FROM RESEARCH TO INDUSTRY

cea tech

Sécurité des communications par étalement de spectre

Mathieu des Noes (CEA-LSOC), Valentin Savin, Laurent Ros, Jean-Marc Brossier

(mathieu.desnoes@cea.fr)

www.cea.fr

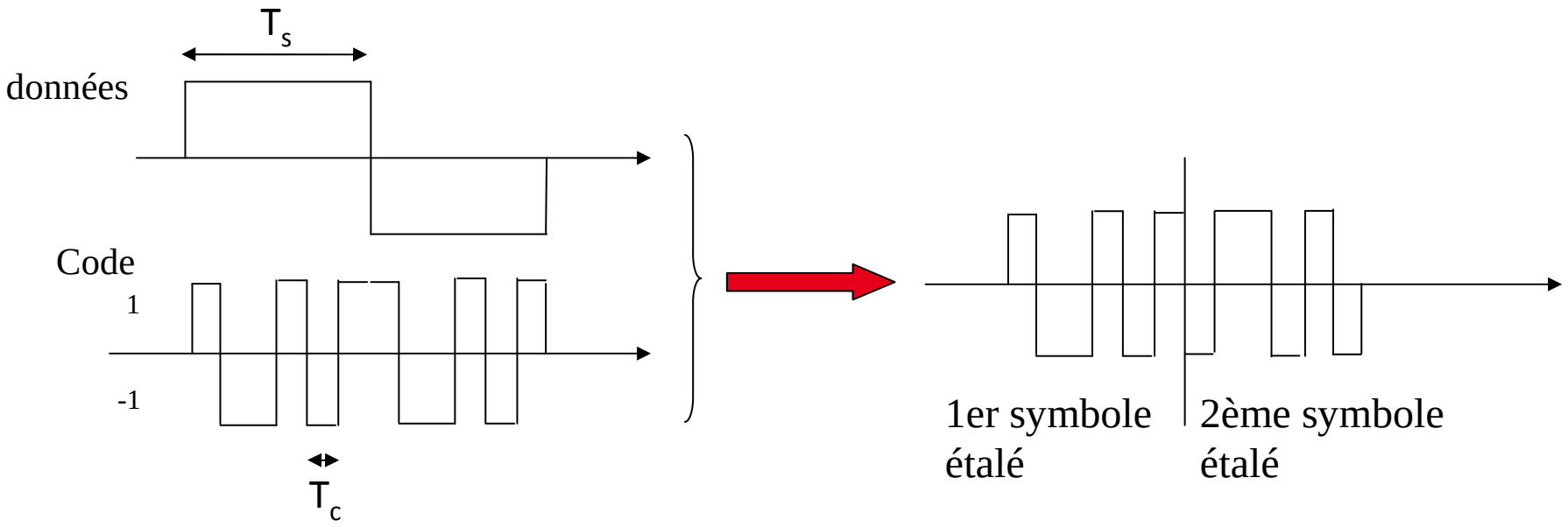
leti

Plan

- Etalement de spectre par séquence directe (ESSD)
- Séquences de Gold: propriétés
- Détection par décodage
  - Principe
  - Equations de parité : nombre, degré minimal
- Performances : cas d'une liaison standardisée (CCSDS)
  - Recherche en série
  - Recherche en parallèle
- Conclusion et perspectives

ESSD: principe d'émission

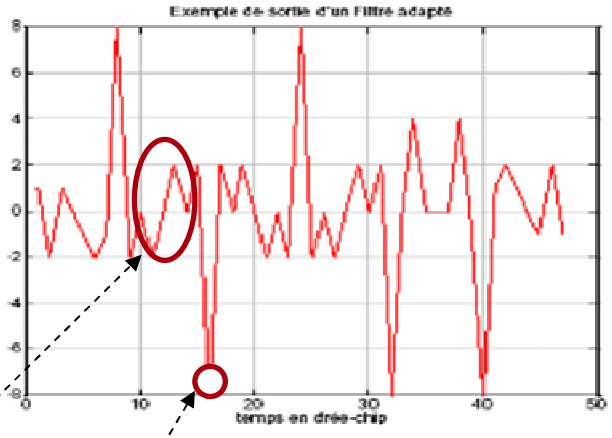
- Etalement de spectre par séquence directe [1]
- Exemples : UMTS (3G), CDMA2000 (2G-3G US), GPS, Galileo, transmissions militaires

