

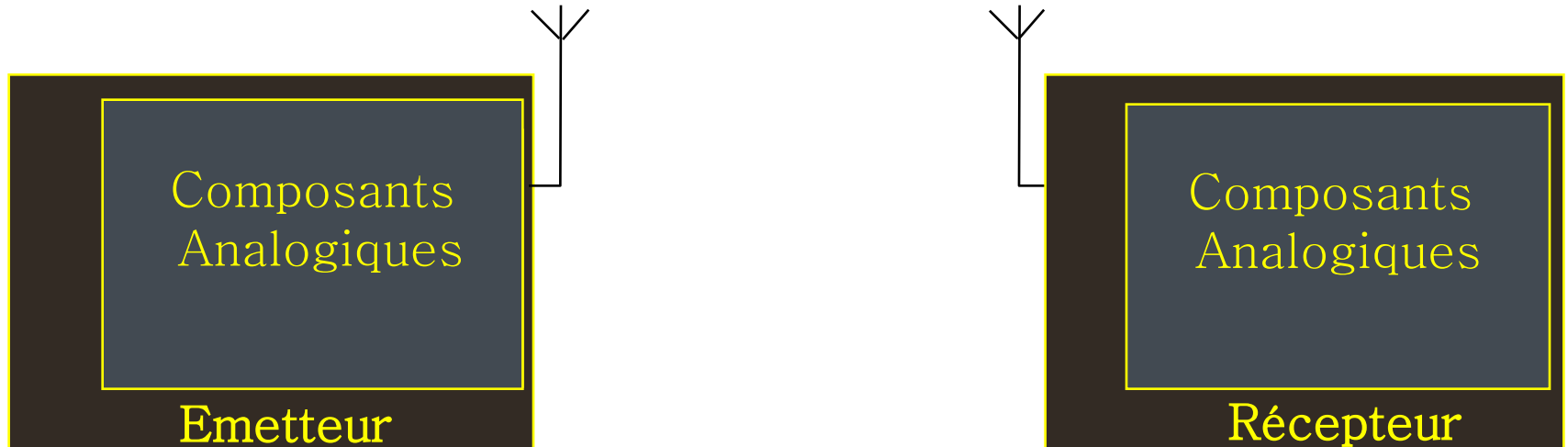
Contribution à l'Etude de l'Opérateur Commun FFT dans le Contexte de la Radio Logicielle: Application au Codage de Canal

Ali AL GHOUWAYEL

**Equipe Signal, Communication, Electronique Embarquée
SUPELEC - IETR**

Contexte de l'étude : La Radio Logicielle

- Concept introduit par Jo Mitola en 1995
- Caractéristiques principales:
 - Sa fonctionnalité est déterminée par logiciel
 - Plusieurs standards peuvent être exécutés sur la même plateforme: **notion du terminal multistandard**



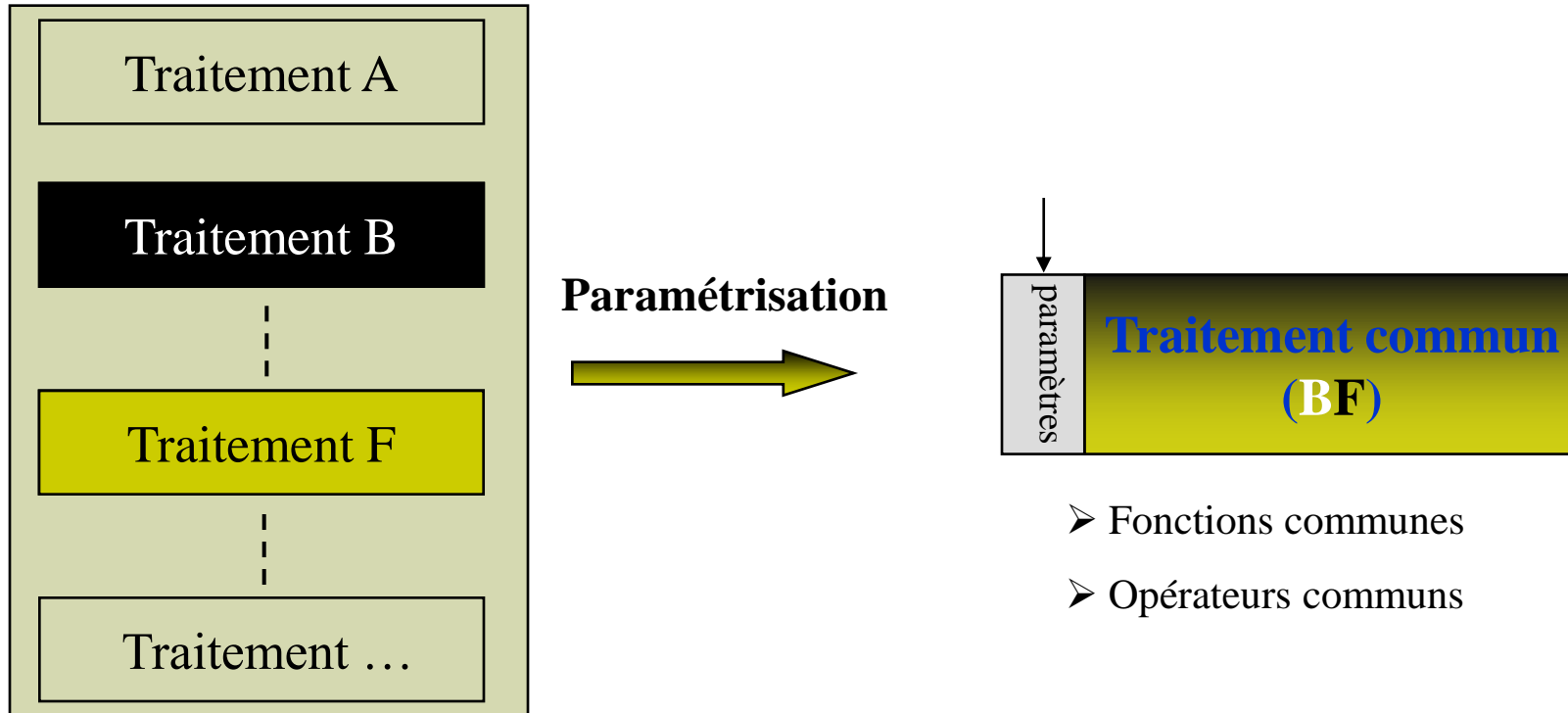
➤ Approches retenues :

- Recherche de traitements communs entre standards
- Mutualisation des traitements



Objectif de la paramétrisation

La paramétrisation :



- Fonctions communes
- Opérateurs communs

- Approche considérée dans la thèse: Opérateur Commun
- Opérateur étudié: FFT

Les différentes fonctions déjà réalisées avec l'opérateur FFT [Palicot03]

- Fonction de filtrage
- Estimation de canal et égalisation
- Fonction Rake
- (De)modulation multiporteuse
- Sélection de canal, ...etc

- **Codage de canal ... ?**

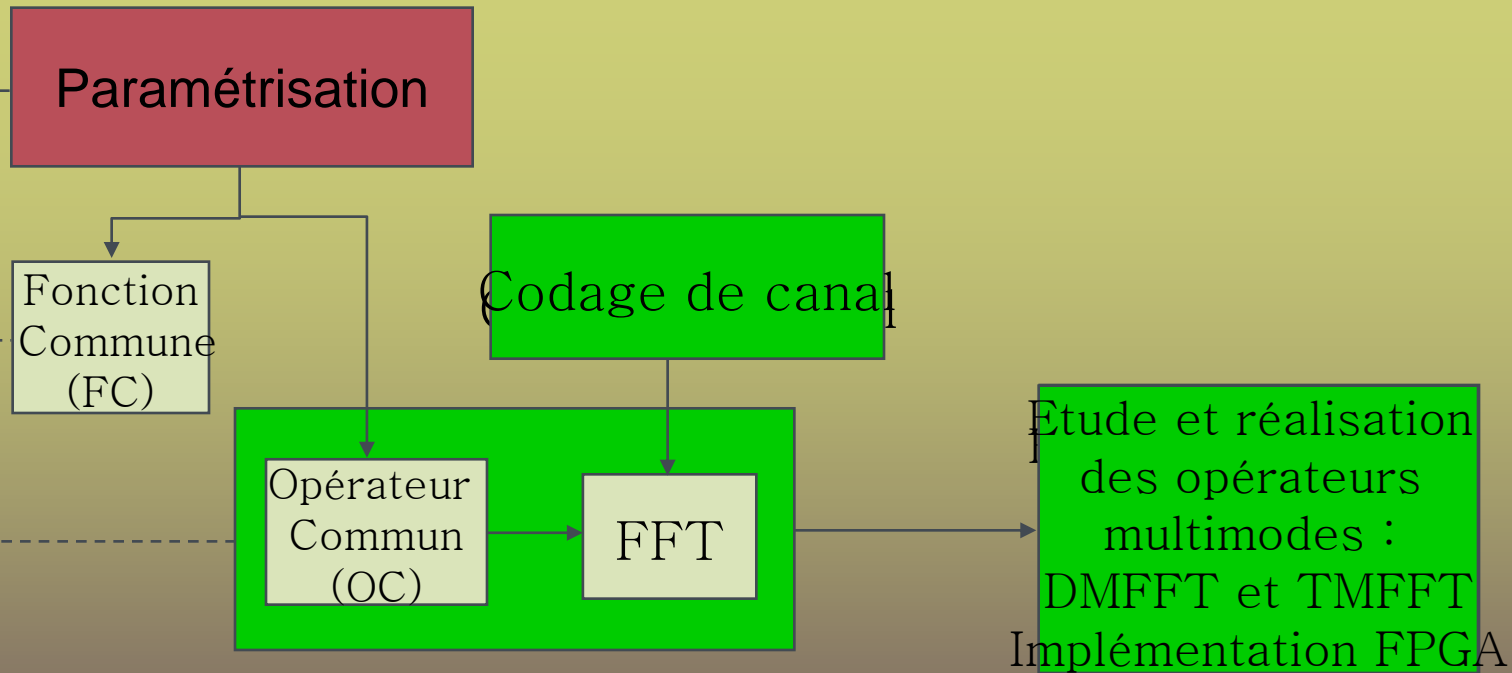
Notre
problématique



**Etendre l'application de l'opérateur
FFT au codage de canal**

[Palicot03] J. Palicot, C. Roland, "FFT: a basic Function for a reconfigurable Receiver", ICT'2003, February 2003, Papeete, Tahiti

Radio Logicielle



0 Introduction

1 La Paramétrisation sous les deux approches FC et OC

2 La FFT et le codage de canal

3 Etude et implémentation de l'opérateur Dual Mode FFT (DMFFT)

4 Vers la réalisation d'un opérateur Triple Mode FFT (TMFFT)

5 Conclusion et perspectives



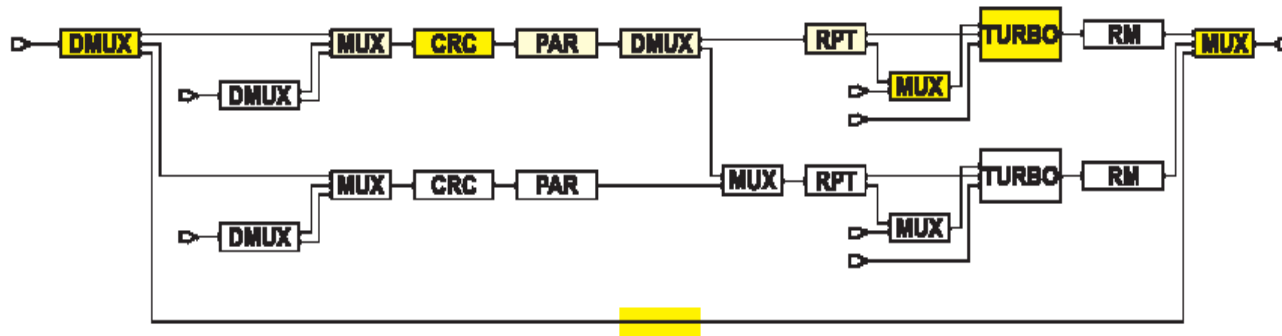
1

La Paramétrisation sous les deux approches FC et OC



La paramétrisation : Approche par Fonction Commune

- **Définition** : c'est la recherche de la fonction utilisée par un ensemble prédéfini de standards et ensuite établir un modèle générique de la fonction identifiée.
- **Exemple** : fonction de codage de canal [Rhiemeier02]



Avantages : Structure commune à trois standards (GSM, TETRAPOL, UMTS)

Inconvénients : évolution impossible et complexité croissante avec le nombre de standards traités

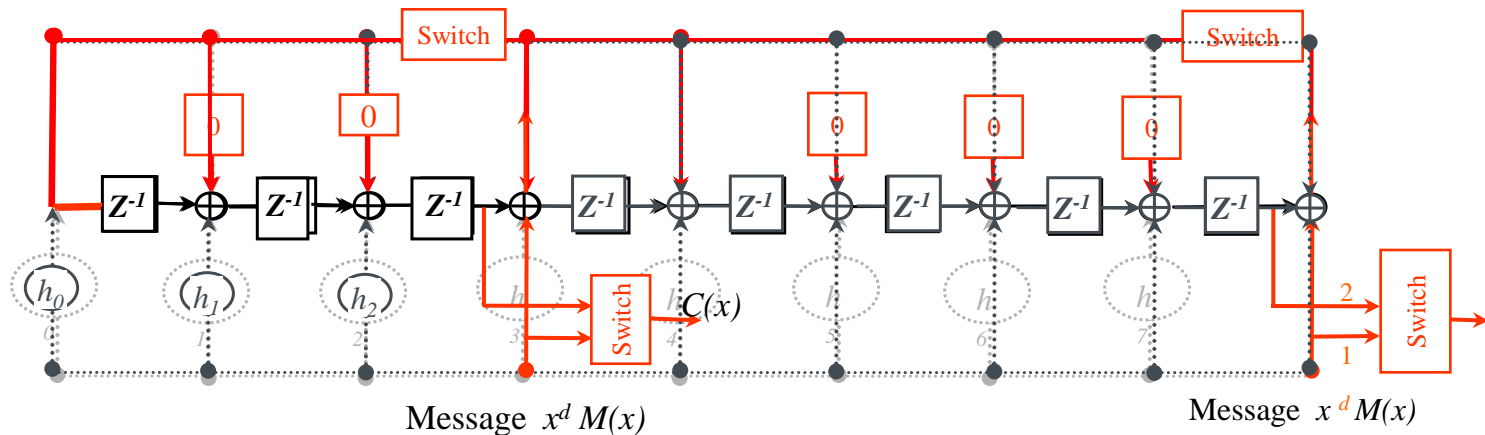
[Rhiemeier02] A. Rhiemeier, "Benefits and Limits of Parameterized Channel Coding for Software-Radio", WSR'02, Germany, March 2002



La paramétrisation : Approche par Opérateur Commun

- **Définition:** A un certain niveau de granularité, c'est la recherche de l'opérateur utilisé par le nombre maximum des fonctions.

