Cryptographie à base de couplages et multiplieurs parallèles en caractéristiques 2 et 3

Nicolas Estibals

11 septembre 2008

Contexte

Arithmétique sur $\mathbb{F}_{p^m}$

Algorithmes de multiplication sur $\mathbb{F}_p[X]$

Architecture du coprocesseur

Résultats

Conclusion

Introduction

- Stage effectué :
  - au LCIS (Laboratory of Cryptography and Information Security)
  - à l'université de Tsukuba, Japon
  - sous l'encadrement de Jean-Luc Beuchat
- Thématique :
  - Cryptographie sur courbes elliptiques (couplage)
  - Arithmétique des corps finis
  - Matériel
- Étude des algorithmes de multiplication sur $\mathbb{F}_{p^m}$
- Implémentation matérielle sur FPGA

Contexte

Arithmétique sur $\mathbb{F}_{p^m}$

Algorithmes de multiplication sur $\mathbb{F}_p[X]$

Architecture du coprocesseur

Résultats

Conclusion

Plan de l'exposé

Contexte

Arithmétique sur $\mathbb{F}_{p^m}$

Algorithmes de multiplication sur $\mathbb{F}_p[X]$

Architecture du coprocesseur

Résultats

Conclusion

Contexte

Arithmétique sur $\mathbb{F}_{p^m}$

Algorithmes de multiplication sur $\mathbb{F}_p[X]$

Architecture du coprocesseur

Résultats

Conclusion

Cryptosystèmes à clef publique

- RSA :
  - Rivest, Shamir et Adleman en 1977
  - Basé sur l'arithmétique des entiers modulo
  - Problème associé : factorisation de grands entiers

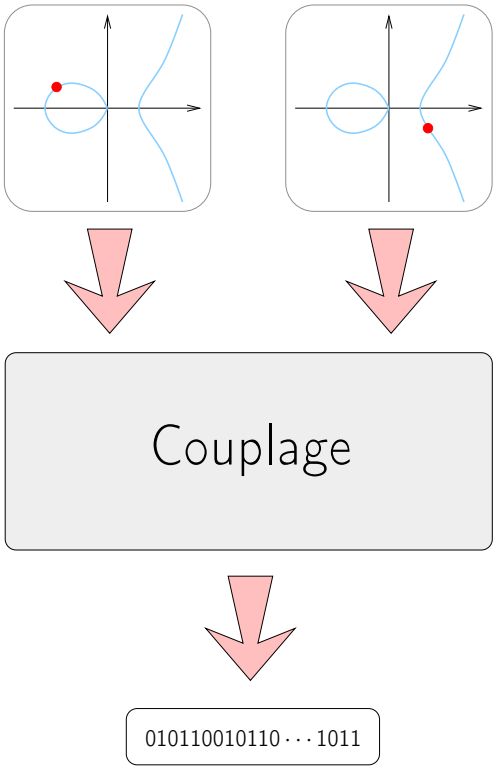
- ECC :
  - *Elliptic Curve Cryptography*
  - Neal Koblitz et Victor Miller en 1985
  - Basé sur le groupe des points d'une courbe elliptique
  - Problème associé : logarithme discret ▸ Définition

AES	RSA	ECC
80 bits	1024 bits	160 bits
112 bits	2048 bits	224 bits
128 bits	3072 bits	256 bits
256 bits	15360 bits	521 bits

Couplage

- 1993 : Menezes, Okamoto et Vanstone, attaque contre le logarithme discret sur les courbes elliptiques
- 2000 : Joux, système cryptographique utilisant les couplages
- Permet de nombreux protocoles cryptographiques originaux (signature basée sur l'identité, ...)

Couplage



- 1993 : Menezes, Okamoto et Vanstone, attaque contre le logarithme discret sur les courbes elliptiques
- 2000 : Joux, système cryptographique utilisant les couplages
- Permet de nombreux protocoles cryptographiques originaux (signature basée sur l'identité, . . .)

▸ Définition

Les couplages en matériel

Calcul d'un couplage :

- exigeant en ressources
- arithmétique spécifique
- processeurs généralistes non-adaptés
  $\Rightarrow$ implémentations logicielles peu performantes

Développer du matériel pour :

- FPGA
- systèmes embarqués (carte à puce, tag RFID, ...)

Motivations

Coprocesseur calculant un couplage :

- Générique :
  - Caractéristiques 2 et 3
  - Différents niveaux de sécurité
- Rapide

Multiplieur performant :

- Beaucoup de produits dans le calcul d'un couplage
- Parallèle
- Pipeliné

Contexte

Arithmétique sur $\mathbb{F}_{p^m}$

Algorithmes de multiplication sur $\mathbb{F}_p[X]$

Architecture du coprocesseur

Résultats

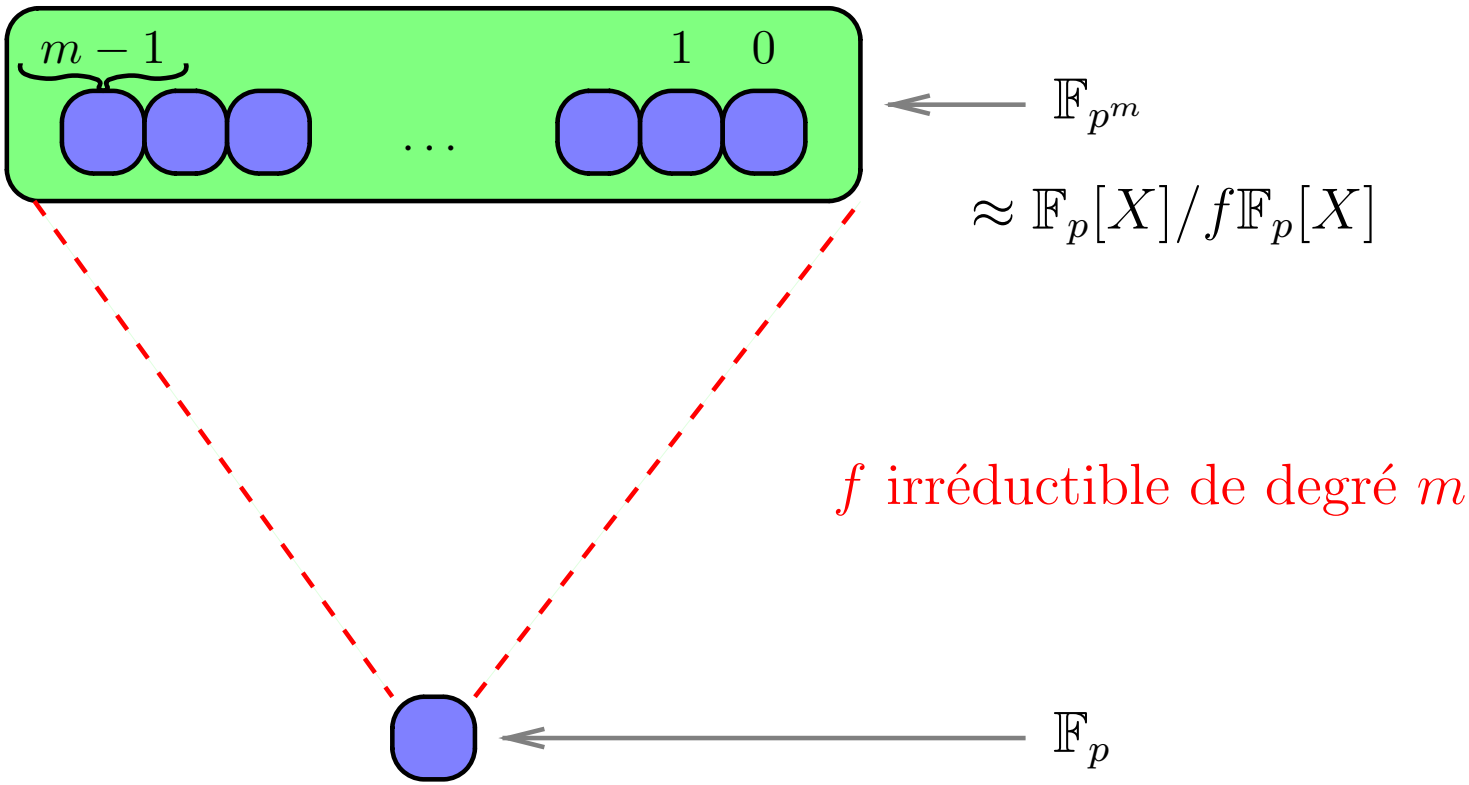
Conclusion

Construction des corps finis

$\mathbb{F}_p$

$\approx \mathbb{Z}/p\mathbb{Z}$

Construction des corps finis



Représentation de $\mathbb{F}_{p^m}$ et réduction modulaire

- Polynôme sur $\mathbb{F}_p$ de degré $< m$
- La somme de deux polynômes de degré au plus m est de degré au plus m

Addition sur $\mathbb{F}_{p^m}$: OK

$$\begin{array}{rl} & X^5 \quad +X^3+X^2 \quad +1 \\ + & X^5+X^4 \quad +X^2 \\ = & \quad X^4+X^3 \quad +1 \end{array}$$

Représentation de $\mathbb{F}_{p^m}$ et réduction modulaire

- Polynôme sur $\mathbb{F}_p$ de degré $< m$
- La somme de deux polynômes de degré au plus m est de degré au plus m

Addition sur $\mathbb{F}_{p^m}$: OK

$$\begin{array}{rl} & X^5 \quad +X^3+X^2 \quad +1 \\ + & X^5+X^4 \quad +X^2 \\ = & \quad X^4+X^3 \quad +1 \end{array}$$

- Le produit de deux polynômes de degré au plus m est de degré au plus $2m-1$

Multiplication sur $\mathbb{F}_{p^m}$: il faut réduire modulo f

$$\begin{array}{rl} & \quad X^4+X^3+X^2 \quad +1 \\ \times & X^5 \quad +X \quad +1 \\ = & X^9+X^8+X^7 \quad +X^2+X \quad +1 \end{array}$$