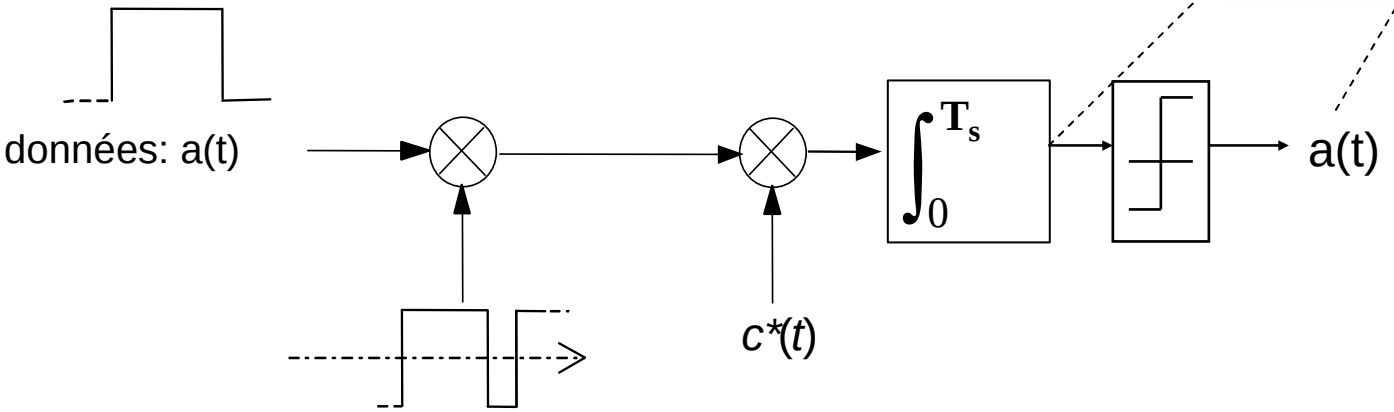


- Facteur d'étalement : $F = T_s/T_c$

ESSD: récepteur

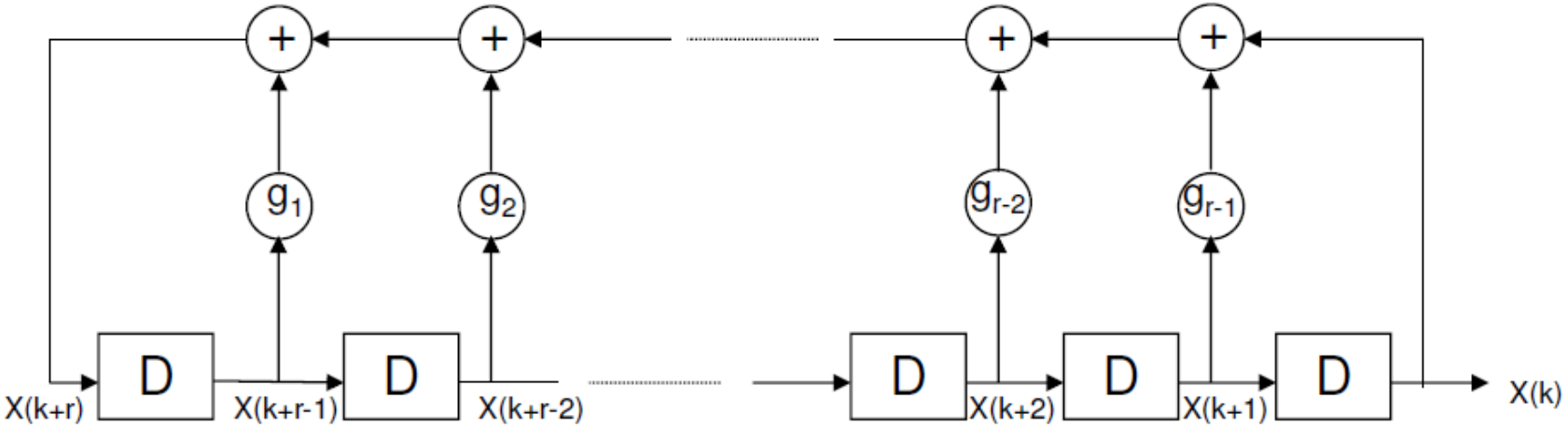
- Corrélation avec la séquence d'étalement
  - Hypothèse: **Séquence connue**
- Faible probabilité de détection :
  - SNR = F. P/σ^2
  - SNR faible (-17 dB en WCDMA UL pour la voix)
- Si la séquence est inconnue : test des N séquences possibles. Pas réaliste si N est grand (ex : N = 33 554 432 en WCDMA)





Séquence de Gold

- $z(k) = x(k) \oplus y(k)$
  - x(k) et y(k) forment une paire préférentielle de m-séquences de même longueur [2]
  - Il existe 2^r+1 séquences de Gold de longueur $N = 2^r-1$
  - Bonne propriétés d'inter-corrélation => CDMA asynchrone
  - Polynôme générateur : $g_z(X) = g_x(X)\, g_y(X)$

