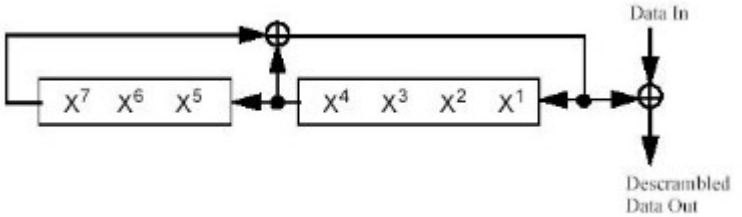
c) Registres à décalages à rétroactions linéaires

Intérêt : le choix de m pour la première technique est trop subjectif et la deuxième technique peut revenir à la suite de Fibonacci classique avec p = 1 et q = 2. D'où l'intérêt de cette méthode pour une suite plus compliquée à prévoir et créer des séquences aléatoires spécifiques

c) Registres à décalages à rétroactions linéaires

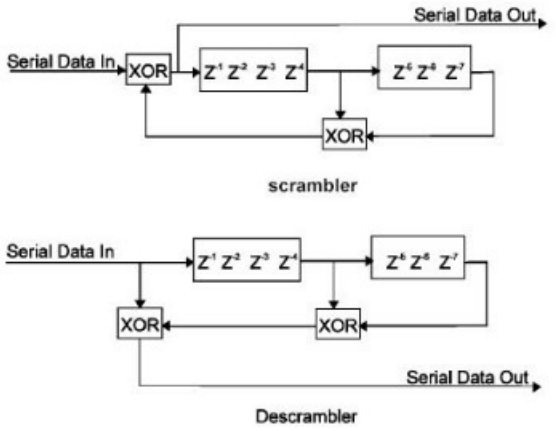
Il est possible de créer une m-séquence, c'est-à-dire une séquence aléatoire de période 2^r-1

Ainsi, une m-séquence a comme particularité principale de présenter une fonction d'auto-corrélation permettant ainsi de mesurer les réponses impulsionnelles



Problème de synchronisme

Les méthodes d'embrouillage présentées précédemment, distinguent le générateur de séquences aléatoires et le mélangeur (dans notre cas d'étude un simple OU EXCLUSIF) à deux entrées. Néanmoins, cette séparation nécessite un processus de synchronisation au niveau de la réception pour bien dé-mélanger. Avec l'auto-synchronisation, voilà le schéma de l'embrouilleur.



Exemples connus

Générateurs de Séquences Aléatoires et Scramblers (IEEE 802.11, IEEE 802.16, 3GPP LTE)					
Standard	Polynôme	Type de Séquence émise	Type de Structure Requise	Utilisation	Remarque
IEEE 802.11	$x^7 + x^4 + 1$	PN-Séquence	LFG	Embrouillage et Désembrouillage des données pour les type de modulation FHSS et OFDM	Emission et Réception
IEEE 802.11	$x^7 + x^4 + 1$	PN-Séquence	LFSR	Embrouillage des données pour les types de modulations DSSS et High Rate DSSS	Uniquement à l'émission. Pas de séquence Initiale, insertion des données directement
IEEE 802.11	$x^7 + x^4 + 1$	-	*Registre à Décalage*	*Désembrouillage des données pour les types de modulations DSSS et High Rate DSSS*	*Uniquement à la Réception*
3GPP LTE	$x^{25} + x^3 + x^2 + x + 1$	Gold-Séquence	Deux FILTRES IIR interconnectés	Embrouillage et Désembrouillage des données pour la voix montante	Uniquement pour l'Uplink
3GPP LTE	$x^{18} + x^{10} + x^7 + x^5 + 1$	Gold-Séquence	Deux FILTRES IIR interconnectés	Embrouillage et Désembrouillage des données pour la voix descendante	Uniquement pour le Downlink
IEEE 802.16	$x^{15} + x^{14} + 1$	PN-Séquence	LFG	Embrouillage et Désembrouillage des données pour les différentes modes Single Carrier, Single Carrier Access, OFDM et OFDMA.	Emission et Réception
IEEE 802.16	$x^{22} + x^{21} + 1$	PN-Séquence	LFG	Génération des séquences pour la construction de la modulation « Spread BPSK » dans le cas Single Carrier et Single Carrier Access	Emission et Réception
IEEE 802.16	$x^{11} + x^9 + 1$	PN-Séquence	LFG	Génération des séquences pour la construction des pilotes des sous porteuses dans le cas de l'OFDM et OFDMA.	Emission Séquences Initiales différentes pour Uplink et Downlink

Bibliographie

https://tel.archives-ouvertes.fr/tel-00538631/document

http://dondon.vvv.enseirb-matmeca.fr/transnum/modnumBPSK/modnum.html

https://hal.archives-ouvertes.fr/tel-01345384/file/HDR_manuscrit-complet.pdf

http://kasttet.free.fr/V29.pdf

https://slideplayer.fr/slide/466077/

https://www.mathworks.com/help/comm/ref/pnsequencegenerator.html

http://www.irisa.fr/cosi/SEMINAIRE/transparents/WCDMA.pdf