1- Opérateur Commun LFSR (Linear Feed-Back Shift Register) [Alaus08]



2- Opérateur Commun : FFT

Objectif déjà défini : Paramétrisation de l'opérateur FFT :

- Adaptation de la structure papillon aux traitements requis par la fonction de **codage de canal**
- Rendre l'architecture reconfigurable

[Alaus08] L. Alaus, D. Noguét and J. Palicot, A Reconfigurable Linear Feedback Shift Register Operator for Software Defined Radio Terminal, ISWPC, May 2008, Santorini, Greece.



2

La FFT et le codage de canal



Codes étudiés dans la thèse : codes en blocs de Reed-Solomon (RS):

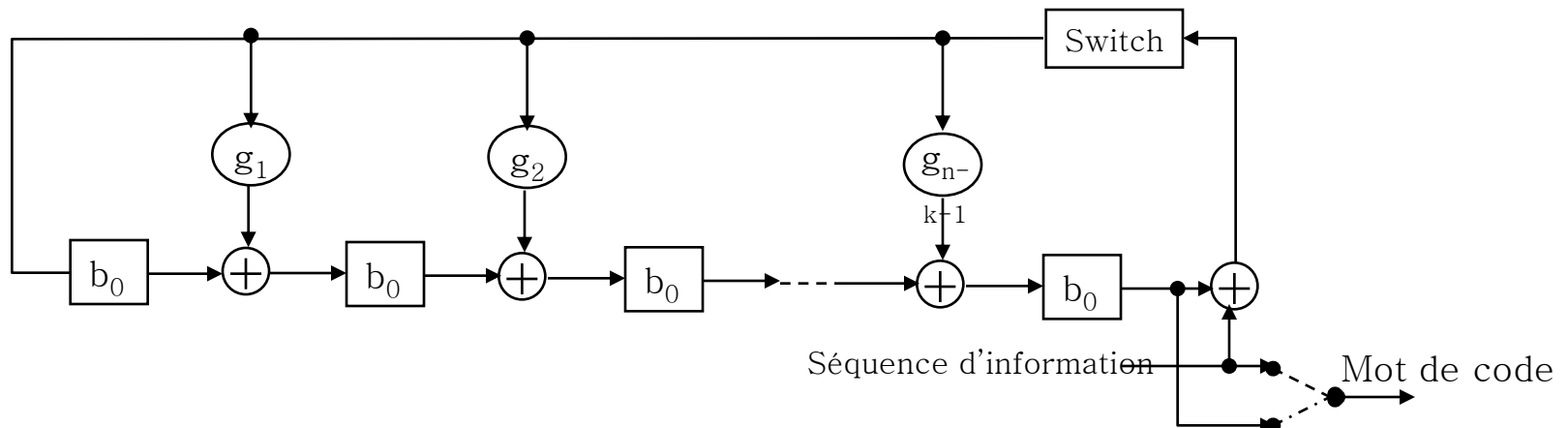
- Codes très puissants
- Codes très utilisés (UMTS (optionnel), 802.16, DVB, ...)
- Adaptés au traitement fréquentiel

➤ Deux traitements possibles pour les codes RS:

- ① Dans le domaine temporel
- ② Dans le domaine fréquentiel



Codage dans le domaine temporel:



$$c(x) = \frac{x^{n-k} m(x)}{g(x)} + m(x)$$

$$g(x) = (x - \alpha^{j_0})(x - \alpha^{j_0+1}) \dots (x - \alpha^{j_0+2t-1})$$

$m(x)$: séquence d'information

$g(x)$: polynôme générateur

$c(x)$: mot de code



Codage dans le domaine fréquentiel:

Mot de code : $\mathbf{c}(\mathbf{x}) = \mathbf{m}(\mathbf{x})\mathbf{g}(\mathbf{x})$ peut être écrit sous la forme d'une convolution :

$$c_i = \sum_{k=0}^{n-1} m_k g_{i-k},$$

$$g(x) = (x - \alpha^{j_0})(x - \alpha^{j_0+1}) \dots (x - \alpha^{j_0+d-2}),$$

Dans le domaine fréquentiel: $C_j = M_j G_j$,

$$C_j = \sum_{i=0}^{N-1} \alpha^{ij} c_i, \quad \Longleftrightarrow \quad c_i = \frac{1}{N} \sum_{j=0}^{N-1} \alpha^{-ij} C_j,$$

C : Transformée de Fourier directe de \mathbf{c} dans le corps fini $\text{CG}(q)$

$$N \leq q - 1,$$

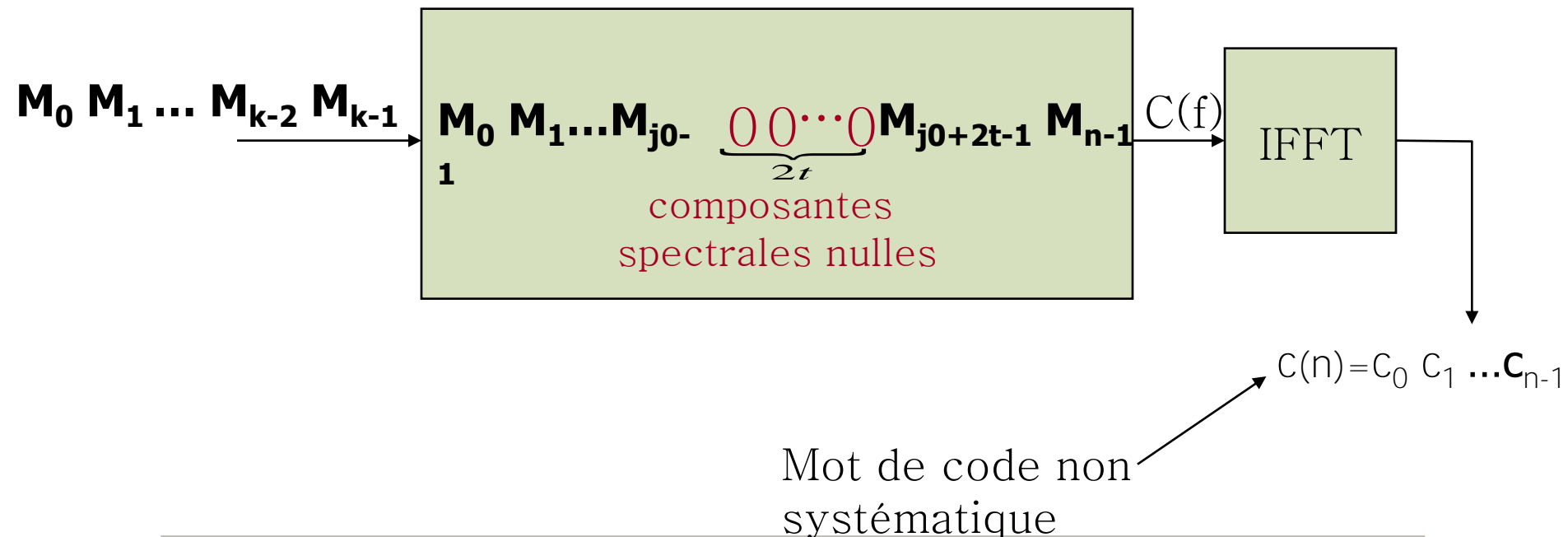
α est un élément primitif d'ordre N du $\text{CG}(q)$, $\alpha^N = 1$.

C_j est nulle si et seulement si α^j est une racine du polynôme $\mathbf{c}(x)$.



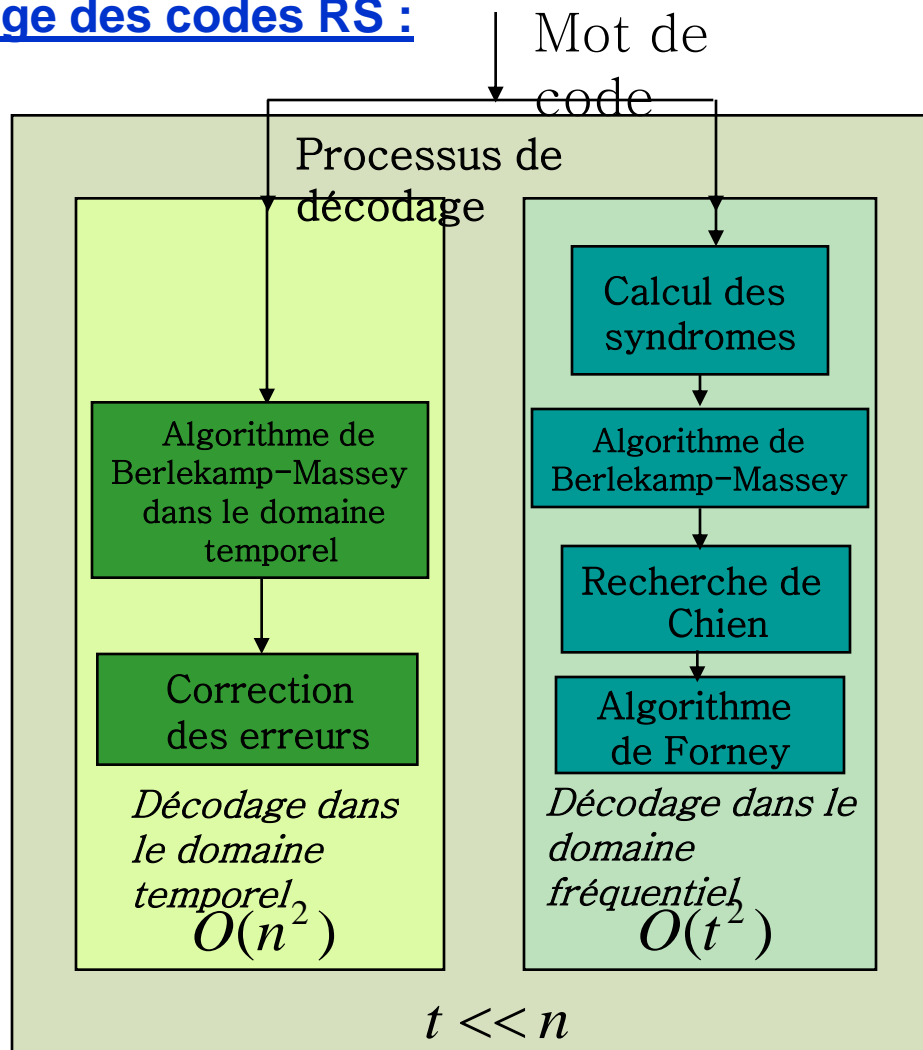
Codage dans le domaine fréquentiel:

- mettre à zéro certaines composantes spectrales
- remplir les autres composantes avec les symboles d'information
- calculer la transformée de Fourier inverse





Processus de décodage des codes RS :