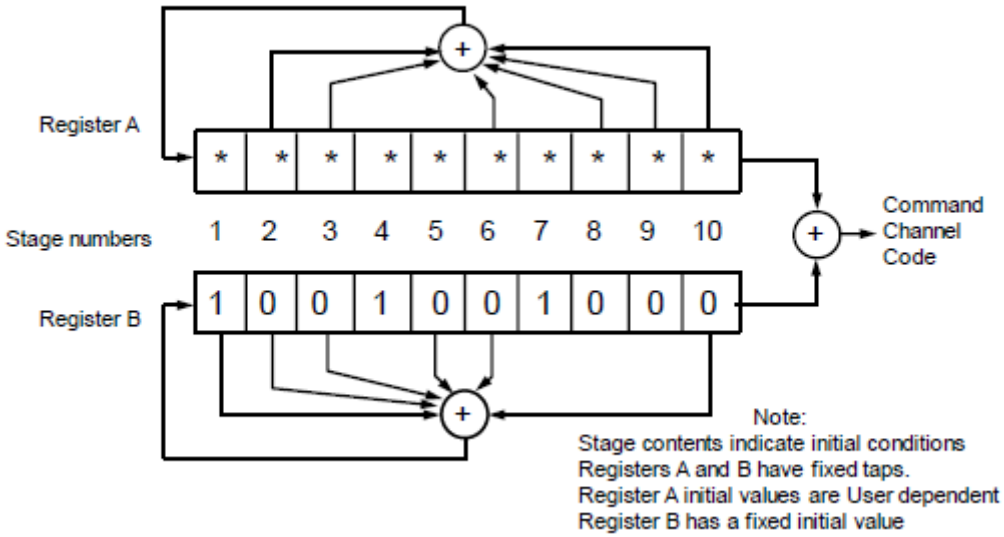


ESSD: sécurité

- Si le polynôme générateur est connu => détection de la séquence = connaître l'état des registres
- **Objectif** : estimation de l'état des registres avec des techniques de décodage
  - Attaques sur les stream ciphers [3]
  - Communications ESSD avec des m-séquences [5]
- **Applications** :
  - détection aveugle du code d'embrouillage des systèmes WCDMA et CDMA2000 => Possibilité de mettre en œuvre des attaques par déni de service [6][7].
  - Acquisition des satellites GPS ou Galileo
  - Mécanismes de synchronisation avec des techniques de codage canal.

Code de Gold

- Code de Gold = code linéaire cyclique de rendement $2r/(2^r-1)$
  - Mot à coder : état des registres (2r),
  - Mot de code : la séquence générée (2^r-1)
  - Particularité de nombreux systèmes : l'état des registres d'une des 2 séquences est connu à un instant donné (ex: WCDMA, GPS, CCSDS)
- Equations de parité :
  - Définies par le code dual: intersection des codes duaux des 2 m-séquences
  - Notation polynômiale : multiple du polynôme générateur : $f(x) = m(x)g_z(x)$



Décodage itératif (1/2)

- Modèle d'observation :
  - Pré-traitements pour observer la séquence de Gold
  - Séquence émise : $z(k) \in \{0;1\}$
  - Signal reçu : $R(k) = (-1)^{z(k)} + n(k)$
- Matrice de parité : $Ez = 0$
  - Equation de parité initiale : $g(X) = g_0+g_1X+\ldots+g_rX^r$
  - Code cyclique => $X^ig(X)$ est aussi une équation de parité

$$\mathbf{E} = \begin{bmatrix} g_r & \cdots & g_0 & 0 & \cdots & \cdots & 0 \\ 0 & g_r & \cdots & g_0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & g_r & \cdots & g_0 & 0 \\ 0 & \cdots & \cdots & 0 & g_r & \cdots & g_0 \end{bmatrix}$$

Décodage itératif (2/2)

- Décodage avec un algorithme de décodage par passage de messages (e.g. Min-sum):
  - Exploitation de toute la théorie et résultats sur le décodage des codes LDPC [4][13] : il faut utiliser des équations de parité de poids faible
  - Graphes redondants : si g(X) est une équation de parité, alors $g_l(X)$ est aussi une équation de parité [5]

$$g_l(X) = [g(x)]^{2^l} = g\left(x^{2^l}\right)$$

  - Matrice de parité avec les graphes redondants: augmente le nombre d'équations de parité sans modifier leur poids *t*

$$E_{\mathrm{RGM}} = \begin{bmatrix} E_0 \\ E_1 \\ \vdots \\ E_{N_{\mathrm{RGM}}-1} \end{bmatrix}$$