▸ Exemple de réduction

Contexte

Arithmétique sur $\mathbb{F}_{p^m}$

Algorithmes de multiplication sur $\mathbb{F}_p[X]$

Architecture du coprocesseur

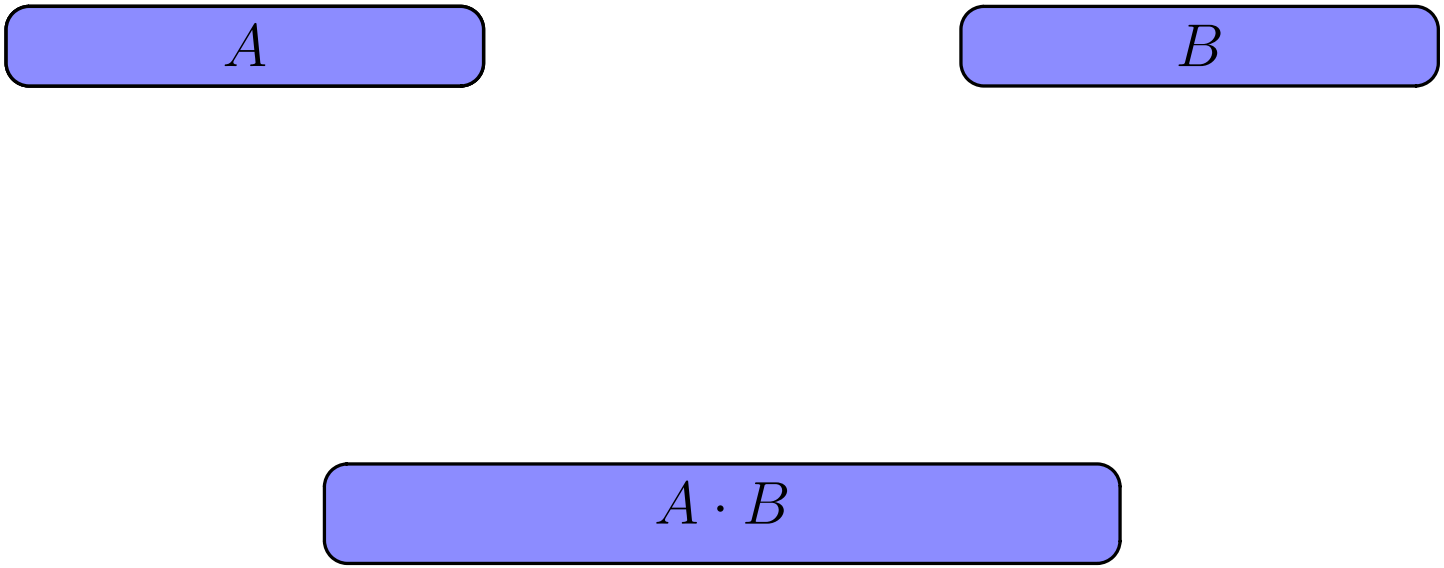
Résultats

Conclusion

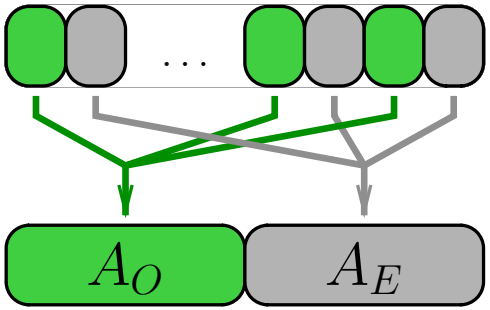
Algorithme naïf

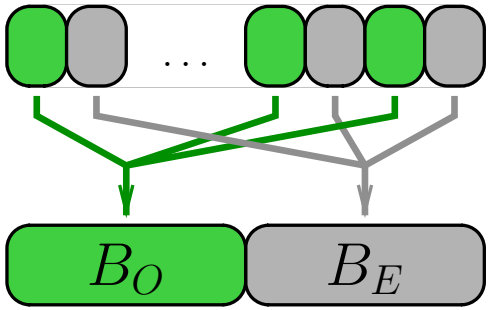
- L'algorithme appris en primaire (*paper-and-pencil*, *schoolbook*)
- Calculer le produit de tous les coefficients puis les sommer correctement.
- Complexité en $O(m^2)$

Algorithme de Karatsuba-Offman sans recouvrement



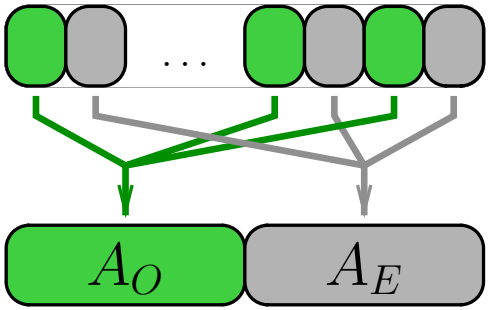
Algorithme de Karatsuba-Offman sans recouvrement

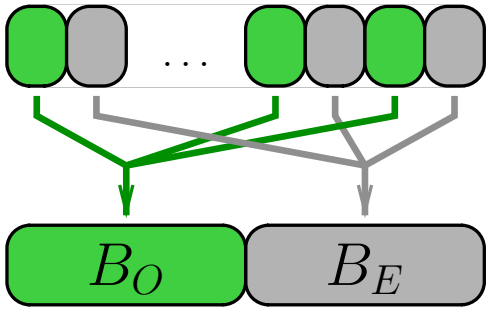




$$(A_0 B_O X^2 + A_E B_E) + X(A_O B_E + A_E B_O)$$

Algorithme de Karatsuba-Offman sans recouvrement



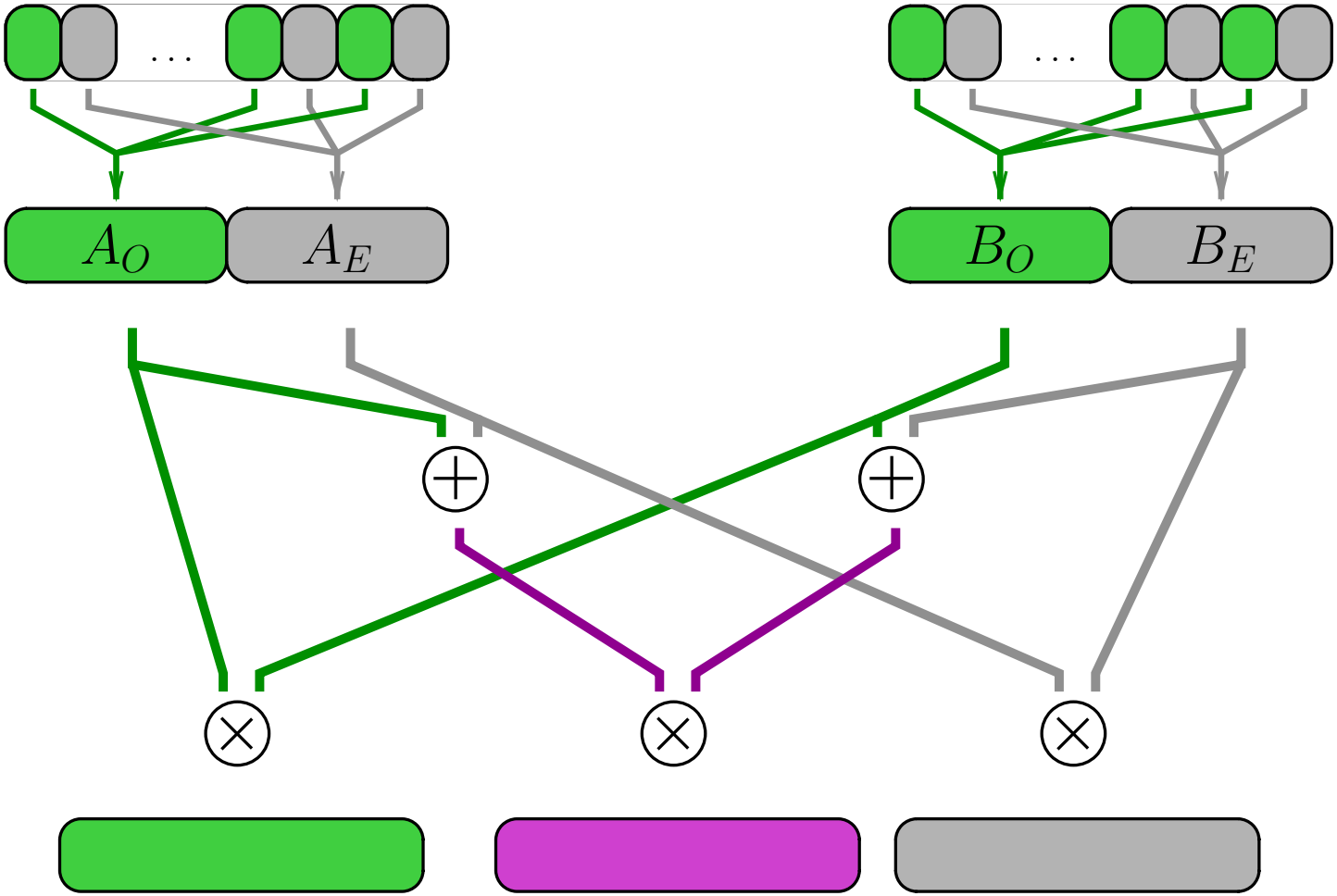


$$(A_0B_OX^2 + A_EB_E) + X(A_OB_E + A_EB_O)$$

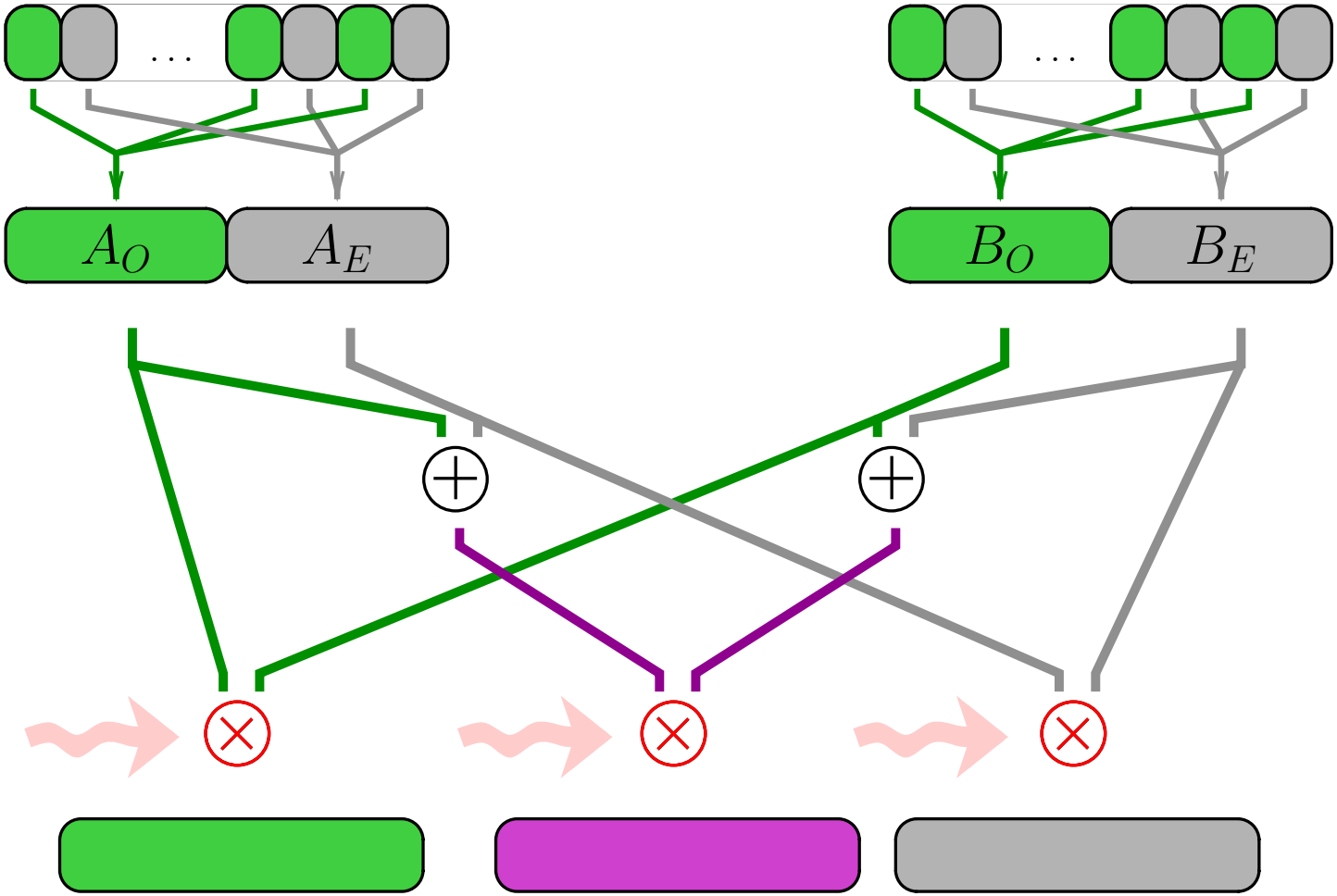
$$ab' + a'b = (a + a')(b + b') - ab - a'b'$$