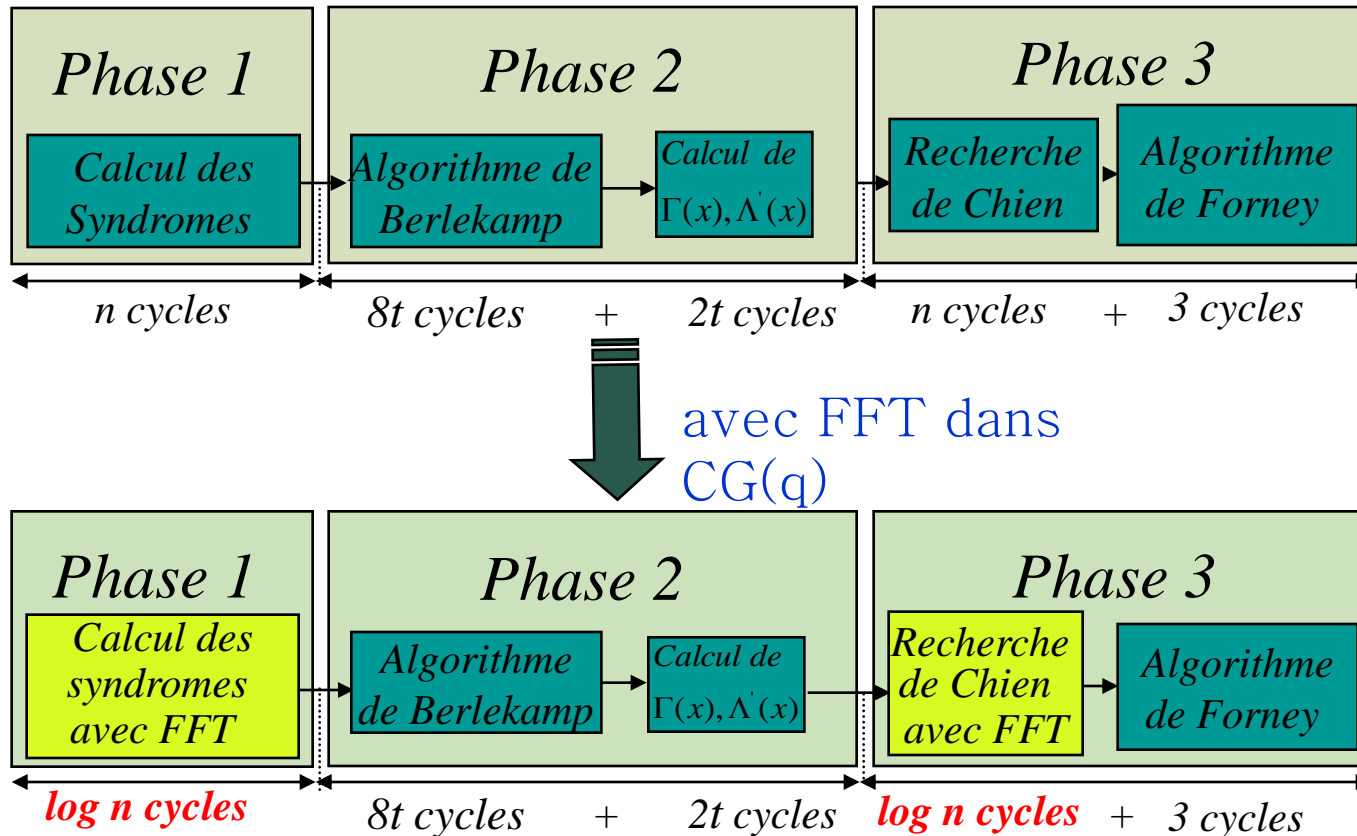
n: longueur des mots de code

t: pouvoir de correction

Décodage fréquentiel plus efficace



Les trois phases du décodage fréquentiel RS :





- La FFT considérée est définie dans le corps fini $\mathbb{C}\mathbb{G}(q)$

Objectif : réaliser un opérateur FFT commun

Quelle architecture commune ?

Démarche :

- Partir de la structure de base de la FFT définie dans \mathbb{C}
- La faire évoluer pour obtenir un opérateur réalisant des transformées dans \mathbb{C} et $\mathbb{C}\mathbb{G}(q)$



☛ Pour pouvoir utiliser les algorithmes efficaces de calcul de la transformée de Fourier, il faut avoir les caractéristiques suivantes:

1. Longueur de transformée de la forme 2^n

2. Les propriétés de symétrie: $\alpha^N = 1$, $\alpha^{k+N} = \alpha^k$ et $\alpha^{k+\frac{N}{2}} = -\alpha^k$

⊗ **Mais:** la longueur des transformées utilisées dans le traitement fréquentiel des codes RS classiques définis dans $CG(2^n)$ est $2^n - 1$

⊗ **Donc** le traitement fréquentiel des codes RS classiques définis dans $CG(2^n)$ ne correspond pas à la structure classique de l'opérateur FFT défini dans \mathbb{C} .

Recherche de codes RS définis dans $CG(q)$, avec $q = 2^n + 1$.



✓ Codes retenus : les codes RS définis dans $CG(F_t)$,

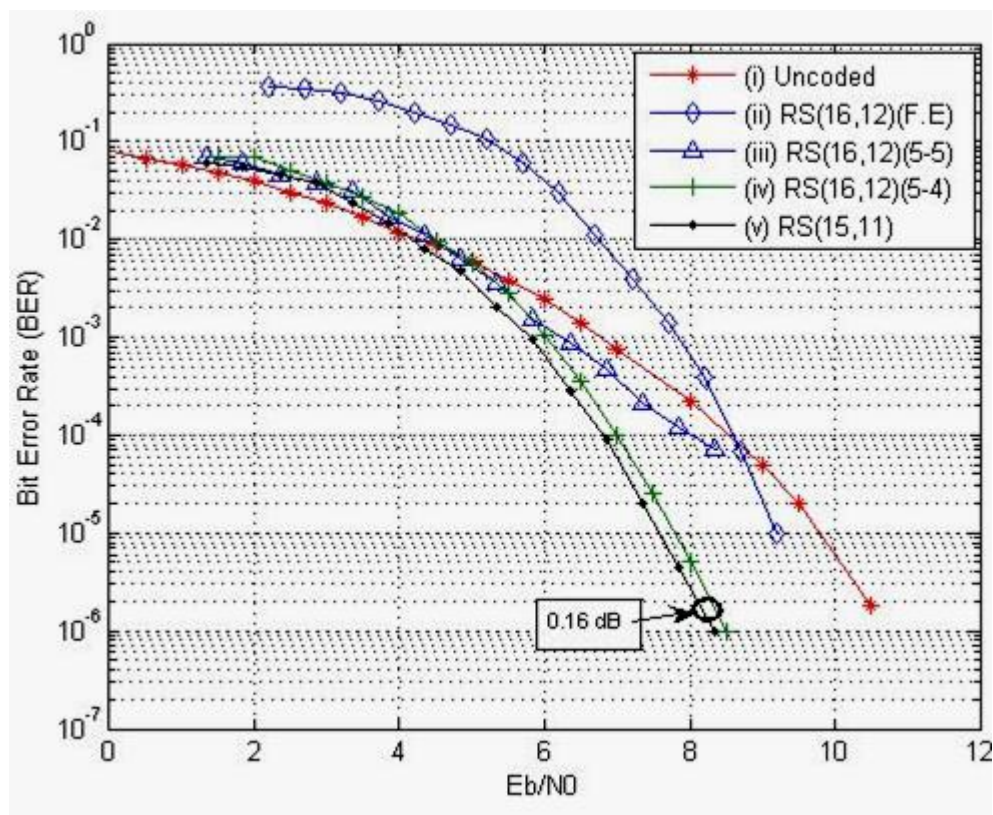
- $F_t = 2^{2^t} + 1$ est un nombre de Fermat,
- F_0, F_1, F_2, F_3, F_4 sont les seuls nombres premiers,
- Les principes de codage et de décodage sont les mêmes que ceux des codes RS définis dans $CG(2^n)$
- Les opérations arithmétiques sont des opérations modulo (F_t) .
- La FFT associée : Transformée de Fermat FNT (Fermat Number Transform)

Ces codes ont été recommandés pour l'utilisation dans les applications de communications spatiales de l'agence spatiale européenne (ESA) [Best81]

[Best81] M.R. Best, H. F. A Roefs, « Technical assistance telemetry channel coding investigation », Contract no. 4184/79/NL/HP, Final report 1981. National Aerospace Laboratory, Amsterdam, The Netherlands.



Performances des codes RS définis dans CG($F_t=17$):



Choix du code validé



3

Etude et implémentation de l'opérateur Dual Mode FFT (DMFFT)



Etude et conception de l'opérateur commun DMFFT

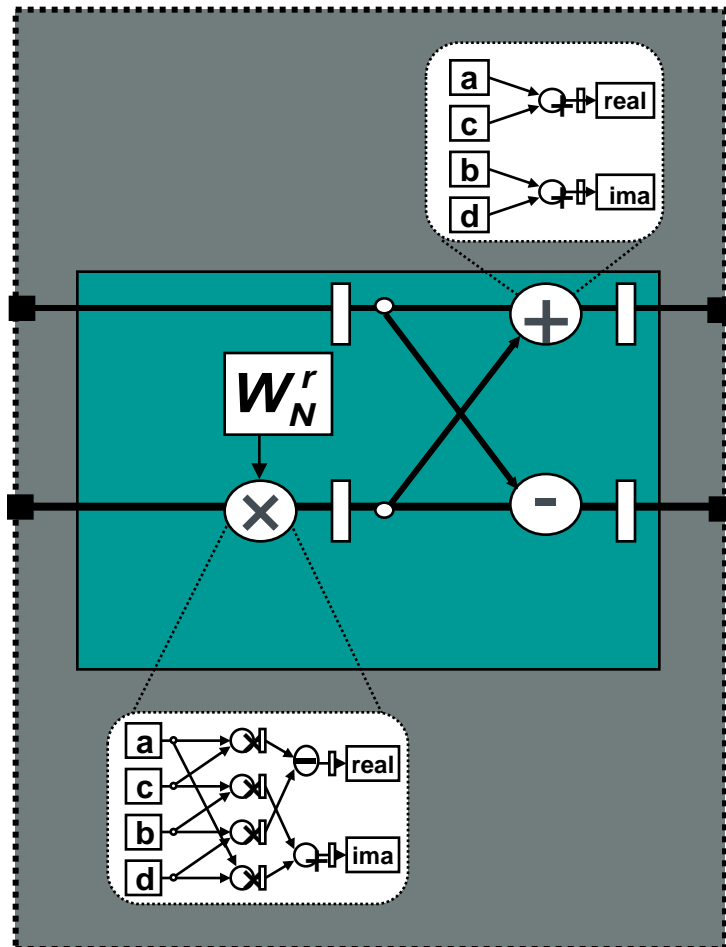
Elément de base : papillon complexe

Démarche :

- 1- Etude théorique des algorithmes de multiplication et d'addition dans $\mathbb{C}G(F_t)$
- 2- **Implémentation des opérateurs modulo (F_t) sur les opérateurs complexes**
- 3- **Réalisation pratique du papillon dual mode**
- 4- **Réalisation du DMFFT**



Papillon complexe classique



1 multiplieur complexe (4 multiplieurs réels)

1 additionneur complexe (2 additionneurs réels)

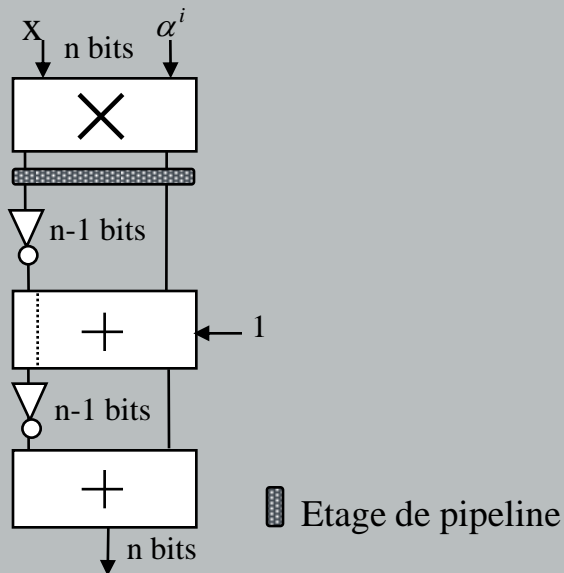
1 soustracteur complexe (2 soustracteurs réels)



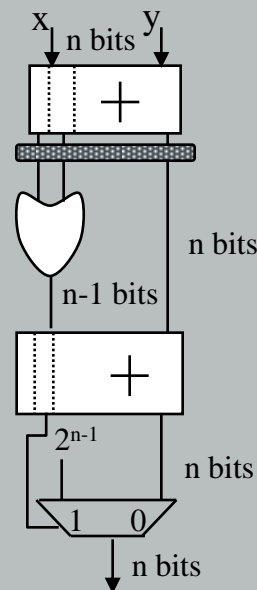
□ Pour réaliser un papillon reconfigurable :

- Les opérateurs arithmétiques doivent être reconçus pour réaliser des opérations dans C ainsi que dans $CG (F_t)$
- Les interconnexions doivent être reconfigurables

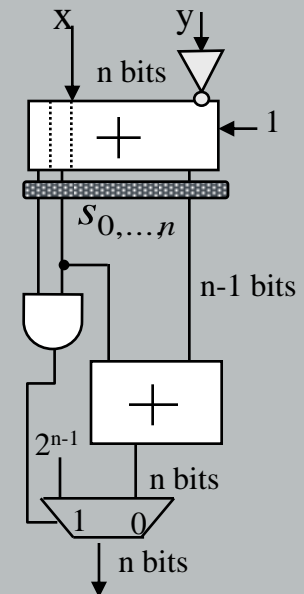
Opérateurs arithmétiques proposés dans cette thèse:



a. Multiplieur modulo (F_t)