Equations de parité (1/2)

- Nombre d'équations de parité de poids *t* : N_t
  - Travaux de Pless [8] et Kasami [9]
  - r pair :
    - $N_1 = N_2 = 0$
    - $N_3 = 1$ et $h_3(x) = x^{2(2^r-1)/3} + x^{(2^r-1)/3} + 1$ [10]
    - $N_4 = (2^r - 4)/3$ (recherche exhaustive)
  - r impair :
    - $N_1 = N_2 = N_3 = N_4 = 0$
    - $N_5 = (2^{2r} - 10\,2^r + 16)/24$

r	6	7	9	10	11	18
N_4	20	0	0	340	0	87380
N_5	-	630	10710	-	173910	-

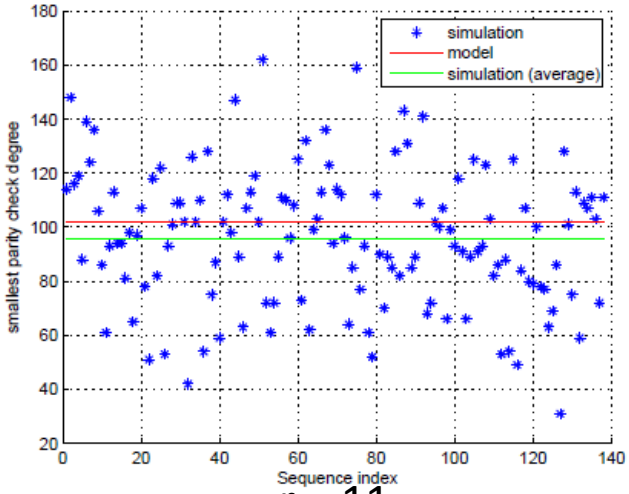
Equations de parité (2/2)

- Degré minimal des équations de parité de poids *t* ?
  - Faisabilité du décodage (complexité, contrainte des standards (e.g. WCDMA)), recherche des équations de parité
  - Modèle pour les m-séquences [11] : applicable aux séquences de Gold

$$N_t \begin{pmatrix} m_0 \\ t-1 \end{pmatrix} = \begin{pmatrix} N-1 \\ t-1 \end{pmatrix}$$ approximation $$m_{0,approx} = \frac{N}{(N_t)^{1/(t-1)}}$$

- Variabilité selon les séquences non prise en compte, utile pour connaître l'ordre de grandeur

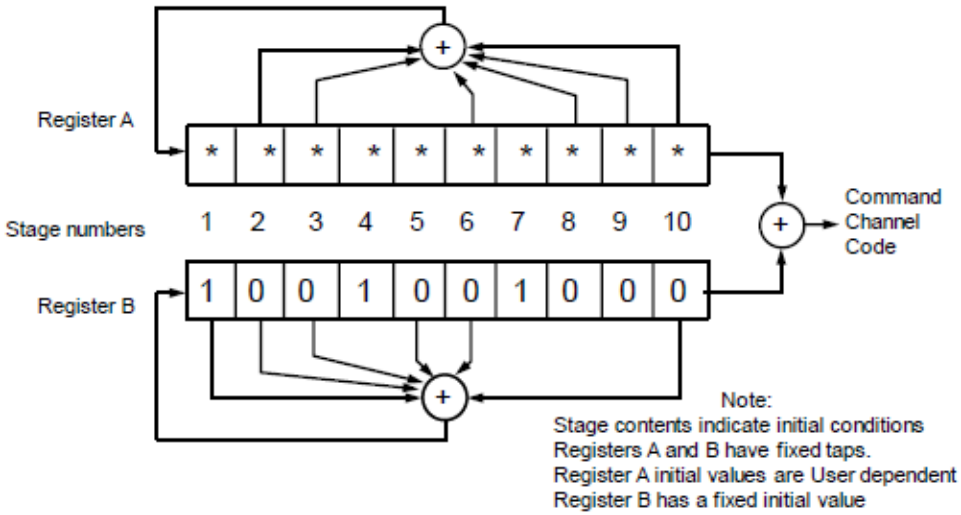
r	7	9	10	11	13	14	18	25
t	5	5	4	5	5	4	4	5
Simulation	24	48	111	114	219	1103	9822	-
Estimation	27	52	148	102	202	930	-	-
Approximation	25	50	146	100	200	930	5907	12821



r = 11

Performance - CCSDS

- CCSDS 415.2-B-1 : data transmission and PN ranging for 2GHz CDMA link via data relay satellite
  - Consultative Committee for Space Data Systems
  - Document public téléchargeable sur internet
- Séquence de Gold: séquence **x** connue, séquence **y** inconnue
- Evaluation de 4 méthodes de décodage:
  - 2 pour une recherche « série »
  - 2 pour une recherche « parallèle »