$$(A_0B_OX^2 + A_EB_E) + X((A_O + A_E)(B_O + B_E) - A_OB_O - A_EB_E)$$

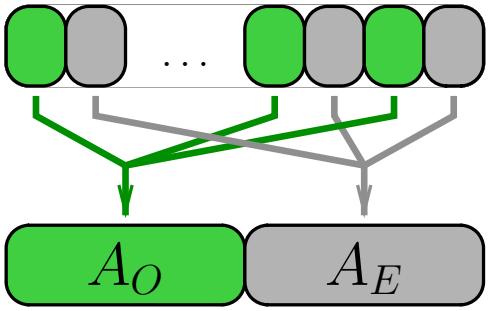
Algorithme de Karatsuba-Offman sans recouvrement

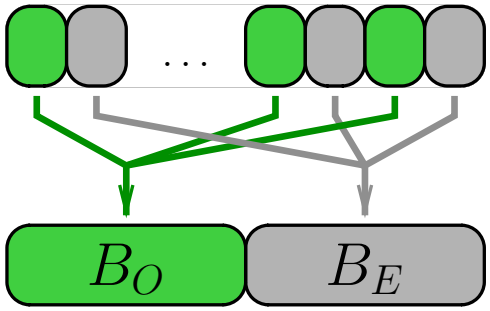


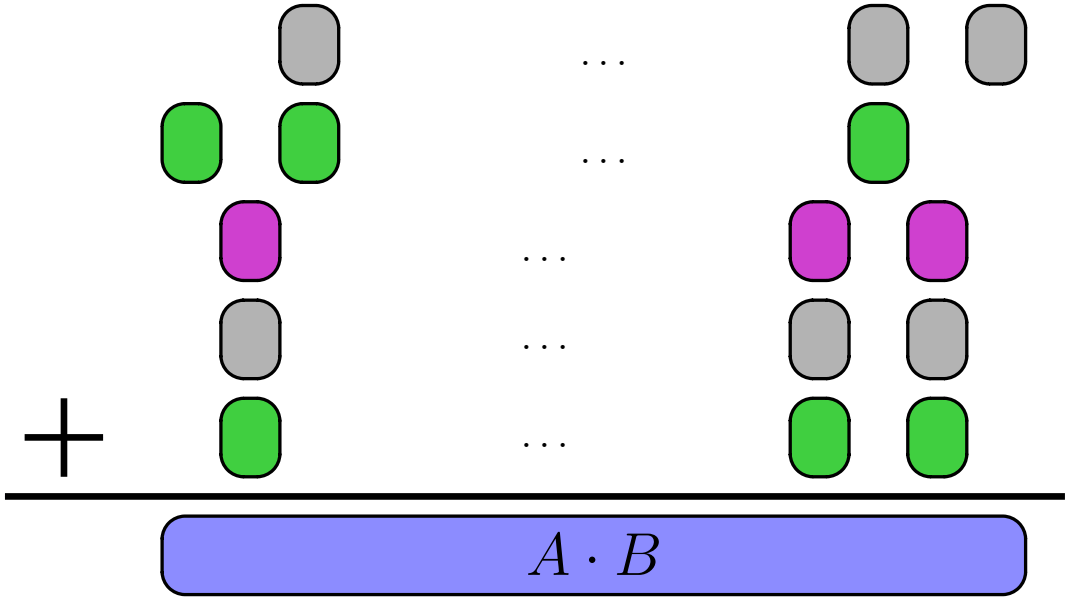
Algorithme de Karatsuba-Offman sans recouvrement



Algorithme de Karatsuba-Offman sans recouvrement







Complexité en $O(m^{1.58})$

D'autres variations

- Découpe des opérandes en 3, 5, ... parties
- Utiliser différents algorithmes selon le degré
  $\Rightarrow$ selon l'étage de récursion
- L'algorithme naïf est le meilleur pour les petits degrés
- Karatsuba est meilleur dès que m grandit

Contexte

Arithmétique sur $\mathbb{F}_{p^m}$

Algorithmes de multiplication sur $\mathbb{F}_p[X]$

Architecture du coprocesseur

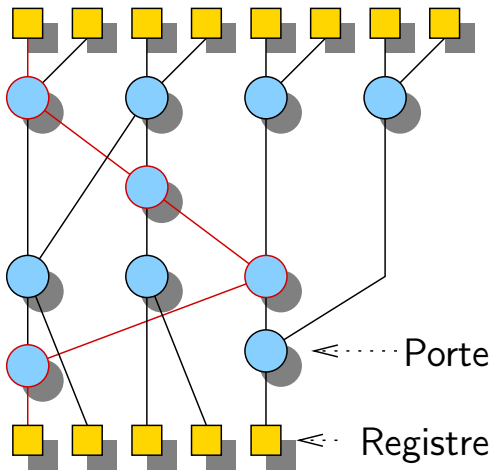
Résultats

Conclusion

Chemin critique et pipeline

Chemin critique :

- le chemin le plus long entre deux registres,
- définit la fréquence de fonctionnement.



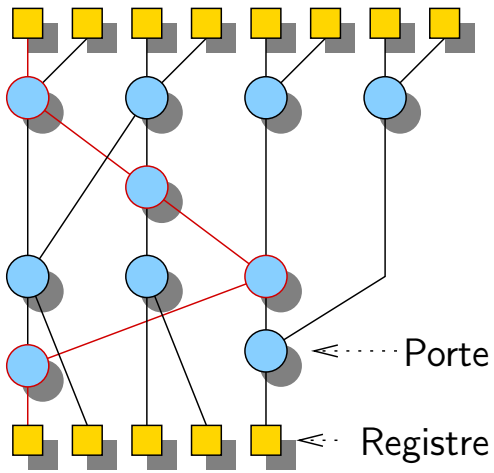
Chemin critique et pipeline

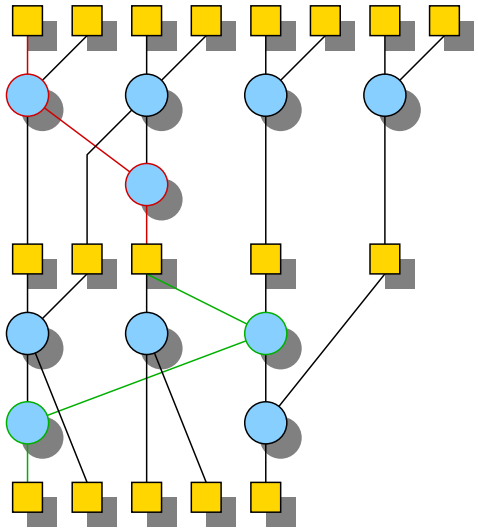
Chemin critique :

- le chemin le plus long entre deux registres,
- définit la fréquence de fonctionnement.

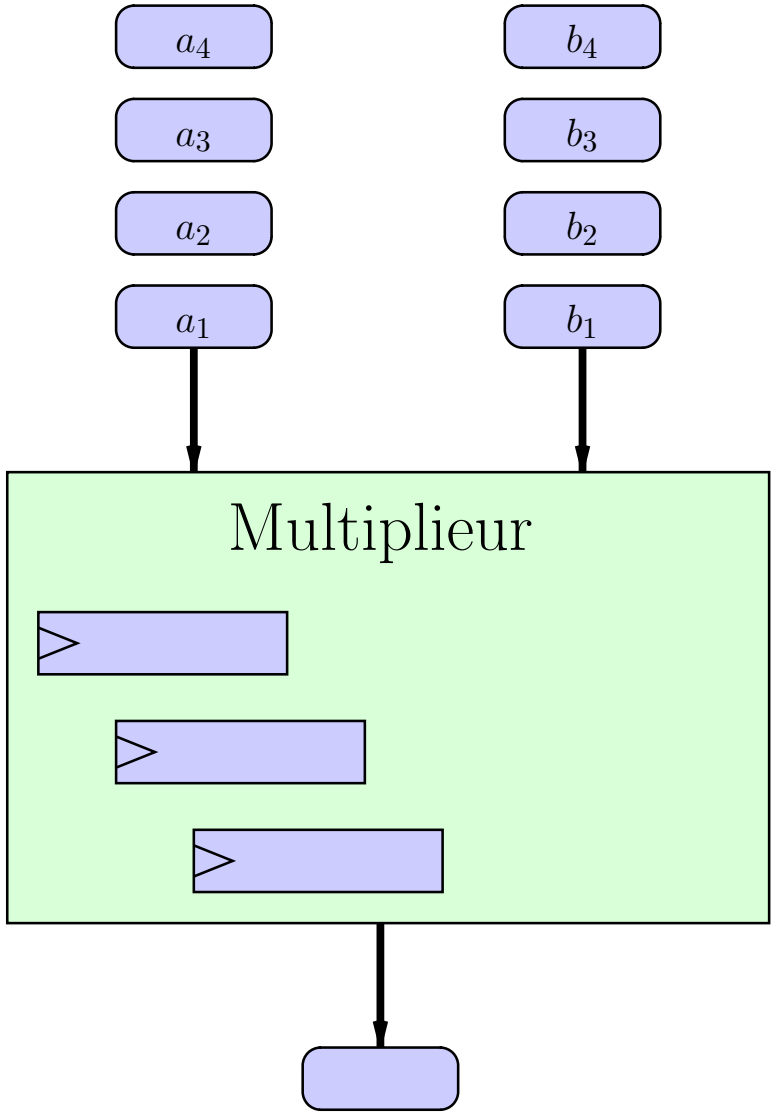
Pipeline :

- principe : couper le chemin critique en plusieurs morceaux pour le rendre plus court,
- fonctionnement : les données mettent plusieurs cycles à sortir du circuit.