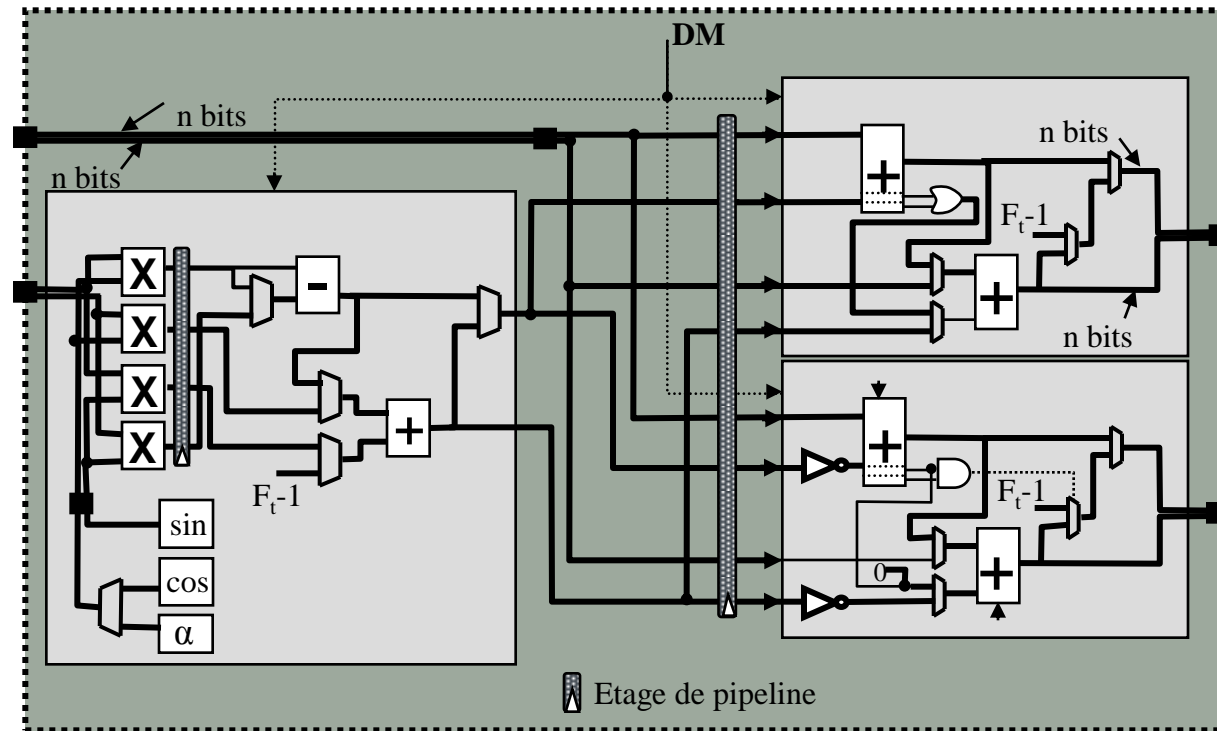
b. Additionneur modulo (F_t)



c. Soustracteur modulo (F_t)



Architecture du Papillon Dual Mode proposée dans cette thèse:

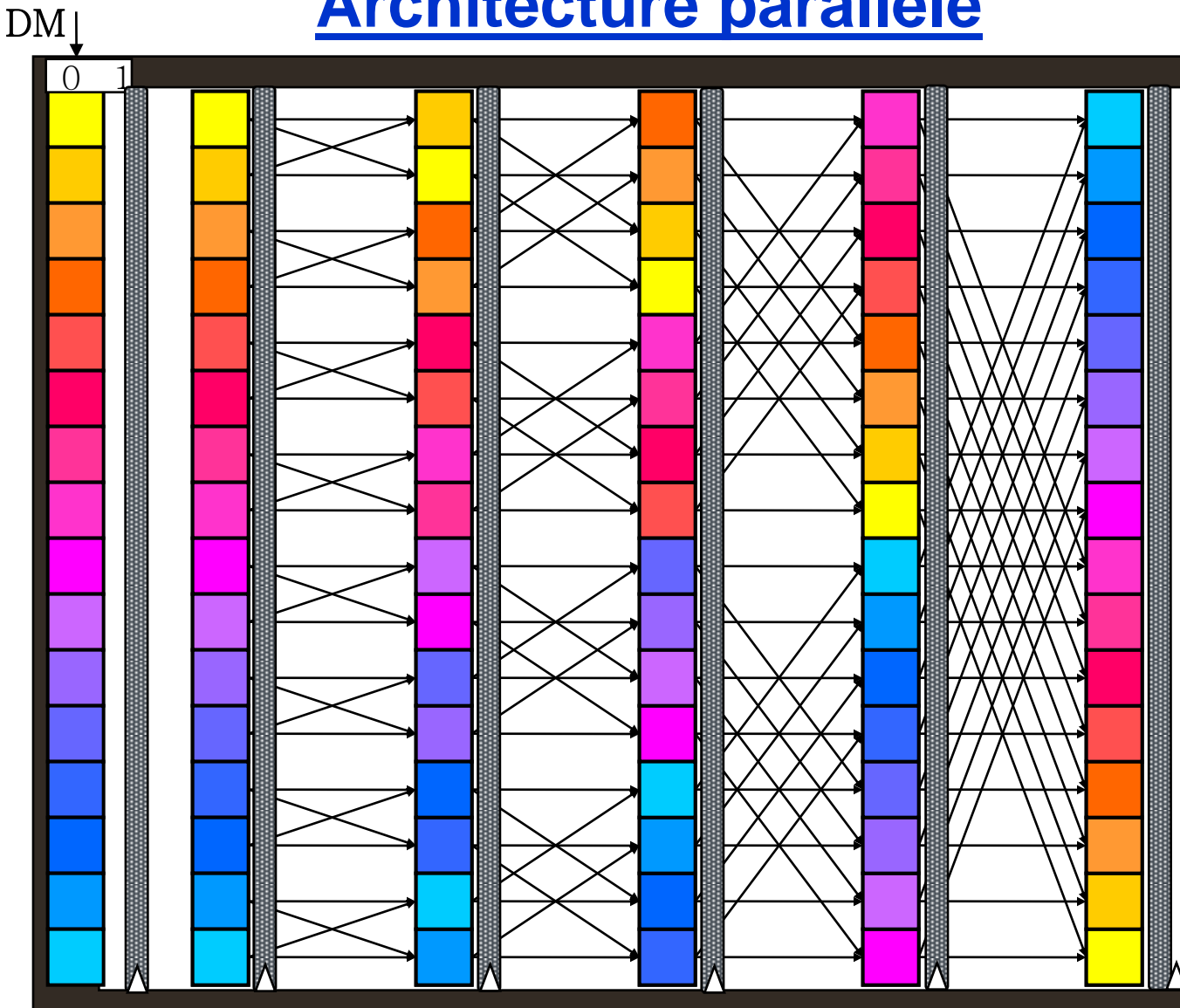


Deux architectures possibles de l'opérateur DMFFT:

- Architecture parallèle
- Architecture série



Architecture parallèle



Log N étages

$N/2$ papillons par étage

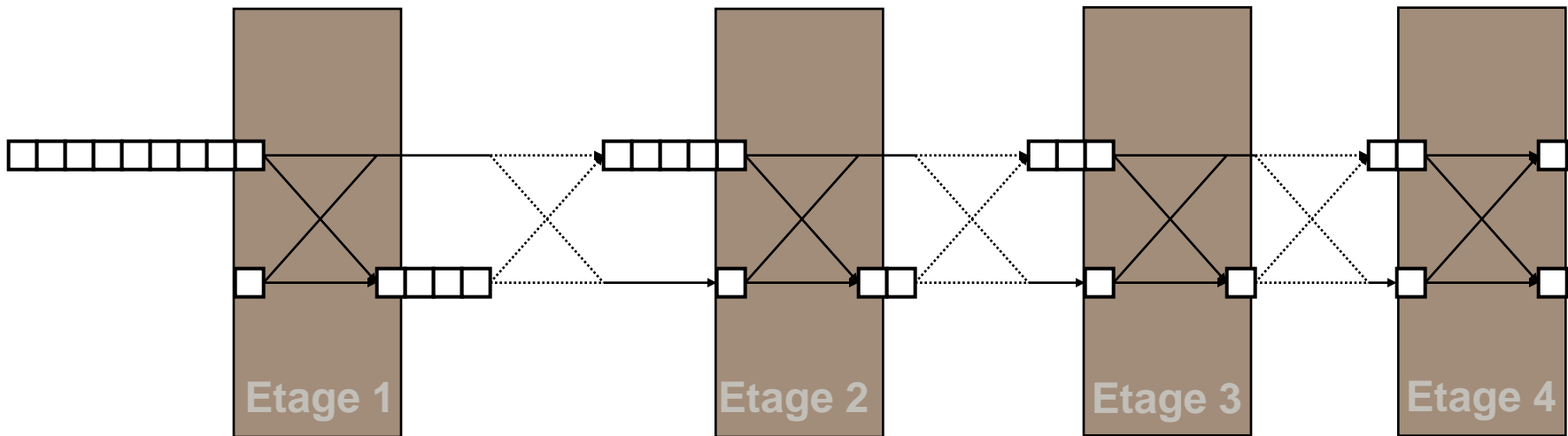
Avantage:
Architecture rapide

Inconvénient:
Architecture complexe



Architecture série

Un papillon par étage



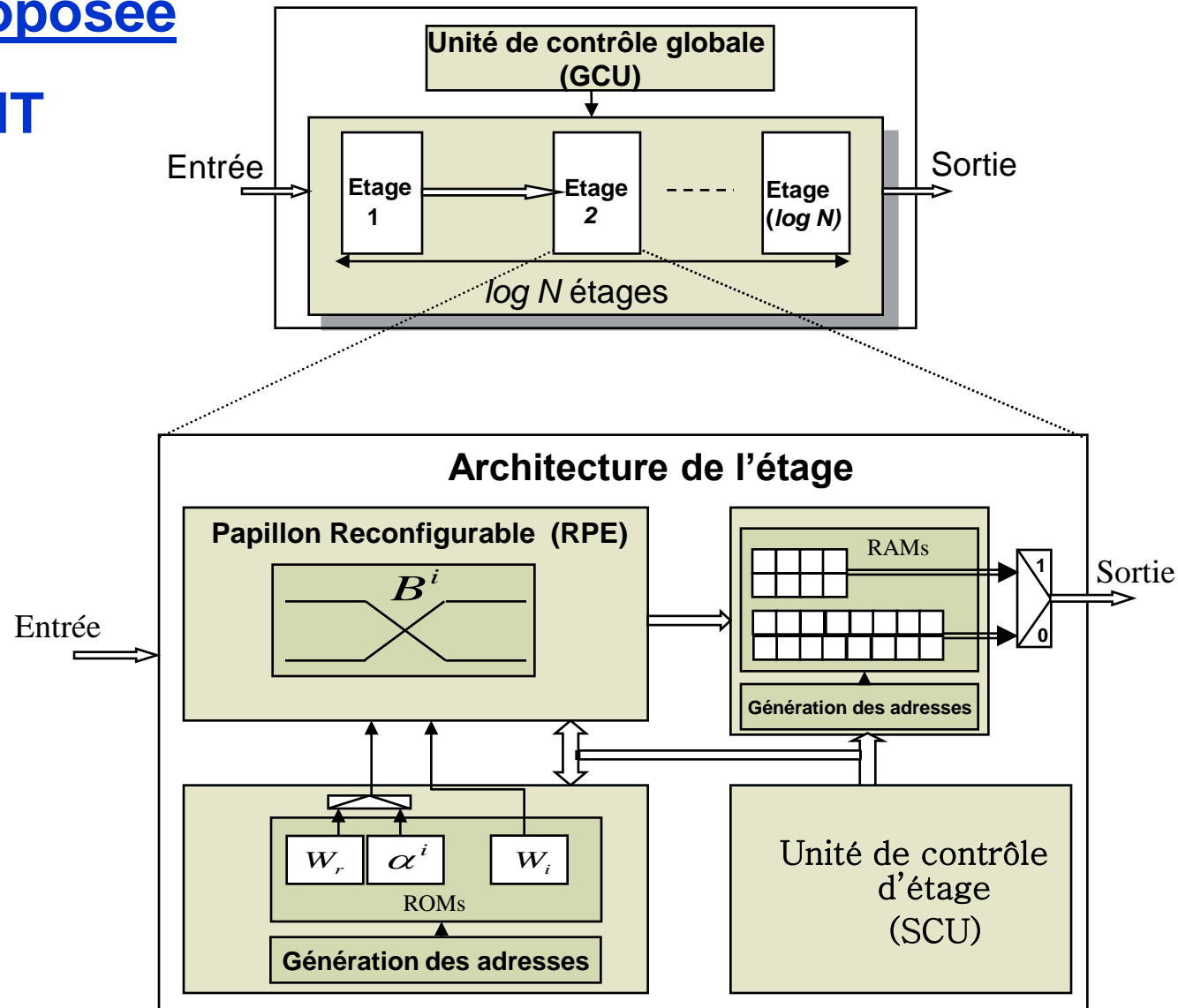
FFT-16

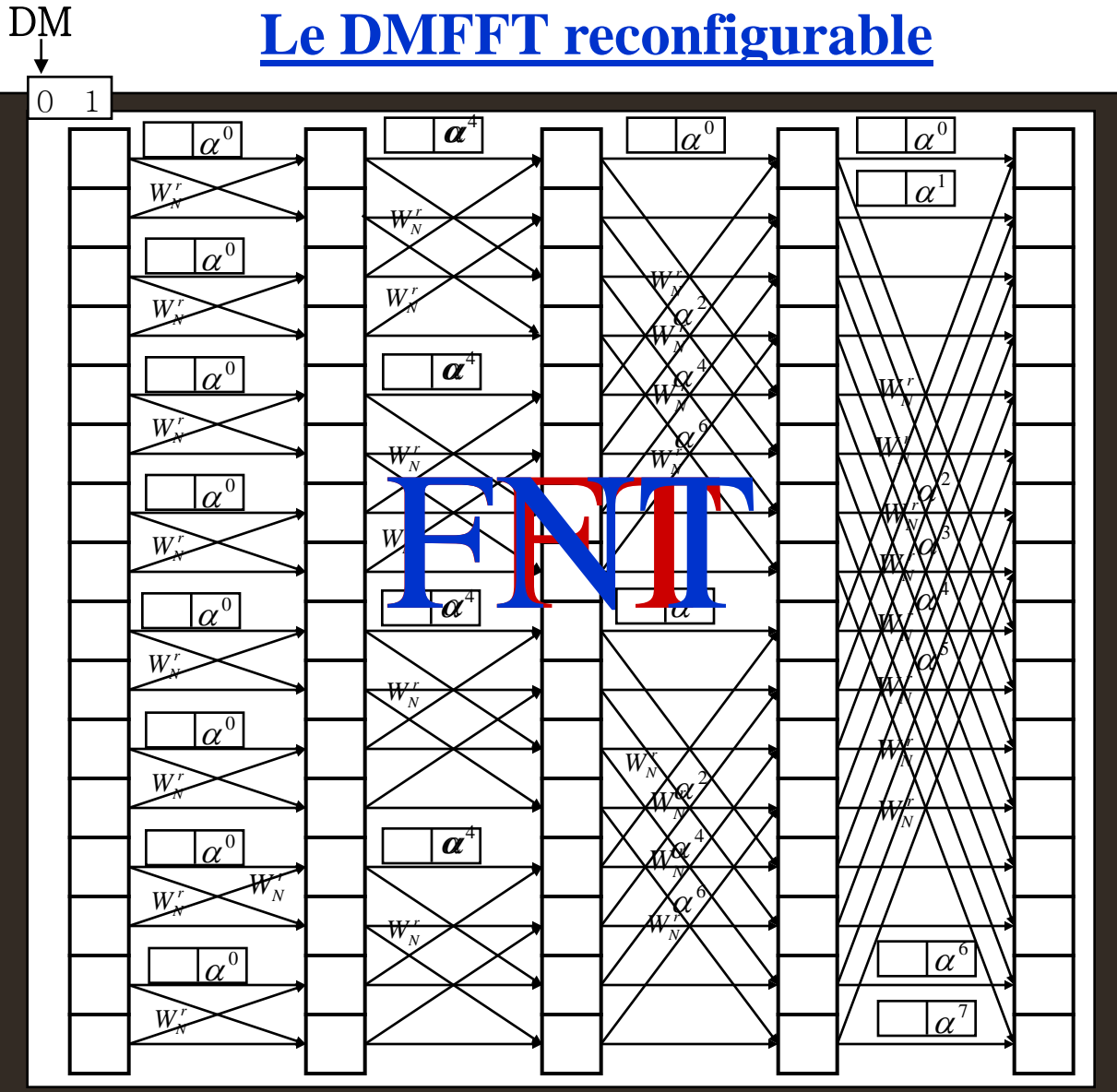
Bon compromis complexité - rapidité



Architecture proposée

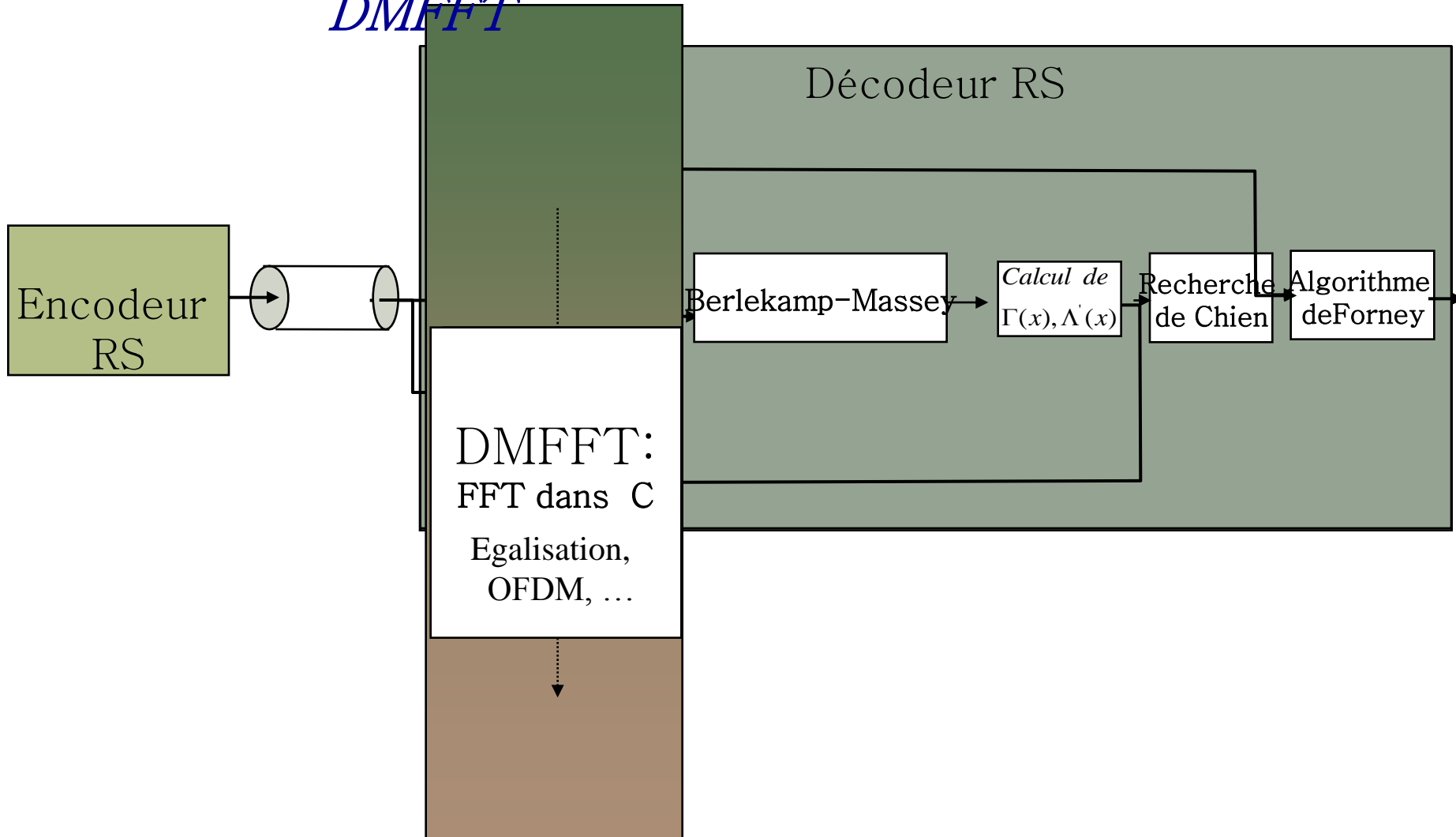
DMFFT : FFT/FNT





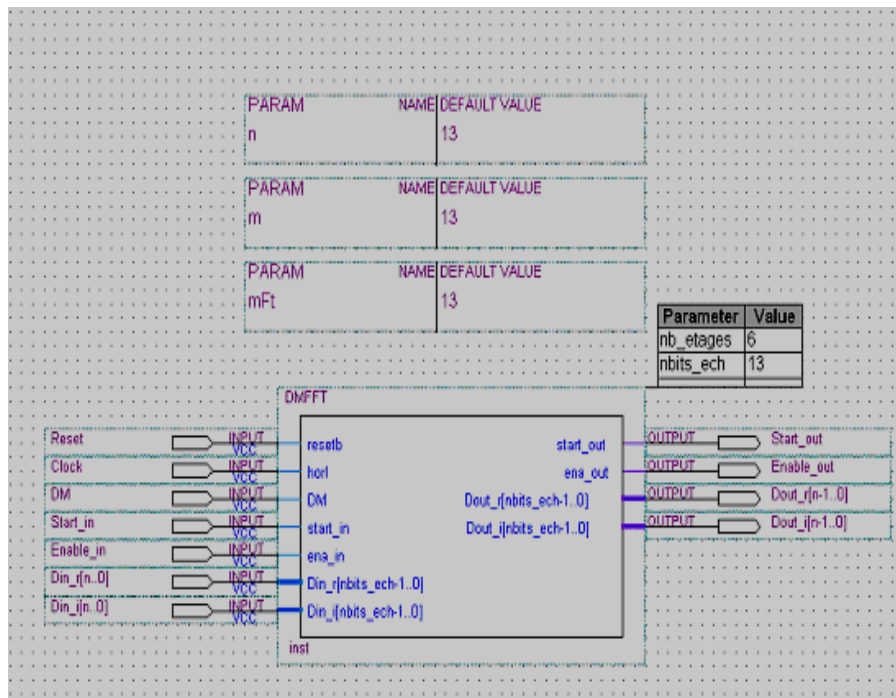


Principe de l'opérateur Commun DMFFT

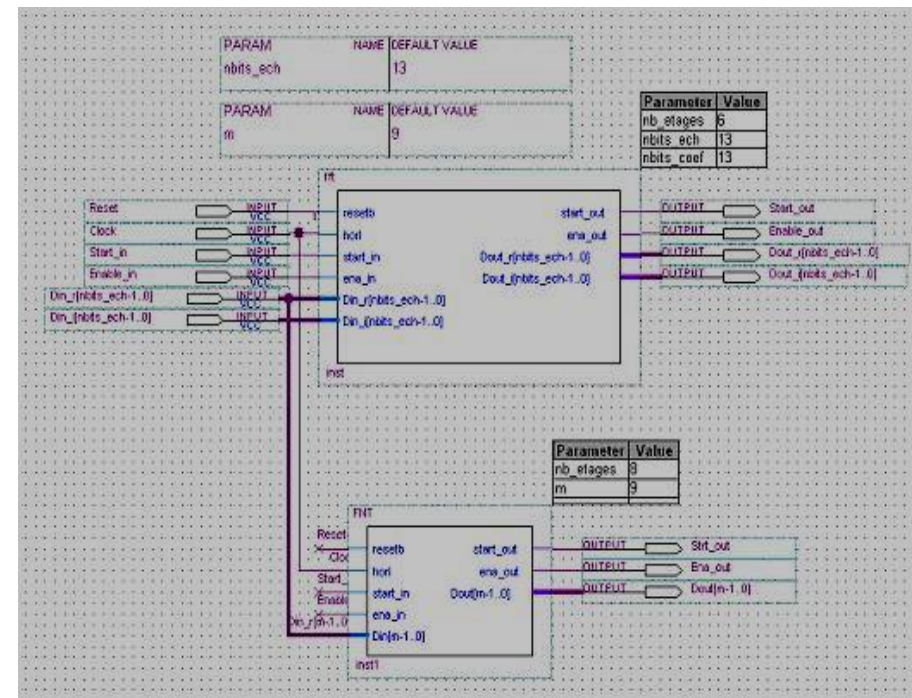




Implémentation du DMFFT sur FPGA - Altera Stratix II



Approche reconfigurable: DMFFT



Approche Velcro: FFT et FNT



Implémentation FPGA, virgule fixe

Gains de l'approche DMFFT vs Velcro

1- Gain en mémoire de 22 – 33 %

2- Evaluation du paramètre:

$$\eta = \frac{1}{TC}$$

T: temps d'exécution (ns)

C: nb. d'ALUTs

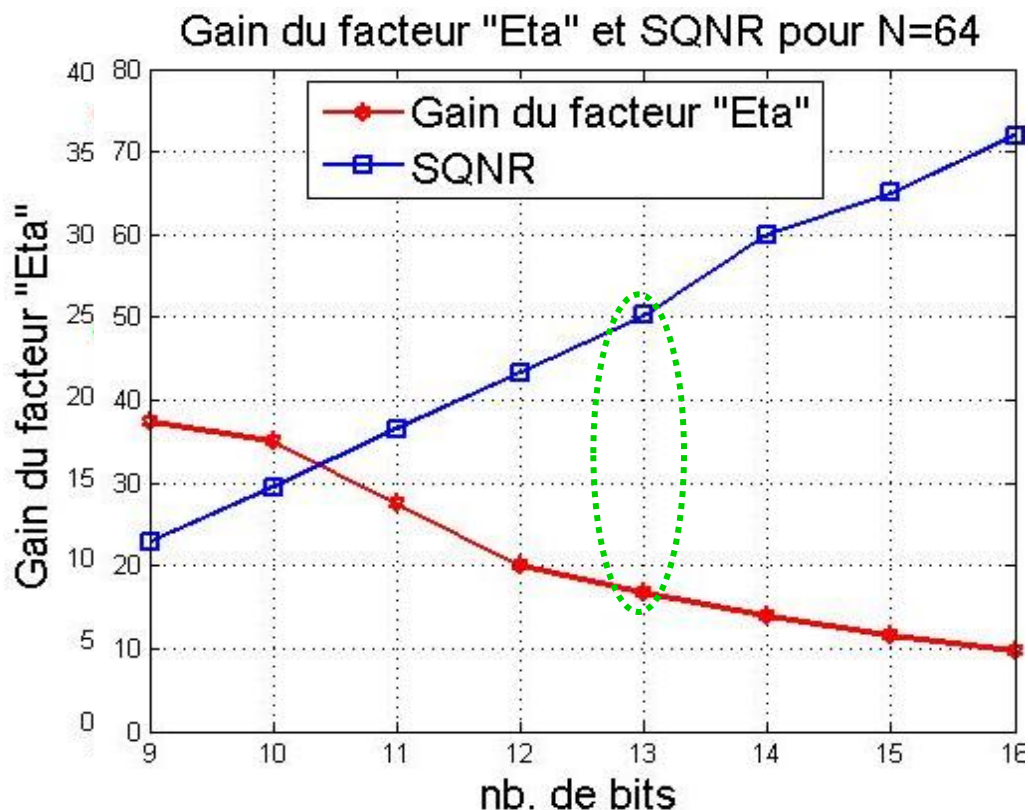
3- Evaluation de la précision

$$SQNR = 10 \log \left(\frac{E[|S(K)|^2]}{E[|N(K)|^2]} \right)$$

(Signal to Quantization Noise Ratio)