Performance - CCSDS

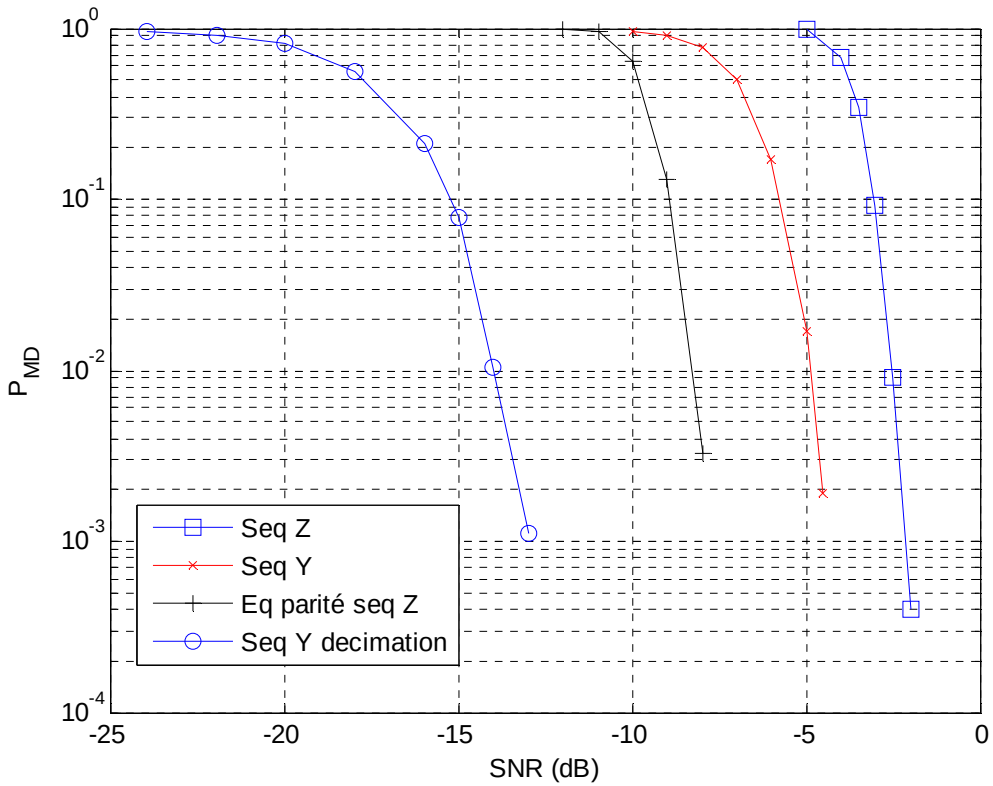
- Recherche « série » :
  - Hypothèse : $R(k) = (-1)^{x(k)+y(k)} + n(k)$
  - Si synchronisation :
    - $V(k) = (-1)^{x(k)} R(k) = (-1)^{y(k)} + n'(k)$
    - Observation de la séquence **y**
  - Décodage de la séquence **y** : **E** est construite à partir de $g_y(X)$
  - Décodage de la séquence **y**, avec exploitation de la relation de décimation entre les m-séquences [12]: **E** est construite à partir de $g_s(X)$ où **s** est tel que $y(k) = s(dk)$, d est le facteur de décimation entre les séquences **y** et **s**
- Recherche « parallèle » :
  - Décodage de la séquence **z**: **E** est construite à partir de $g_z(X)$
  - Décodage de la séquence **z** à partir des équations de parité de poids t=3 et t= 4

Performance - CCSDS

- Décodeur :
  - Min-Sum [13]
  - Arrêt si toutes les équations de parité sont satisfaites ou si $N_{iter} = 60$
  - $N_{RGM} = 6$
- r= 10, taille du vecteur d'entrée : N = 1023
- Equations de parité employées (recherche parallèle):
  - $X^{682}+X^{341}+1$; $X^{171}+X^{106}+X^{54}+1$; $X^{185}+X^{166}+X^{4}+1$; $X^{205}+X^{168}+X^{28}+1$; $X^{222}+X^{77}+X^{22}+1$; $X^{230}+X^{98}+X^{31}+1$
- $g_s(X) = X^{10}+X^{3}+1$
- Mesures de performance:
  - Probabilité de détection correcte (P_{CD}), Probabilité de détection ratée ($P_{MD} = 1 - P_{CD}$), Probabilité de fausse alarme (P_{FA}), Probabilité de décodage erroné (P_{WD}) et probabilité de non détection ($P_{ND} = P_{MD} - P_{WD}$)
  - Recherche « parallèle » : $P_{WD} < 10^{-6}$