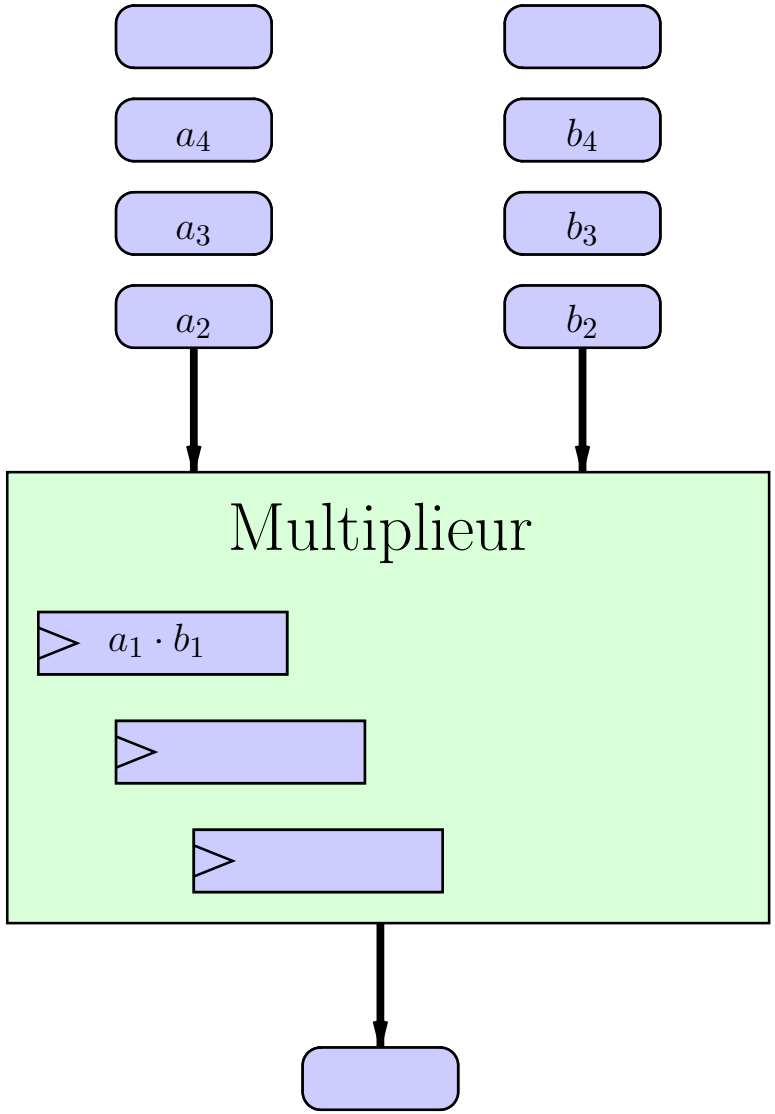




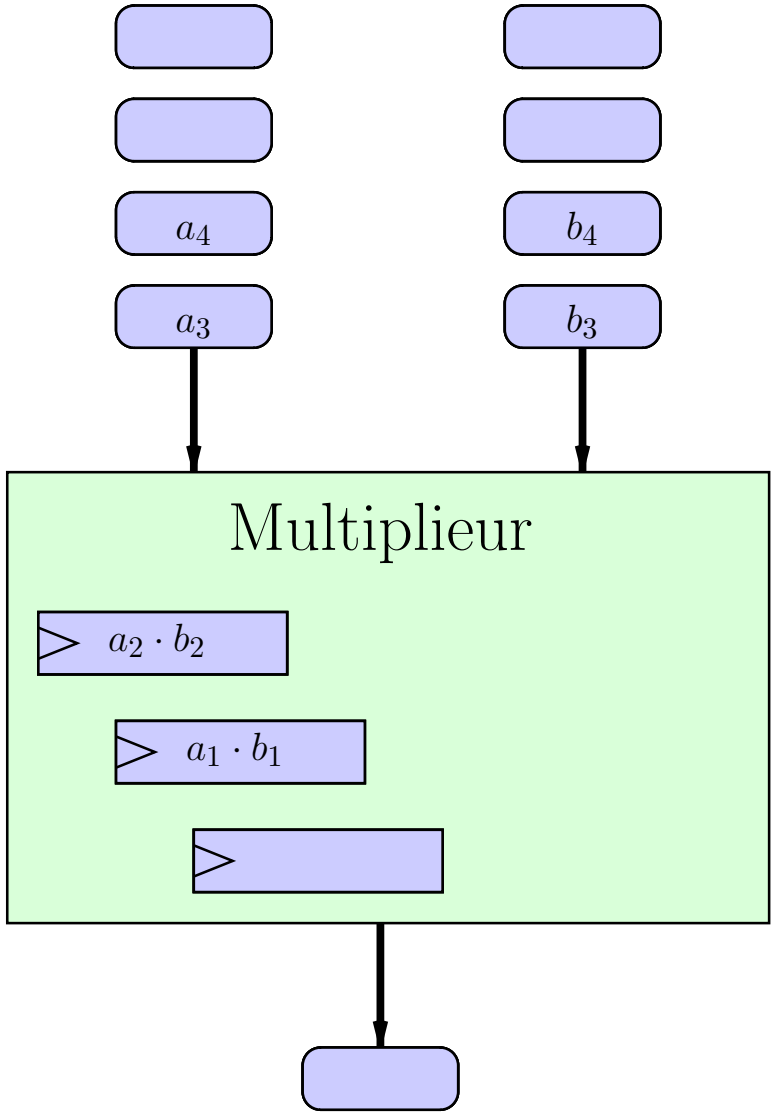
Exemple de fonctionnement d'un opérateur pipeliné



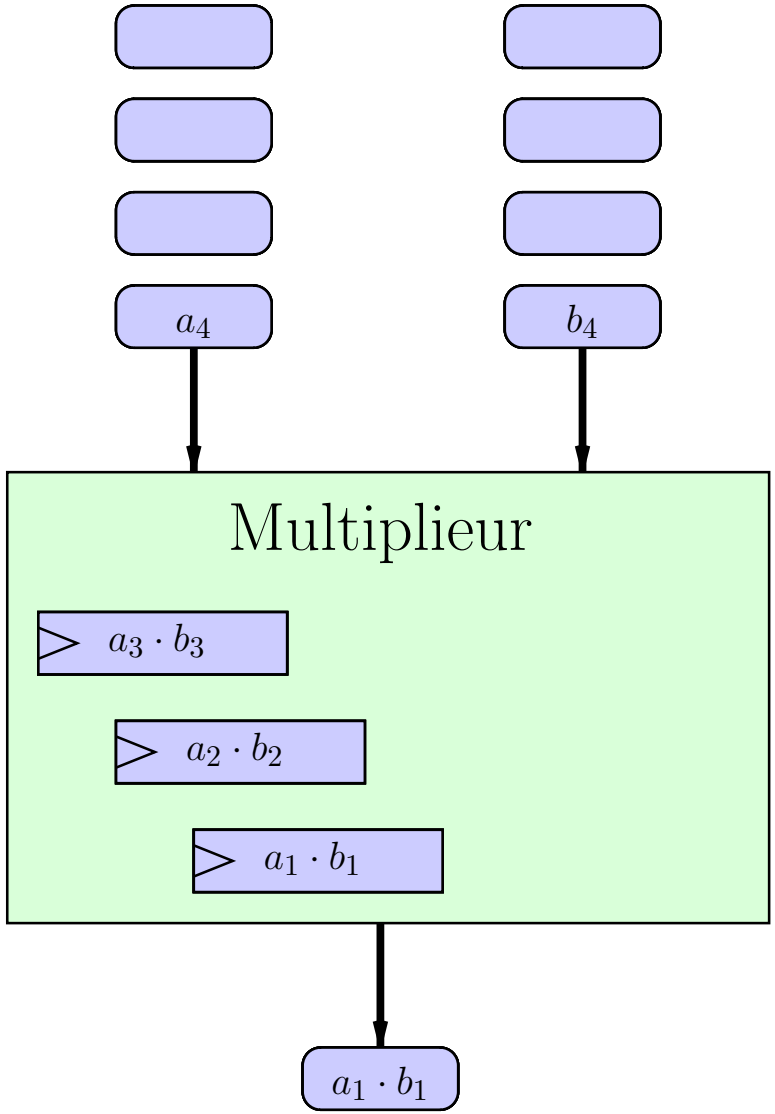
Exemple de fonctionnement d'un opérateur pipeliné



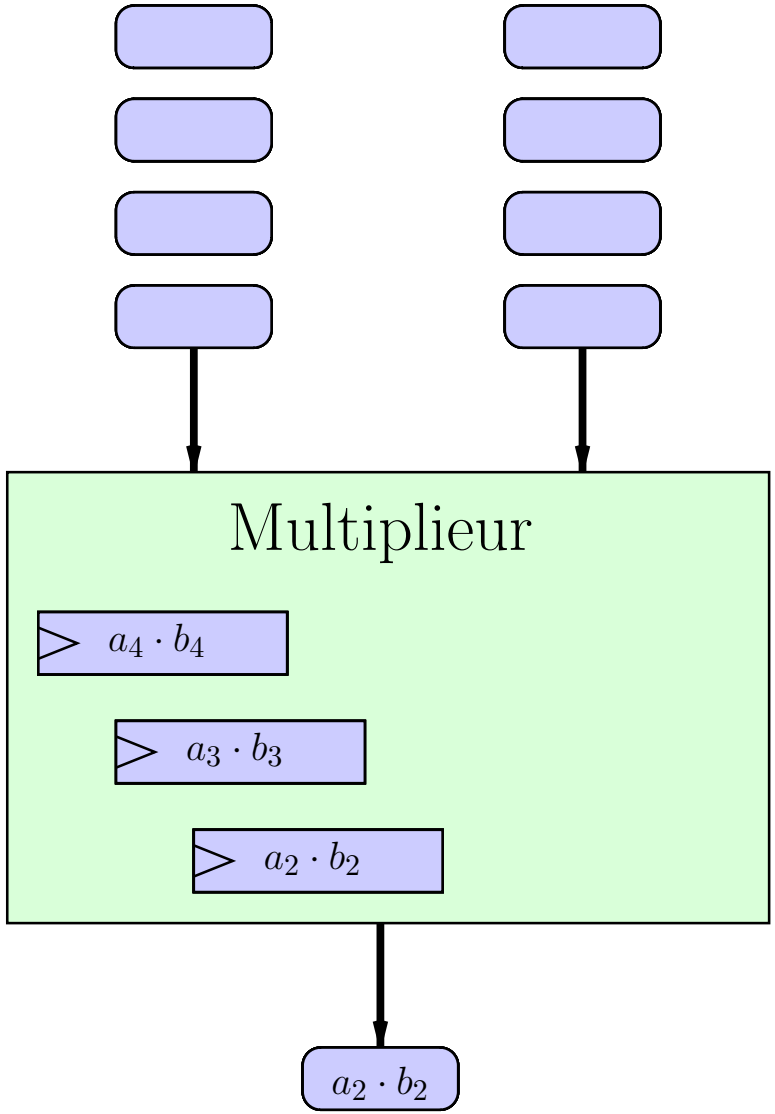
Exemple de fonctionnement d'un opérateur pipeliné