S(K): moyenne quadratique du signal (virgule flottante)

N(k): moyenne quadratique de l'erreur de quantification





.✓ DMFFT réalisée (deux fonctionnalités: FFT et FNT)

→ Etape suivante : réalisation d'un opérateur triple mode

Triple mode FFT : FFT + FNT + FFT dans CG(2^m)

Objectif: étendre le traitement fréquentiel avec l'opérateur FFT vers les codes RS définis dans CG(2^m)

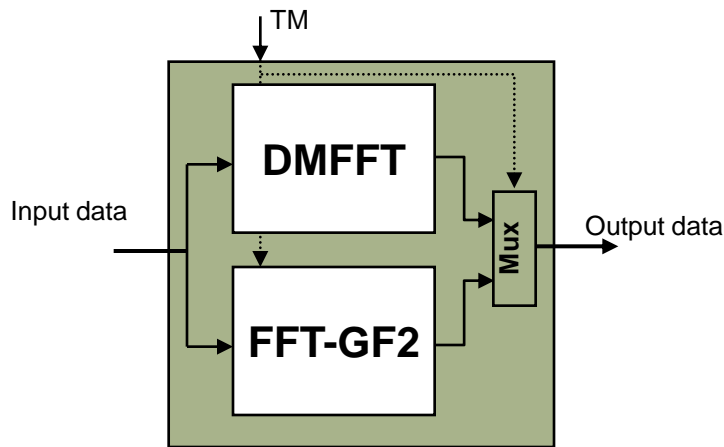


4

Vers la réalisation d'un opérateur Triple Mode FFT (TMFFT)



Architecture de départ:



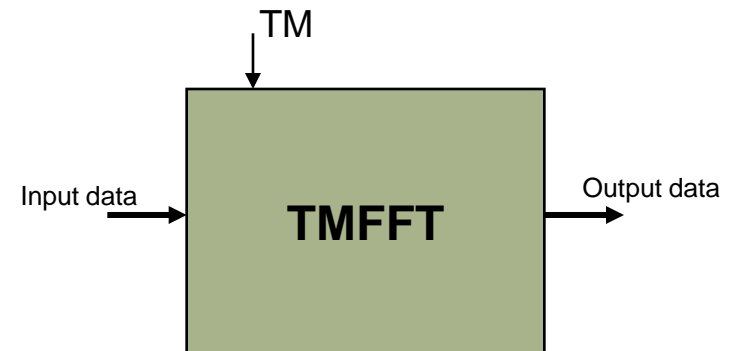
(FFT dans $CG(2^m)$: FFT-GF2)

Version Velcro : TM~~V~~FFT

Scénari proposés:

Scénario 1: accélération matérielle des opérateurs DMFFT et FFT-GF2

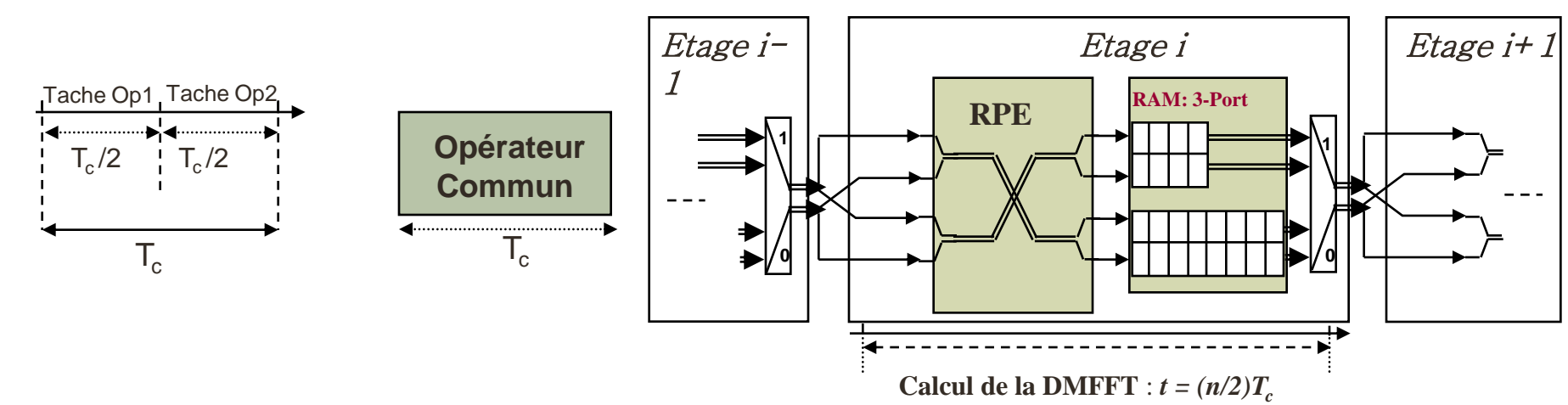
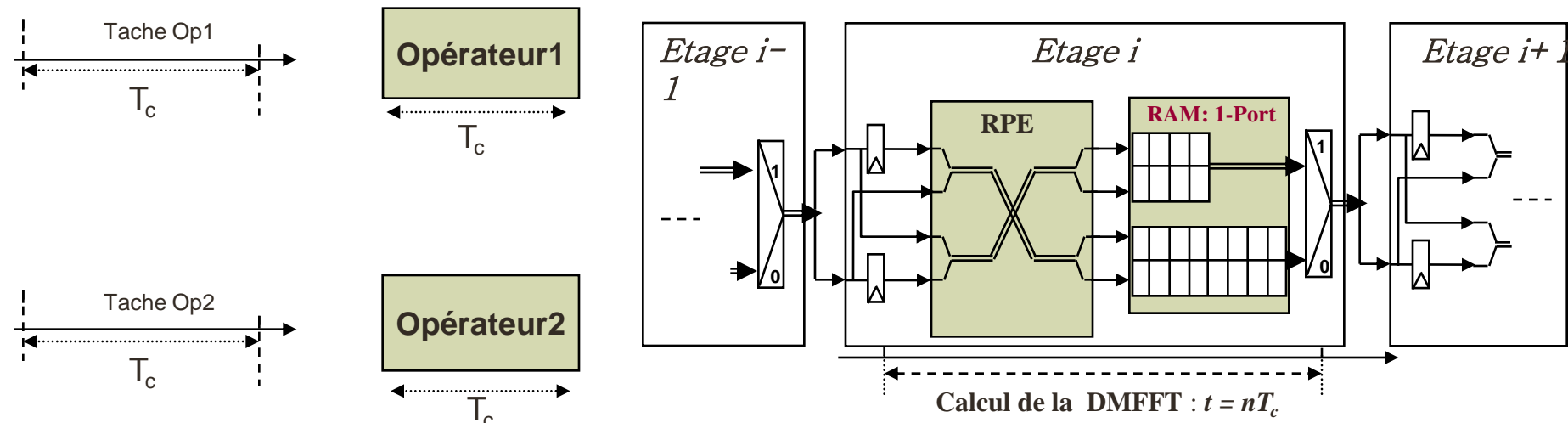
Scénario 2: Mutualisation des deux opérateurs DMFFT et FFT-GF2 pour obtenir un seul opérateur reconfigurable TMFFT



TMFFT reconfigurable



Scénario 1 : Accélération matérielle de l'opérateur DMFFT

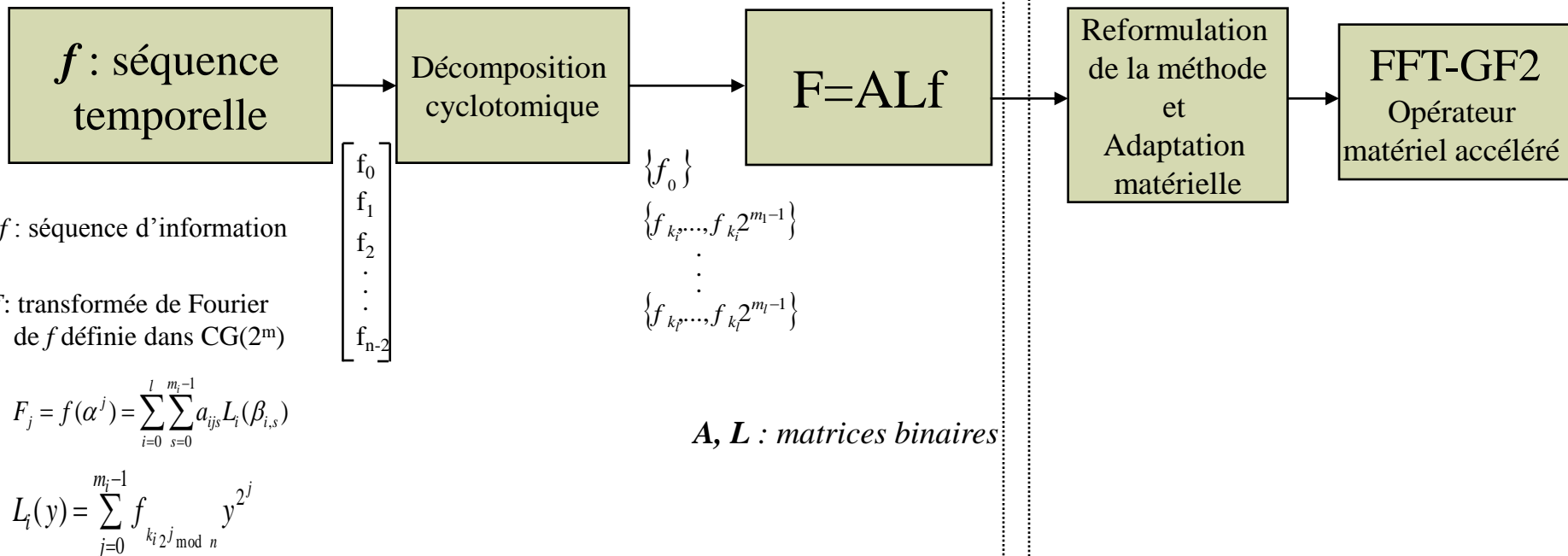




Scénario 1 : Accélération matérielle de l'opérateur FFT-GF2

Aspect algorithmique [Fedorenko03]

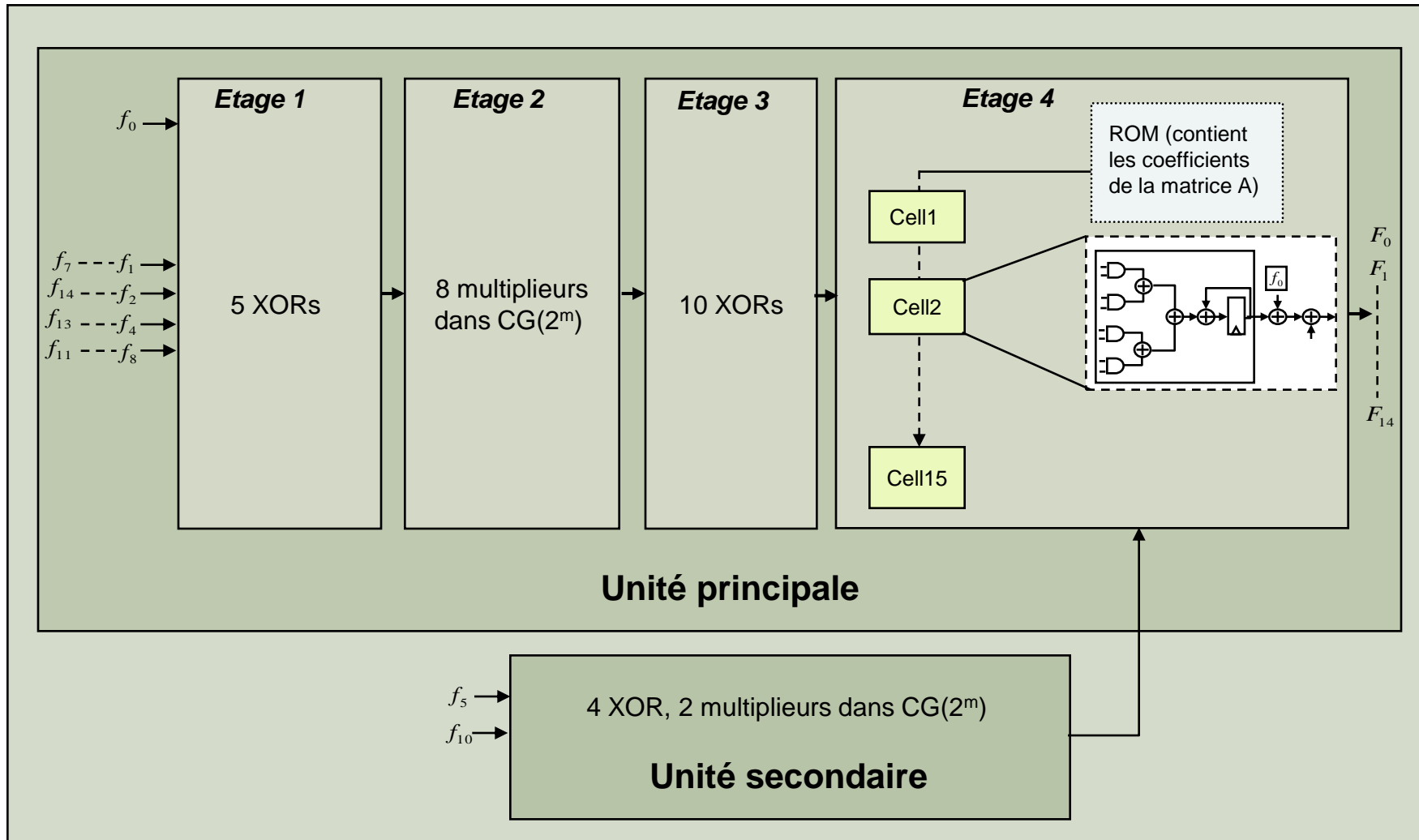
Contribution :
Aspect architectural



[Fedorenko03] S. V. Fedorenko and P. V. Trifonov, A method for Fast Computation of the Fast Fourier Transform over a Finite Field, Problems of Information Transmission, 39(3):231-238, July-September 2003. Translation of Problemy Peredachi Informatisii.