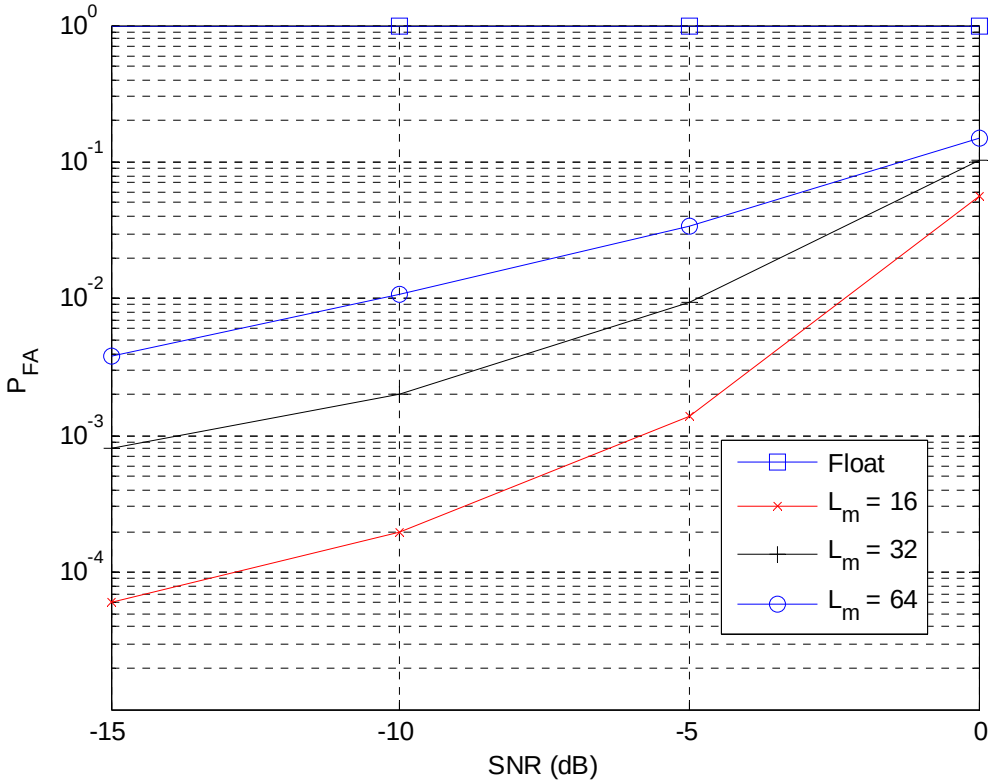
Performance – CCSDS

- Probabilité de détection correcte
  - Recherche en série avec exploitation de la décimation : gain de l'ordre de 12 dB par rapport à la recherche parallèle avec $g_z(x)$
  - Poids des équations de parité: seq Z => 9, seq Y => 7, seq Y decimation => 3