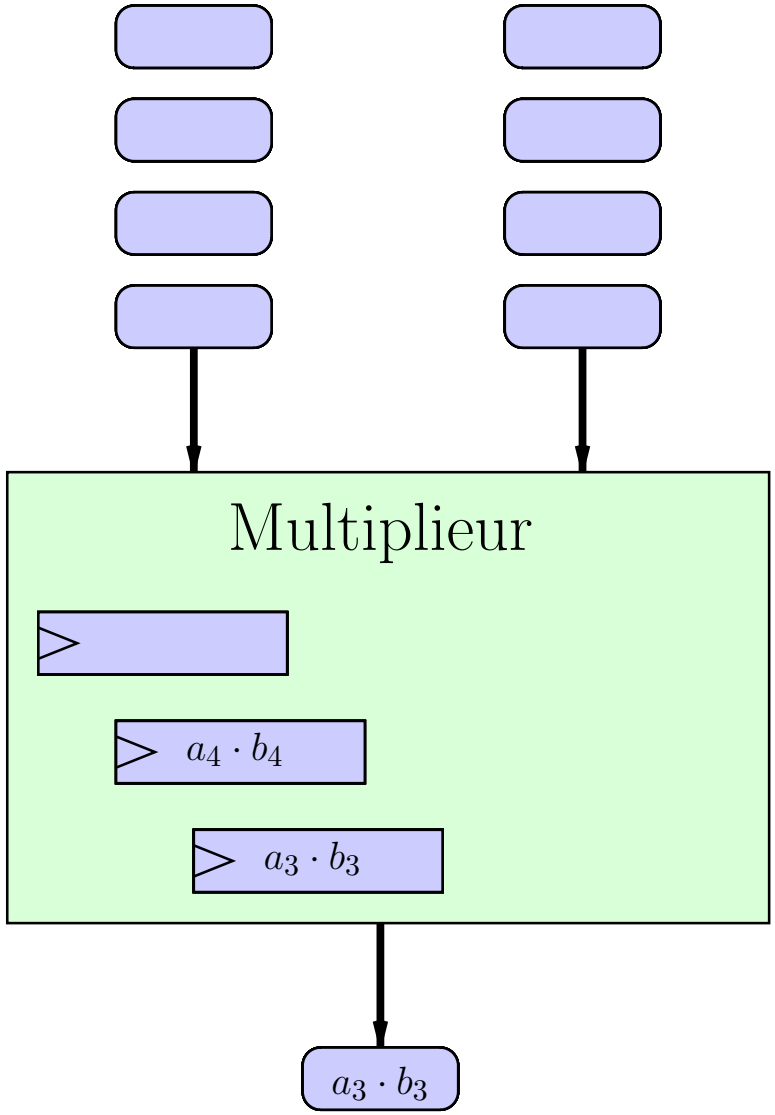
Exemple de fonctionnement d'un opérateur pipeliné



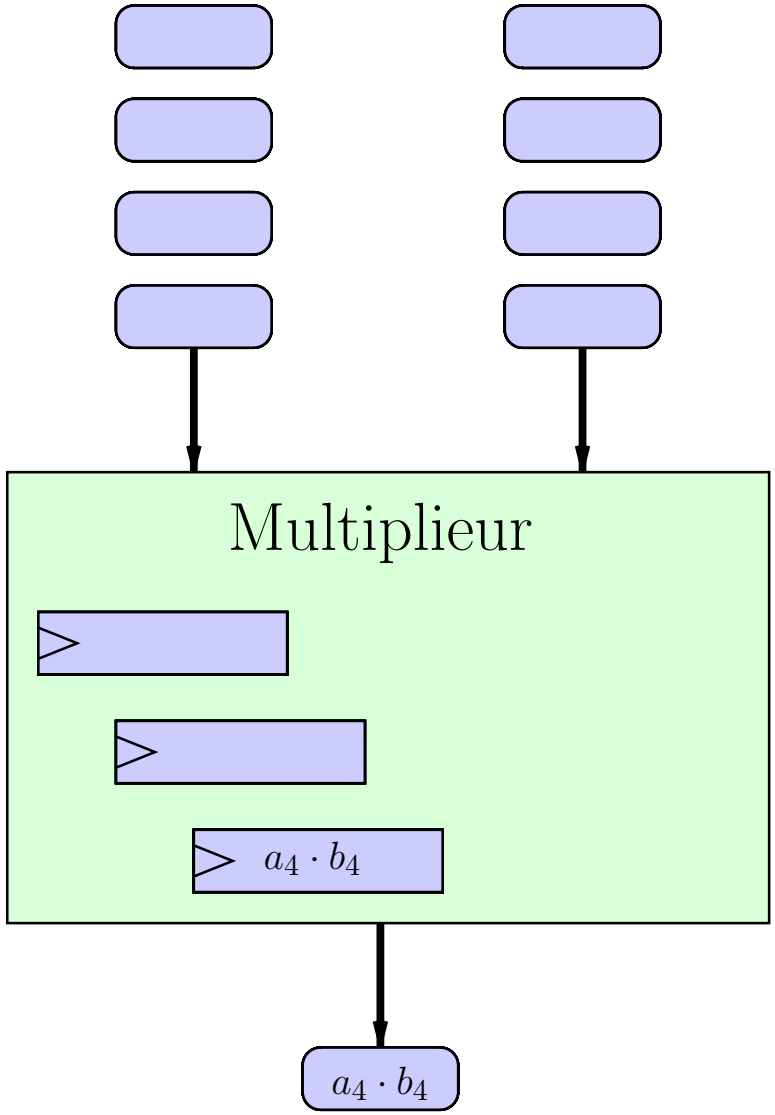
Exemple de fonctionnement d'un opérateur pipeliné



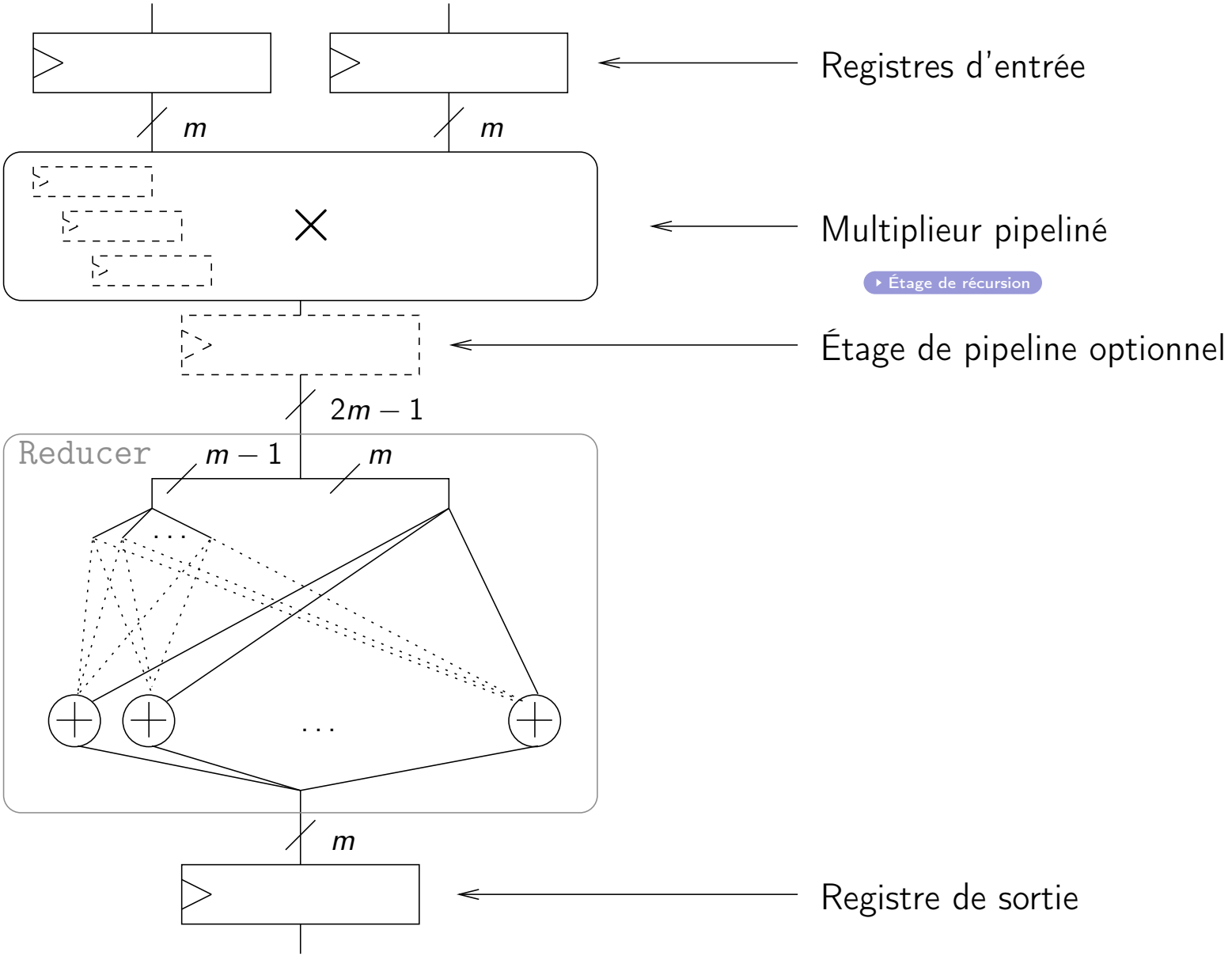
Exemple de fonctionnement d'un opérateur pipeliné