Architecture matérielle proposée pour FFT-15 dans CG(16)





Décomposition cyclotomique des différents corps de Galois $CG(2^m)$: Temps d'exécution théoriques basés sur l'architecture du dernier étage

CG	Groupes cyclotomiques
$CG(2^3)$	1 $C\{1\}$, 2 $C\{3\}^*$
$CG(2^4)$	1 $C\{1\}$, 1 $C\{2\}$, 3 $C\{4\}$
$CG(2^5)$	1 $C\{1\}$, 6 $C\{5\}$
$CG(2^6)$	1 $C\{1\}$, 1 $C\{2\}$, 2 $C\{3\}$, 9 $C\{6\}$
$CG(2^7)$	1 $C\{1\}$, 18 $C\{7\}$
$CG(2^8)$	1 $C\{1\}$, 1 $C\{2\}$, 3 $C\{4\}$, 30 $C\{8\}$

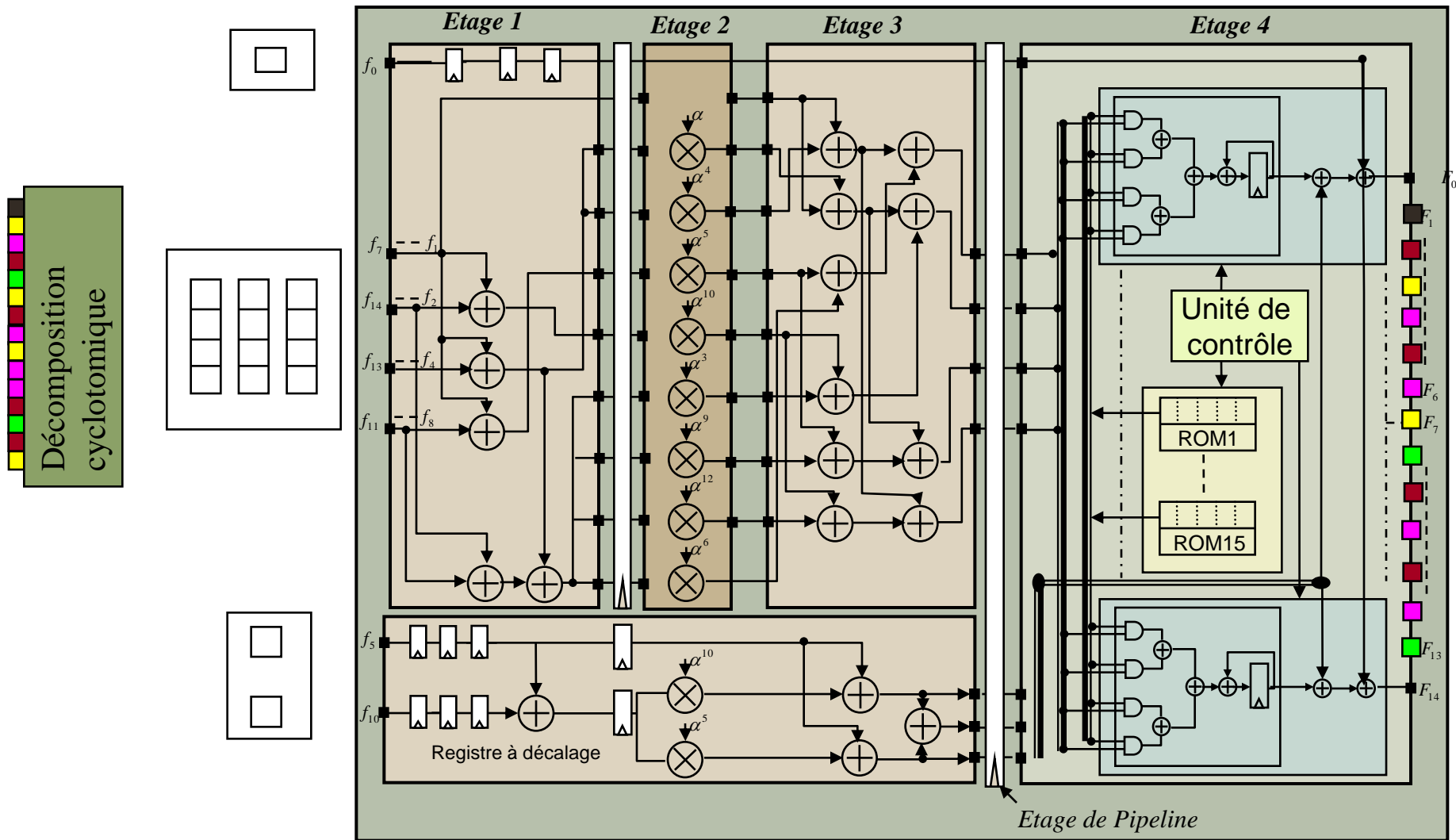
CG	Temps d'exécution (architecture [Wang98])	nb. de groupes	nb. de cellules	Temps d'exécution (architecture proposée)
$CG(2^4)$	$16 T_c$	3	8	$6 T_c$
			15	$3 T_c$
$CG(2^5)$	$32 T_c$	6	16	$12 T_c$
			31	$6 T_c$
$CG(2^6)$	$64 T_c$	9	32	$18 T_c$
			63	$9 T_c$
$CG(2^7)$	$128 T_c$	18	64	$36 T_c$
			127	$18 T_c$
$CG(2^8)$	$256 T_c$	30	64	$120 T_c$
			128	$60 T_c$
			255	$30 T_c$

T_c : temps de multiplication dans $CG(2^m)$

[Wang98] Y.Wang and X. Zhu, « A Fast Algorithm for the Fourier Transform over Finite Fields and its VLSI Implementation », IEEE Journal on Selected Areas in Communications, vol. 6, no. 3, April 1998.



Vue interne et traitement des données:





Etude de complexité et comparaison des performances avec [Wang98] :

Implémentation FPGA sur STRATIX II du FFT-15 (m = 4)

$$t = 16T_c \text{ [Wang98]}$$

T_c : temps de multiplication dans CG(2^m)

Architecture	nb. de multiplieurs	nb. de portes XOR	Temps d'exécution
[Wang98]	$\frac{1}{2}m(m+1)$	$\frac{1}{2}m(m+1)$	t
Architecture proposée	$\leq \frac{1}{2}m(m+1)$	$> \frac{1}{2}m(m+1)$	$t' = \frac{t}{\beta}, \beta = [2, \dots, 8]$

Temps d'exécution	nb. de cellules	Surface	T_c
$t' = 3 T_c$	15	343 ALUTs	2 ns
$t' = 6 T_c$	8	203 ALUTs	2 ns

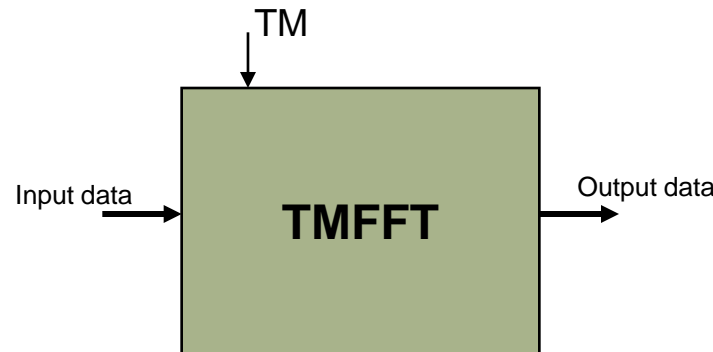
Opérateur FFT-GF2 flexible et rapide

[Wang98] Y.Wang and X. Zhu, « A Fast Algorithm for the Fourier Transform over Finite Fields and its VLSI Implementation », IEEE Journal on Selected Areas in Communications, vol. 6, no. 3, April 1998.



Scénario 2: Mutualisation matérielle du DMFFT et FFT-GF2

Vers un opérateur TMFFT:

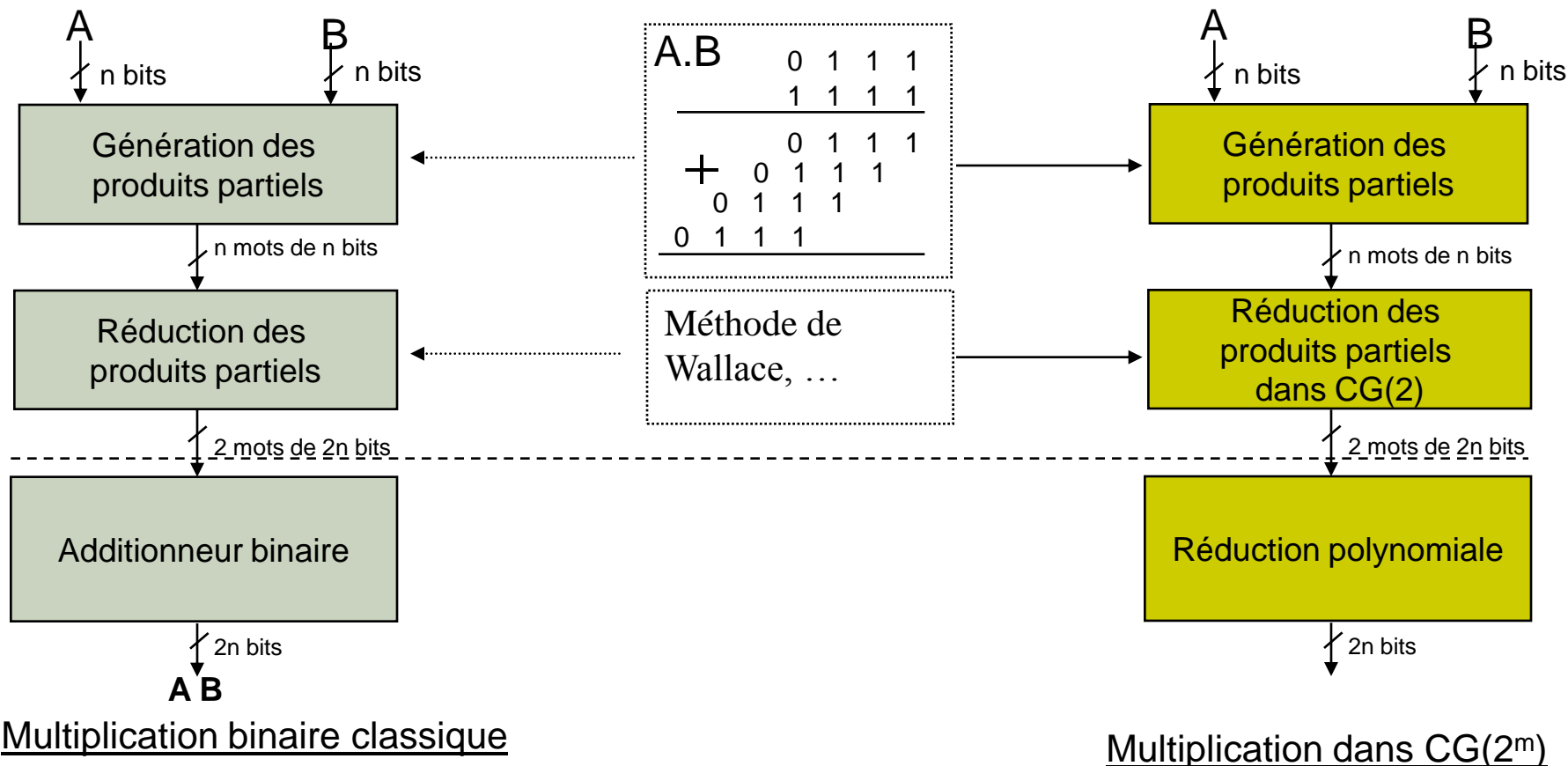


Deux étapes :

- 1- Réalisation des opérateurs arithmétiques triple modes
- 2- Elaboration d'une méthodologie d'incorporation du FFT-GF2 dans DMFFT