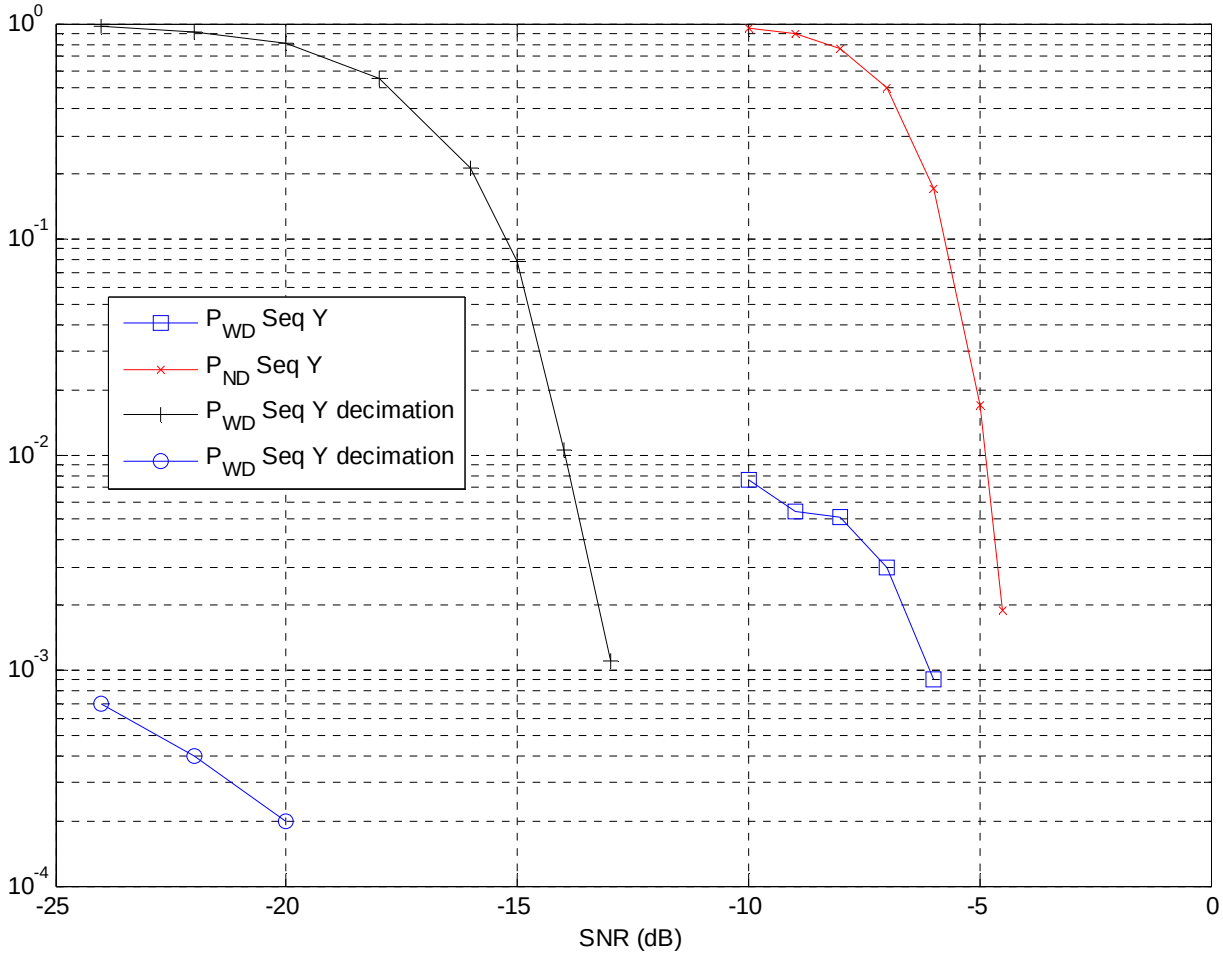
Performance - CCSDS

- SeqY, seqZ, équation de parité : $P_{FA} < 10^{-6}$
- Fausse alarme (recherche série, exploitation de la décimation):
  - Implémentation en flottant : catastrophique
  - Amélioration en passant en dynamique finie : message $\in [-L_m, +L_m]$



Performance - CCSDS

- P_{WD} faible et P_{ND} élevée avec t = 7 (« seq Y ») : quand il ne trouve pas le bon mot de code, le décodeur converge rarement (souhaitable)
- P_{WD} élevé et P_{ND} faible avec t = 3 (« seq Y decimations »): le décodeur converge presque toujours sur un mot de code (pas souhaitable)