Exemple de fonctionnement d'un opérateur pipeliné



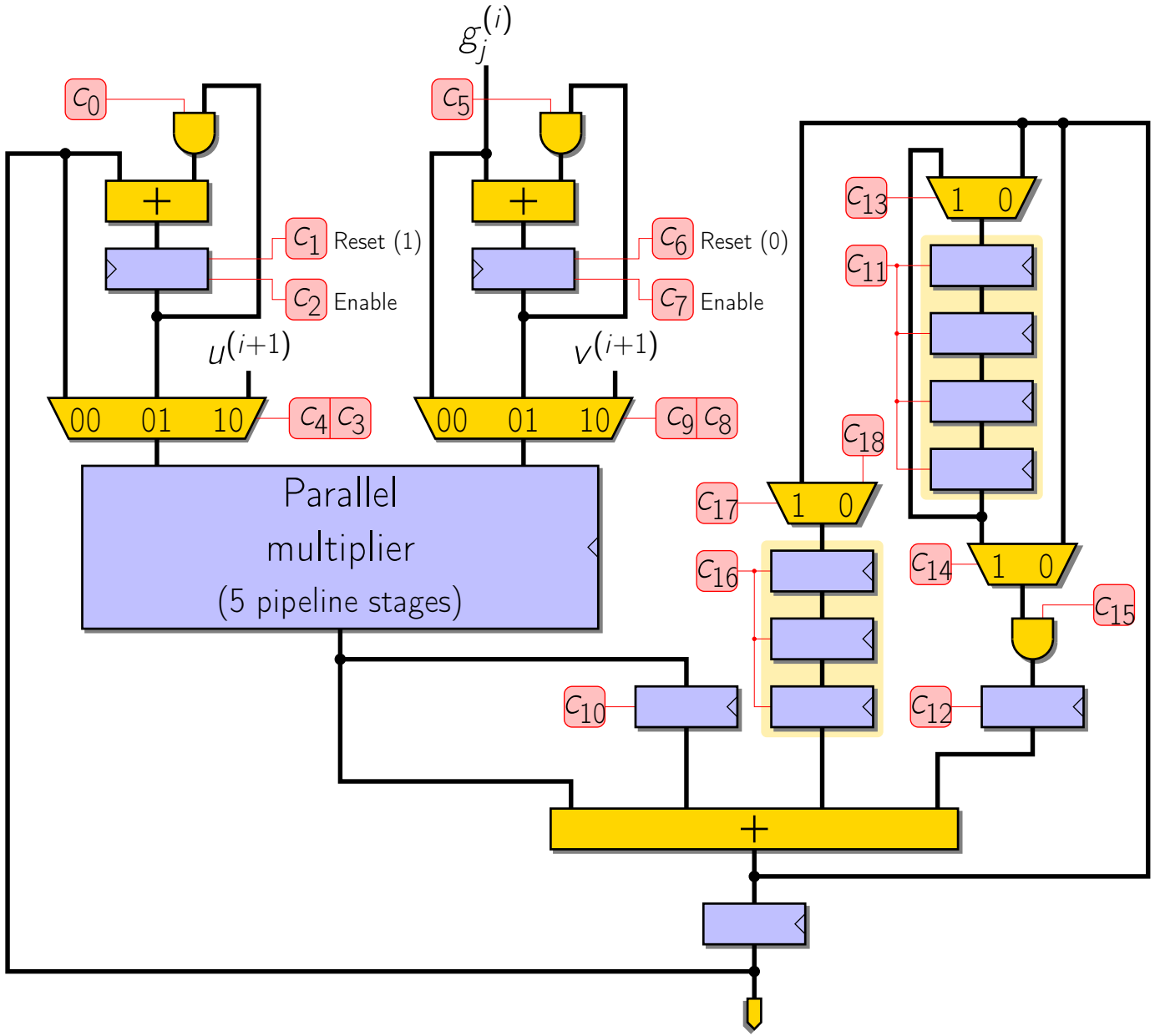
Multiplieur complet



Calcul du couplage

- Calcul itératif ▸ Algorithme
- 7 multiplications à chaque itération en caractéristique 2
- Nous *remplissons le pipeline* :
  - nous démarrons une multiplication à chaque cycle
  - nous utilisons un produit à chaque cycle
  - ce qui n'est pas trivial . . .

Calcul du couplage



▸ En fonctionnement

Contexte

Arithmétique sur $\mathbb{F}_{p^m}$

Algorithmes de multiplication sur $\mathbb{F}_p[X]$

Architecture du coprocesseur

Résultats

Conclusion

Comparaison avec la littérature

Comparaison avec des multiplieurs de la littérature

Algorithme	$\mathbb{F}_{p^m}$	FPGA	Temps (ns)	Fréquence (MHz)	Surface (slices)	Produit temps-surface (μs·slices)
G. Bertoni *et al.* (2003)	$\mathbb{F}_{3^{97}}$	`Virtex II pro`	74.15	94	3561	264
J.-L. Beuchat *et al.* (2007)	$\mathbb{F}_{3^{97}}$	`Cyclone II`	221.5	149	700	155
$\mathcal{K}'_{2,97}$, $\mathcal{K}'_{2,49}$, $\mathcal{K}'_{2,25}$, $\mathcal{K}'_{2,13}$, $\mathcal{K}'_{2,7}$, Naïf	$\mathbb{F}_{3^{97}}$	`Virtex II pro`	7.705	130	10316	79.5

Comparaison avec la littérature

Comparaison avec des multiplieurs de la littérature

Algorithme	$\mathbb{F}_{p^m}$	FPGA	Temps (ns)	Fréquence (MHz)	Surface (slices)	Produit temps-surface (μs·slices)
G. Bertoni *et al.* (2003)	$\mathbb{F}_{3^{97}}$	`Virtex II pro`	74.15	94	3561	264
J.-L. Beuchat *et al.* (2007)	$\mathbb{F}_{3^{97}}$	`Cyclone II`	221.5	149	700	155
$\mathcal{K}'_{2,97}$, $\mathcal{K}'_{2,49}$, $\mathcal{K}'_{2,25}$, $\mathcal{K}'_{2,13}$, $\mathcal{K}'_{2,7}$, Naïf	$\mathbb{F}_{3^{97}}$	`Virtex II pro`	7.705	130	10316	79.5

Comparaison avec des coprocesseurs de calcul de couplage de la littérature

Algorithme	$\mathbb{F}_{p^m}$	FPGA	Temps (μs)	Fréquence (MHz)	Surface (slices)	Produit temps-surface (s·slices)
J.-L. Beuchat *et al.* (2007)	$\mathbb{F}_{2^{239}}$	`Virtex II pro`	127	165	2736	347
C. Shu *et al.* (2006)	$\mathbb{F}_{2^{239}}$	`Virtex II pro`	41	84	25287	1040
Estimation pour notre architecture	$\mathbb{F}_{2^{239}}$	`Virtex II pro`	≈10	≈140	≈20000	≈200
J. Jiang (2007)	$\mathbb{F}_{3^{97}}$	`Virtex 4`	21	78	74105	1556

Contexte

Arithmétique sur $\mathbb{F}_{p^m}$

Algorithmes de multiplication sur $\mathbb{F}_p[X]$

Architecture du coprocesseur

Résultats

Conclusion

Conclusion

- Étude d'algorithmes de multiplication
- Conception d'architectures
- Générateur de multiplieurs en caractéristiques 2 et 3

Conclusion

- Étude d'algorithmes de multiplication
- Conception d'architectures
- Générateur de multiplieurs en caractéristiques 2 et 3

Beaucoup de concepts nouveaux pour moi :

- Arithmétique des corps finis
- *Elliptic Curve Cryptography*
- Conception d'architectures
- FPGA :
  - programmation en `VHDL`
  - outils de synthèse et de simulation
- Génération de code

Perspectives

- Finir le coprocesseur et le proposer à Arith 19
- D'autres algorithmes de multiplication :
  - Toom-Cook
  - Formules de Montgomery
  - ...
- Étude sur des extensions plus grandes
- Arithmétique en caractéristique p

Des Questions ?

Problème du logarithme discret

Définition (*Discrete Logarithm Problem*)

Le problème du logarithme discret sur un groupe G est de retrouver $a \in \mathbb{Z}$ étant donné seulement $P \in G$ et la somme aP.

- G le groupe des points sur une courbe elliptique
- Le DLP sur ce groupe est considéré comme *difficile*
  Meilleur attaque : Pollard's ρ

◂ ECC

Définition formelle d'un couplage

Définition (Couplage)

Un couplage est une application bilinéaire $\hat{e} : G_1 \times G_1 \longrightarrow G_2$ où G_1 et G_2 sont des groupes cycliques de même cardinal :

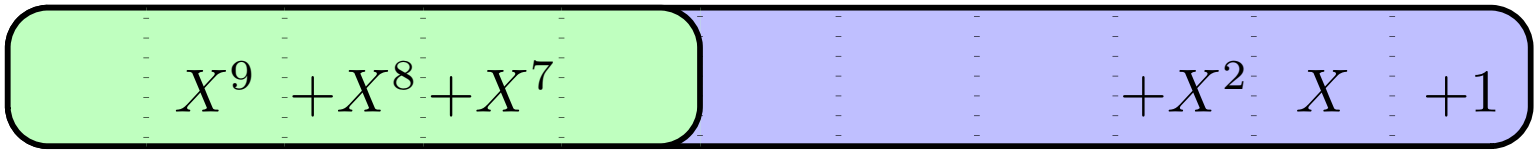
$$\forall P, Q \in G_1, \forall a, b \in \mathbb{Z}, \hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$$

G_1 est le groupe des points d'une courbe elliptique,
G_2 une extension de $\mathbb{F}_p$. ◂ Couplage