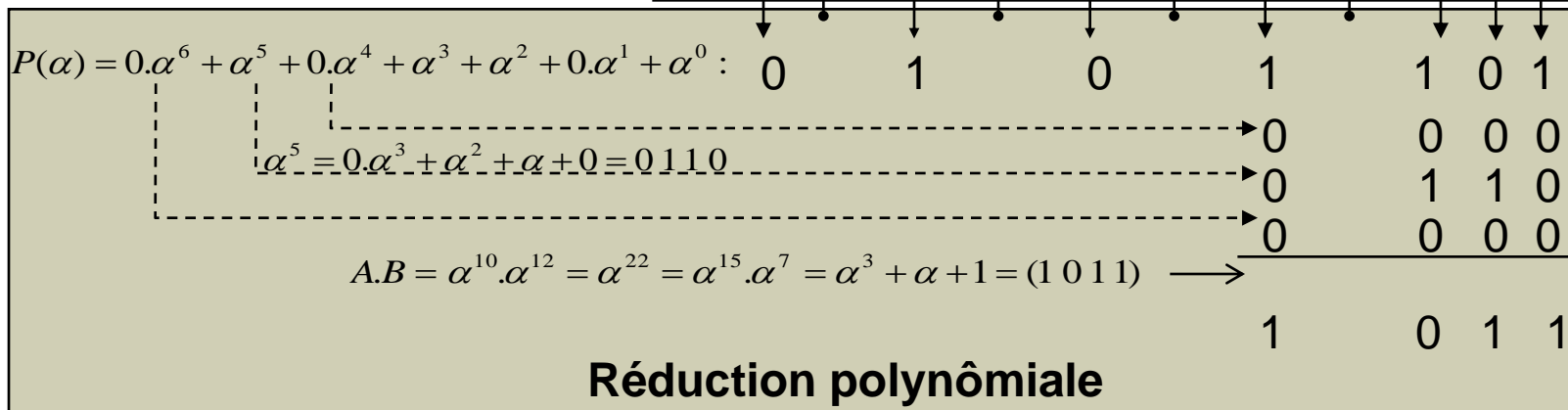
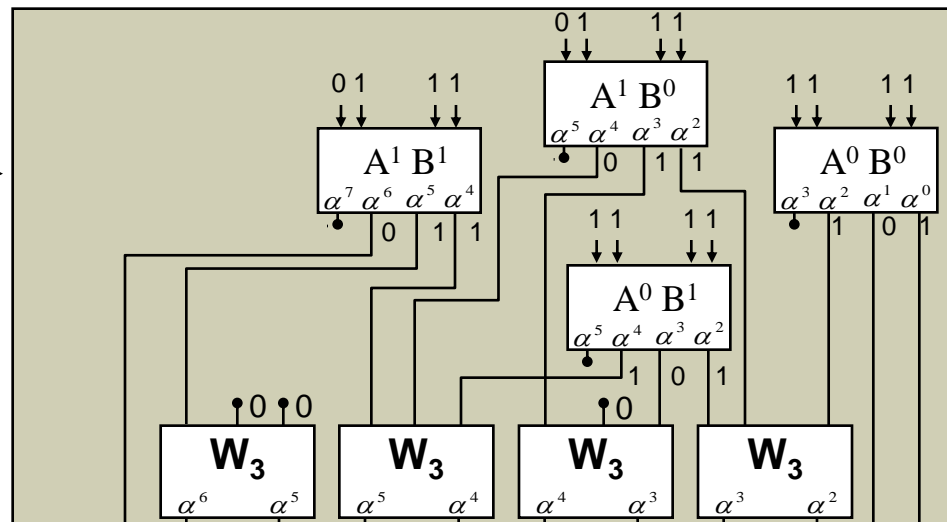
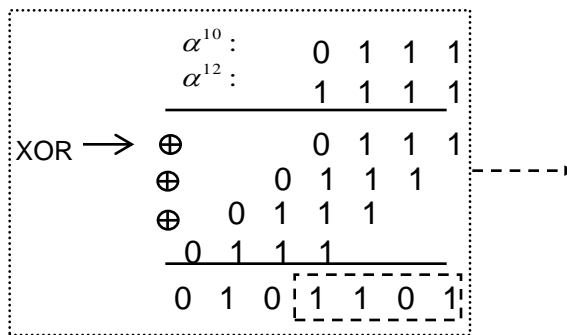
Scénario 2 – Etape 1: Réalisation des opérateurs arithmétiques tri-mode



[Garcia02] J. Garcia and M. J. Schulte, A Combined 16-bit Binary and Dual Galois Field Multiplier, In IEEE International Symposium on Circuits and Systems ISCAS'02, pp.63-68, 2002.

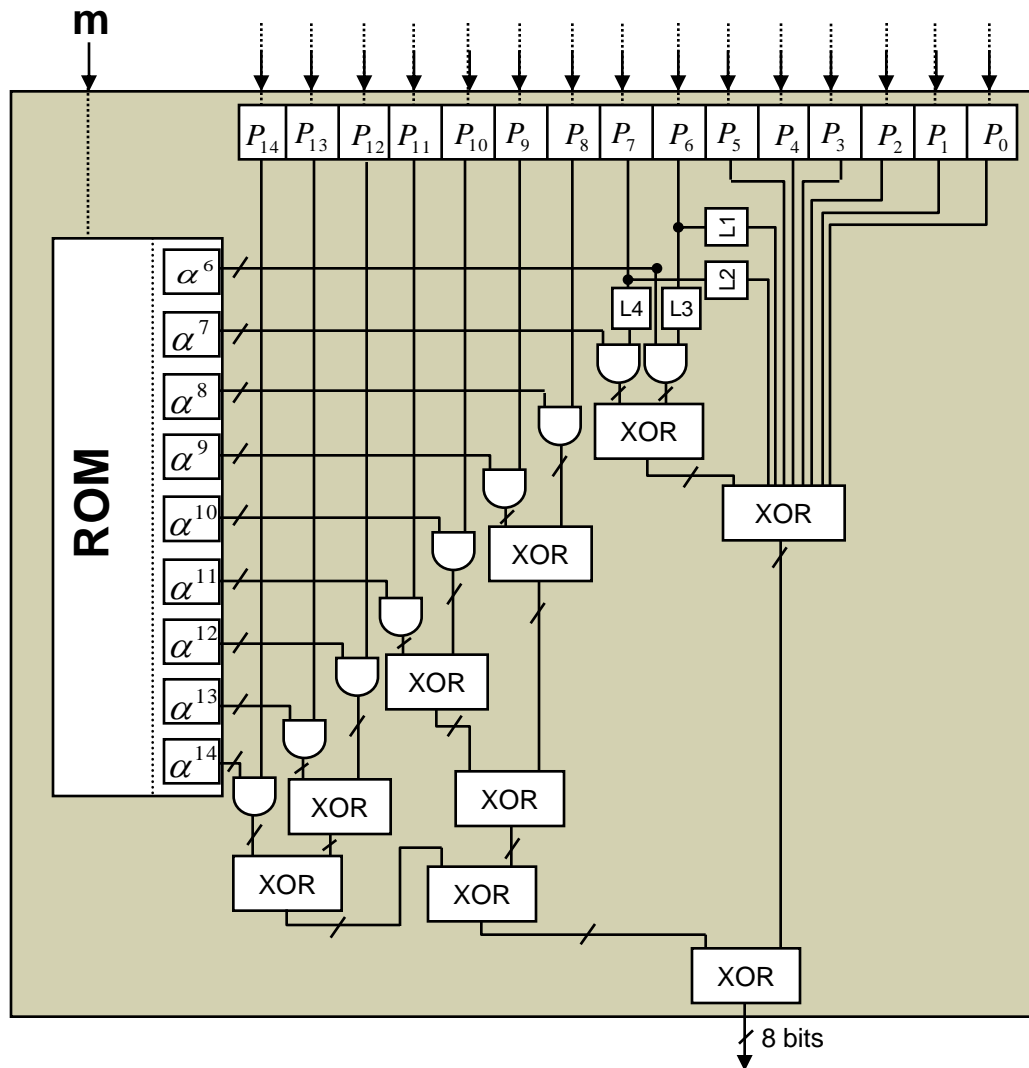


Entité de réduction polynômiale : Reconfiguration de l'arbre de Wallace





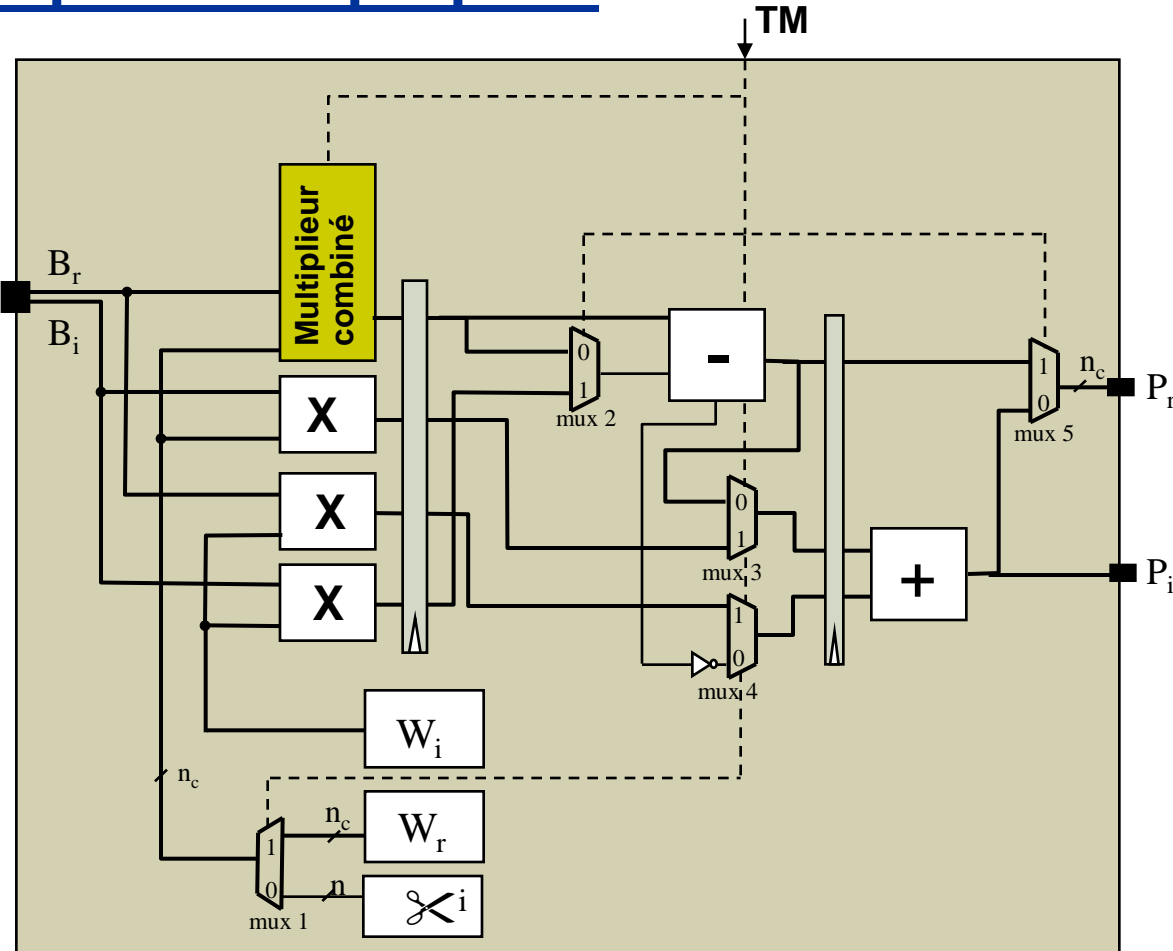
Entité de réduction polynômiale reconfigurable proposée : $m = 6, 7, 8$



Configuration des LUTs :

taille de multiplieur	L1	L2	L3	L4
$m = 6$	0	0	P_6	P_7
$m = 7$	P_6	0	0	P_7
$m = 8$	P_6	P_7	0	0

Multiplieur triple mode proposé



Première étape du scénario 2 réalisée



5

Conclusion et Perspectives



- Etude d'optimisation des ressources de calcul selon la technique de paramétrisation sous l'approche Opérateur Commun
- Etude du traitement fréquentiel des codes cycliques et en particulier les codes RS
- Redécouverte des codes RS spécifiques définis dans un corps de Galois de caractéristique nombre de Fermat
- Proposition des opérateurs arithmétiques reconfigurables opérant dans C et dans $CG(F_\lambda)$
- Réalisation et implémentation sur FPGA d'un opérateur FFT dual mode (DMFFT)
- Gain en mémoire de 21 - 33% et gain en surface de 4 – 25 %
- Proposition d'un approche d'évolution vers un opérateur TMFFT opérant dans C , $CG(F_\lambda)$ et $CG(2^m)$



Perspectives:

- Réalisation de l'étape 2 du deuxième scénario de mutualisation du DMFFT et FFT-GF2
- Etude de l'apport de la reconfiguration partielle
- Etude de l'ordonnancement des tâches et gestion du partage des ressources
- Etude algorithmique des codes RS classiques définis dans $CG(2^m)$
- Extension de l'utilisation de l'opérateur FFT reconfigurable vers les codes LDPC non-binaires et les codes convolutifs



Publications

Ali AL GHOUWAYEL, Yves LOUËT, Amor NAFKHA and Jacques PALICOT, "**On the FPGA Implementation of the Fourier Transform over Finite Fields $GF(2^m)$** ", IEEE ISCT'07, Sydney, Australia, October 2007

Ali AL GHOUWAYEL, Yves LOUËT and Jacques PALICOT, "**Complexity Evaluation of a Re-Configurable Butterfly with FPGA for Software Radio Systems**", IEEE PIMRC'07, Athens, Greece, September 2007

Ali AL GHOUWAYEL, Yves LOUËT and Jacques PALICOT, "**A reconfigurable architecture for the FFT operator in a Software Radio context**", IEEE ISCAS'06, Island of Kos, Greece, May 2006

Ali AL GHOUWAYEL, Yves LOUËT and Jacques PALICOT, "**A Reconfigurable Butterfly Architecture for Fourier and Fermat Transforms**", IEEE WSR'06, Karlsruhe, Germany, March 2006

Ali AL GHOUWAYEL, Yves LOUËT and Jacques PALICOT, "**Un opérateur reconfigurable dans un contexte Radio Logicielle: de la transformée de Fourier à la transformée de Fermat**", Majestic'06, Lorient, France, Novembre 2006

Merci pour votre attention

Questions ?