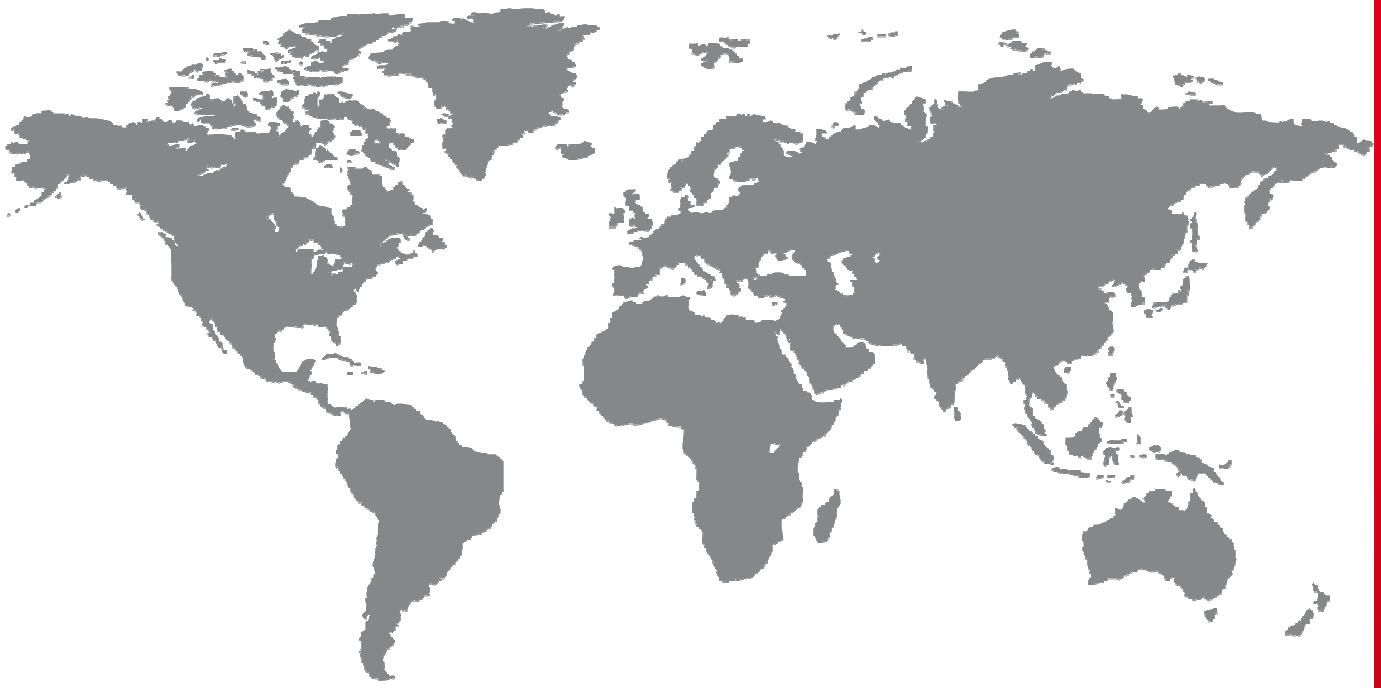


Conclusion et perspectives

- Transmission par étalement de spectre avec des m-séquences ou des séquences de Gold :
  - Détection et attaque plus facile avec les techniques de décodage par passage de messages.
  - Réutilisation des travaux sur les attaques sur les stream ciphers

	P_{CD}	P_{FA}	P_{WD}
Poids faible	+ +	- -	- -
Poids élevé	- -	+ +	+ +

- Sujets d'études :
  - Probabilité de fausse alarme et de décodage erroné : comprendre le mécanisme et trouver des améliorations (quantification, vérification) => analyse du décodeur MP dans des configurations peu usuelles (ex : pas de convergence à SNR très faible)
  - Complexité du décodeur : implémentation en temps réel ?
  - Méthodes constructives pour déterminer les équations de parité d'un poids *t* donné
  - Modification des séquences d'étalement : stream cipher appliqué aux communications ESSD ? ex: code P(Y) du GPS



Merci de votre attention !

leti

Centre de Grenoble
17 rue des Martyrs
38054 Grenoble Cedex

Références

[1] R.L. Peterson, R.E Ziemer and D.E. Borth, “Introduction to spread-spectrum communications”, Prentice Hall, 1995
[2] R.J. Mc Eliece, “Finite fileds for computer scientists and engineers”, Springer, 1997
[3] W. Meier and O. Staffelbach, “Fast correlation attacks on certain stream ciphers”, *Journal of Cryptology*, Vol. 1, N°3, 1989
[4] F.R. Kschischang, B.J. Frey and H.A. Loeliger, “Factor graphs and the sum-product algorithm”, *IEEE Trans. On Information Theory*, Vol. 47, N°2, 2001
[5] K.M. Chugg and M. Zhu, “A new approach to rapid PN code acquisition using iterative message-passing techniques”, *IEEE Journal on Selected Areas in Communications*, Vol. 23, N°5, 2005
[6] M. des Noes, V. Savin, L. Ros and J.M. Brossier, “Blind identification of the uplink scrambling code index of a WCDMA transmission and application to femtocell networks”, *IEEE International Conference on Communications*, Budapest, 2013
[7] M. des Noes, V. Savin, L. Ros and J.M. Brossier, “Blind identification of the uplink scrambling code of a reverse link CDMA2000 transmission”, *IEEE International Conference on Communications*, Budapest, 2013
[8] V. Pless, “Power moment identities on weight distributions in error correcting codes” , *Information and Control*, Vol. 6, N°2, 1963
[9] T. Kasami, S. Lin and W. Peterson, “Some results on cyclic codes which are invariant under the affine group and their applications”, *Information and Control*, Vol. 11, N°5, 1967
[10] K. Huber, “Some comments on Zech’s logarithms”, *IEEE Trans. On Information Theory*, Vol. 36, N°4, 1990
[11] S. Maitra, K.C. Gupta and A. Venkateswarlu, “Results on multiples of primitive polynomials and their products over GF(2)”, *Theorical Computer Science*, Vol. 341, N°1, 2005
[12] M. des Noes, V. Savin, L. Ros and J.M. Brossier,” Improving the Decoding of M-Sequences by Exploiting their Decimation Property”, Eusipco, Septembre 2013, Marrakech
[13] N. Wiberg,”Codes and decoding on general graphs ”, Ph.D. dissertation, Linköping University, Sweden, 1996