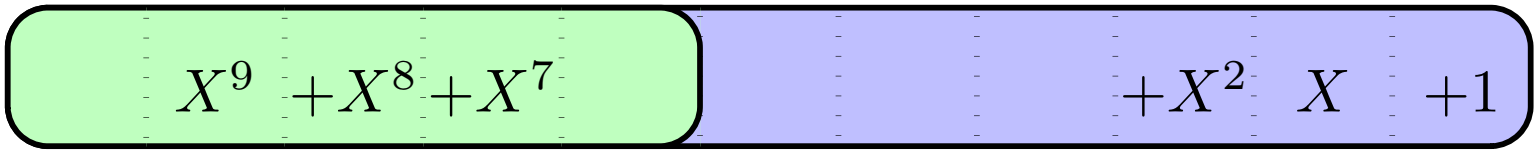
Un exemple de réduction

$$X^9 + X^8 \quad X^7 \qquad\qquad + X^2 \quad X \quad +1$$

Un exemple de réduction

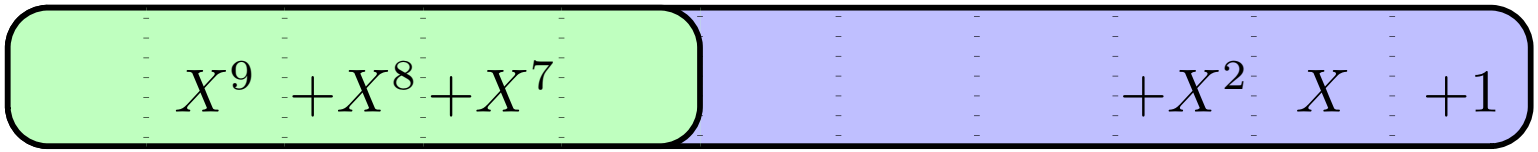


Un exemple de réduction



$$F = X^6 + X + 1$$

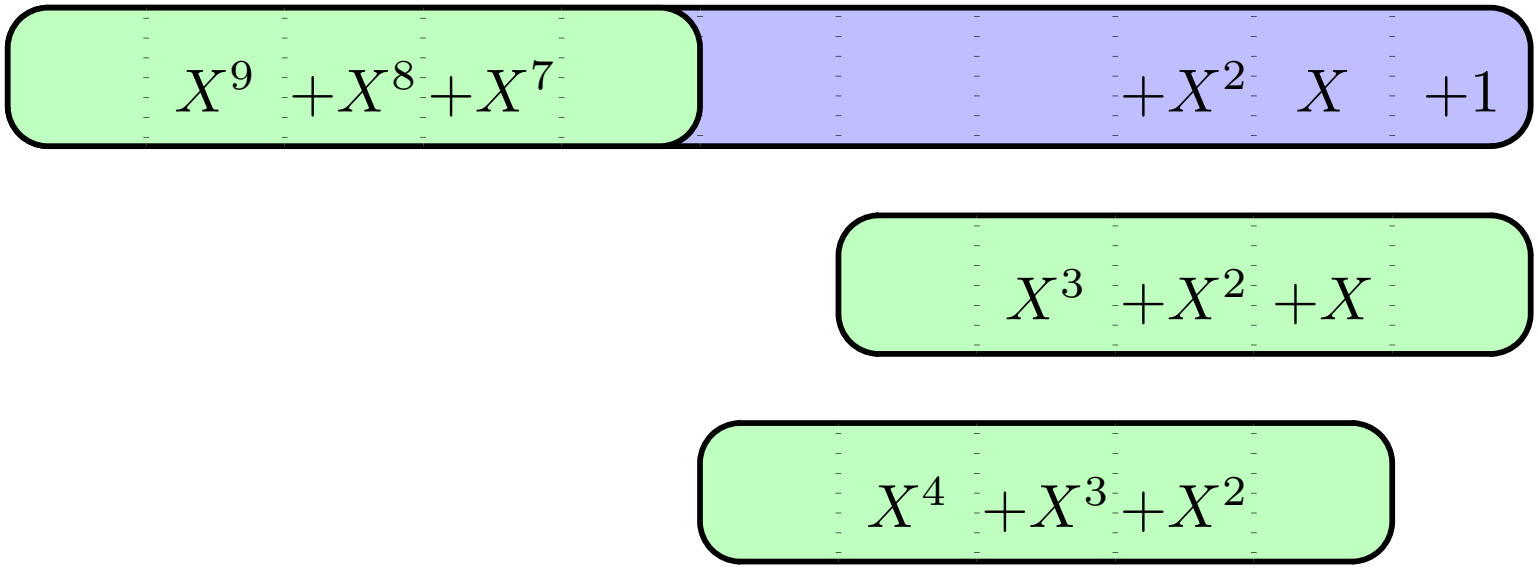
Un exemple de réduction



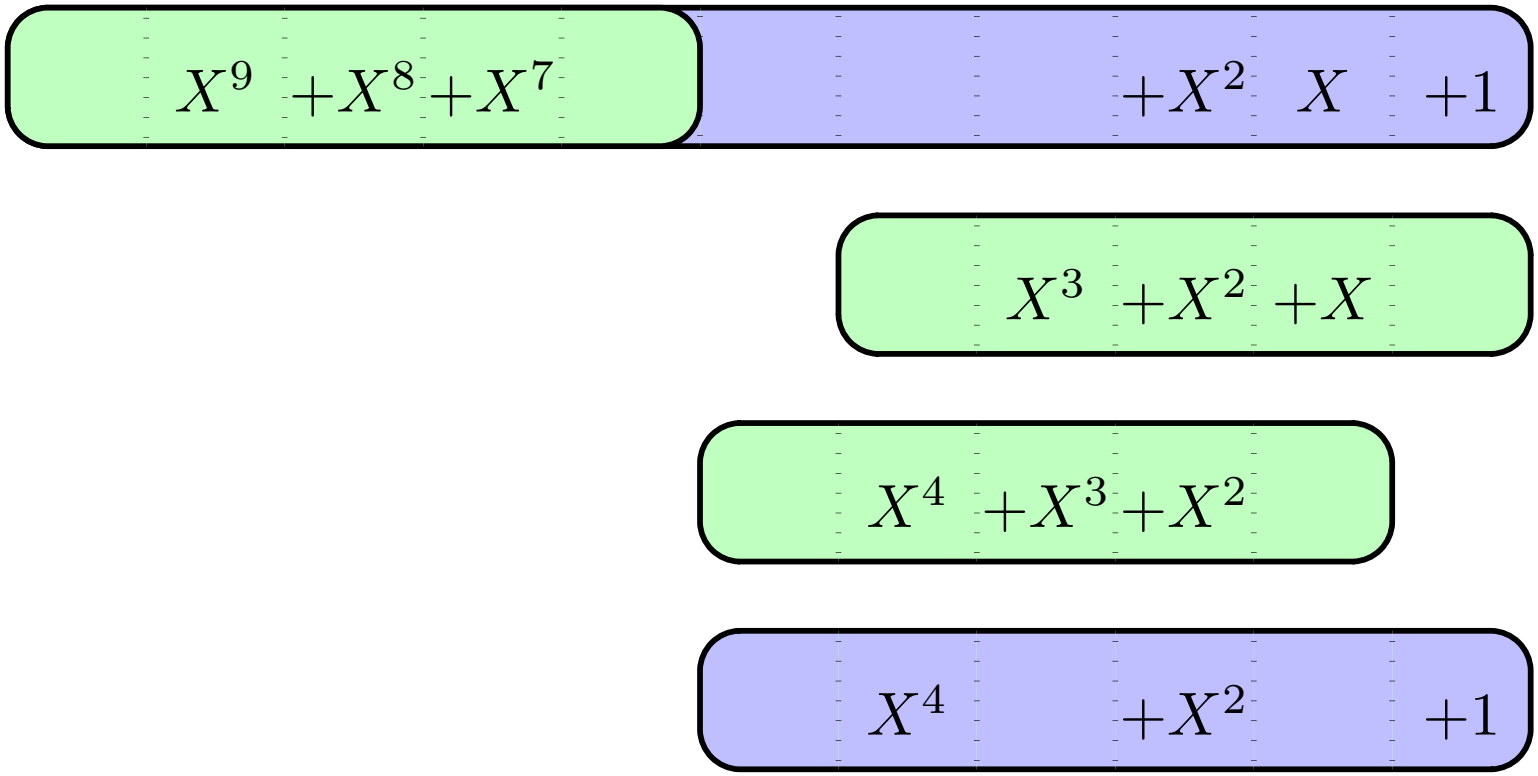
$$F = X^6 + X + 1$$

$$X^6 \bmod F = X + 1$$
$$X^7 \bmod F = X^2 + X$$
$$X^8 \bmod F = X^3 + X^2$$
$$X^9 \bmod F = X^4 + X^3$$

Un exemple de réduction

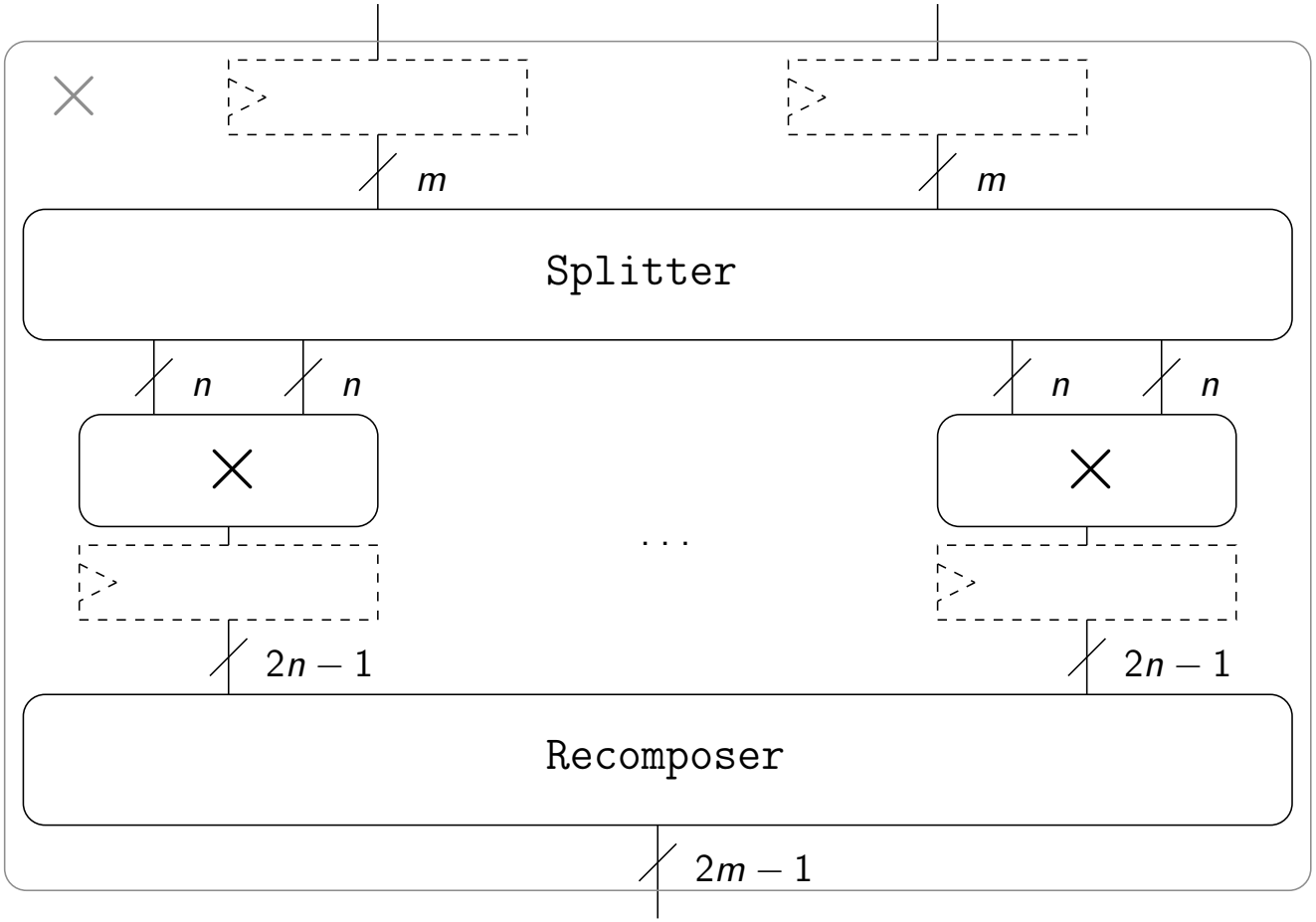


Un exemple de réduction



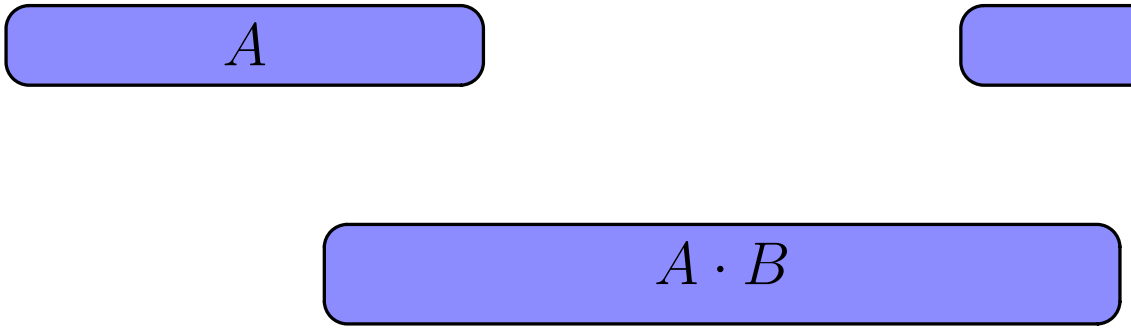
◂ Représentation de $\mathbb{F}_{p^m}$

Architecture d'un étage de récursion



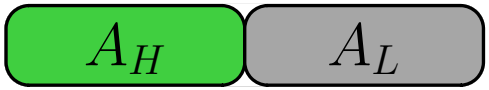
◂ Multiplieur complet

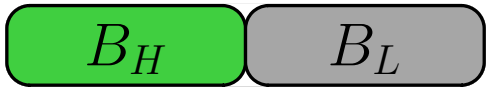
Algorithme de Karatsuba-Offman



Algorithme de Karatsuba-Offman

Approche *divide-and-conquer*





$$A_H B_H X^{2n} + (A_H B_L + A_L B_H) X^n + A_L B_L$$

Algorithme de Karatsuba-Offman

Approche *divide-and-conquer*

A_H A_L B_H B_L

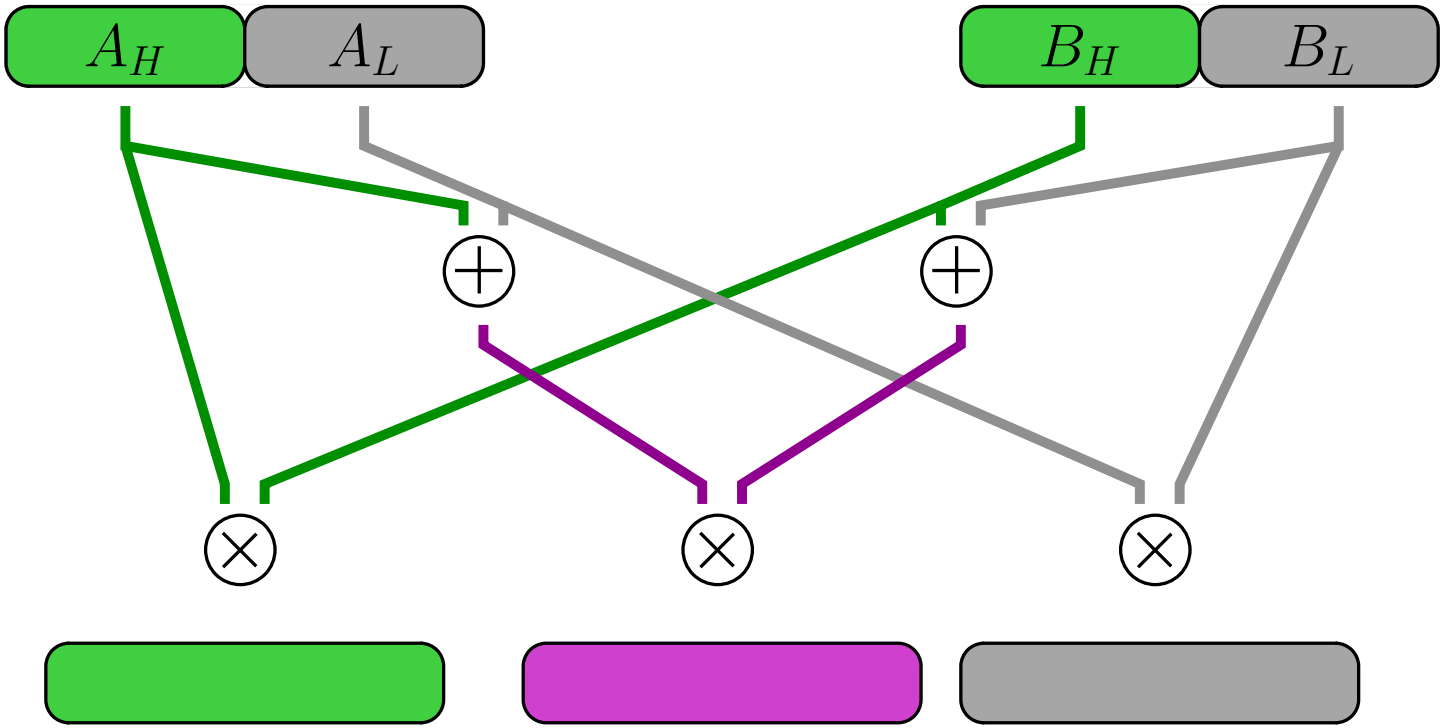
$$A_H B_H X^{2n} + (A_H B_L + A_L B_H) X^n + A_L B_L$$

$$ab' + a'b = (a + a')(b + b') - ab - a'b'$$

$$A_H B_H X^{2n} + ((A_H + A_L)(B_H + B_L) - A_H B_H - A_L B_L) X^n + A_L B_L$$

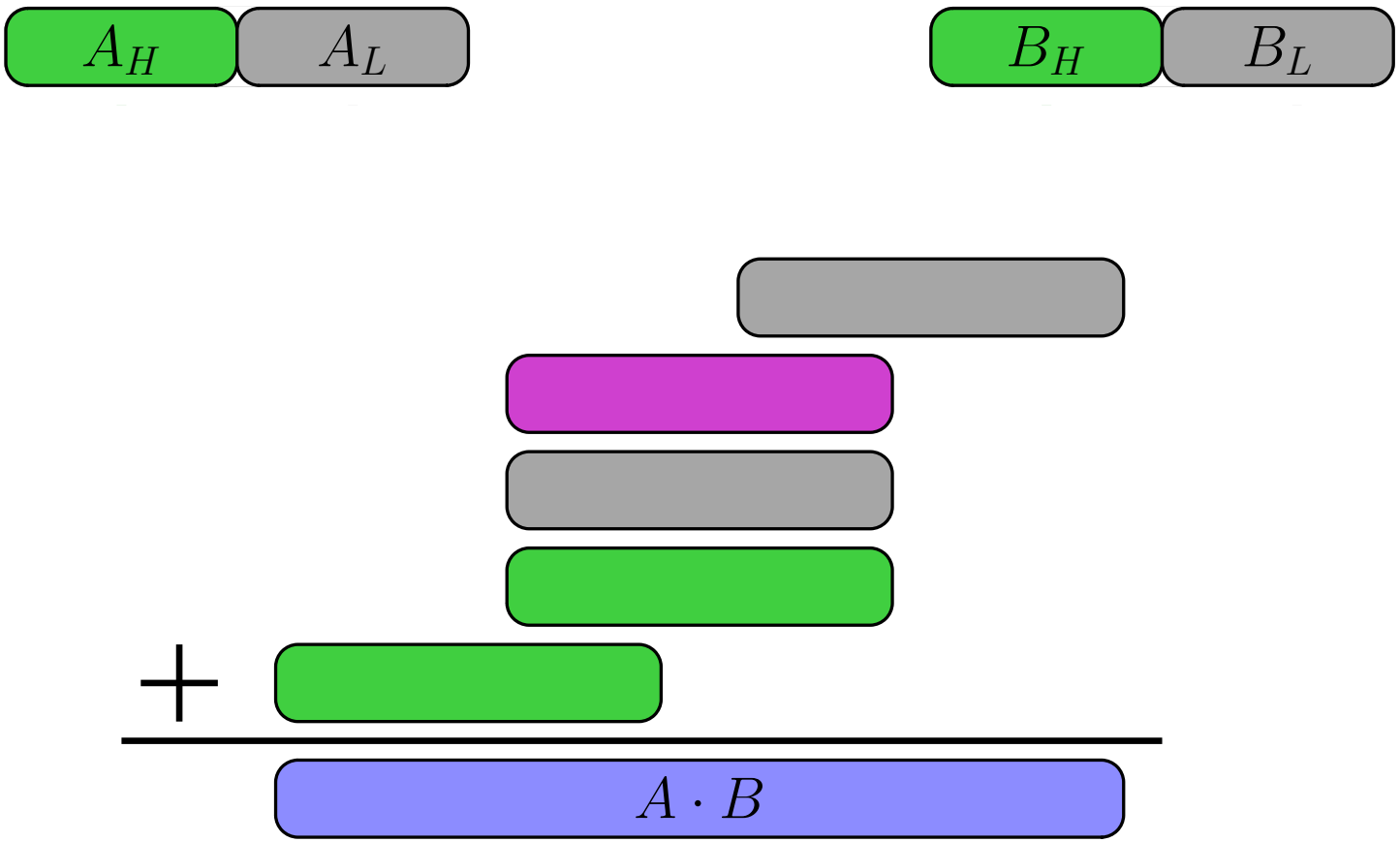
Algorithme de Karatsuba-Offman

Approche *divide-and-conquer*



Algorithme de Karatsuba-Offman

Approche *divide-and-conquer*



Complexité en $\Theta(n^{1.58})$ ◂ Karatsuba modifié

Algorithme de calcul du couplage η_T en caractéristique 2

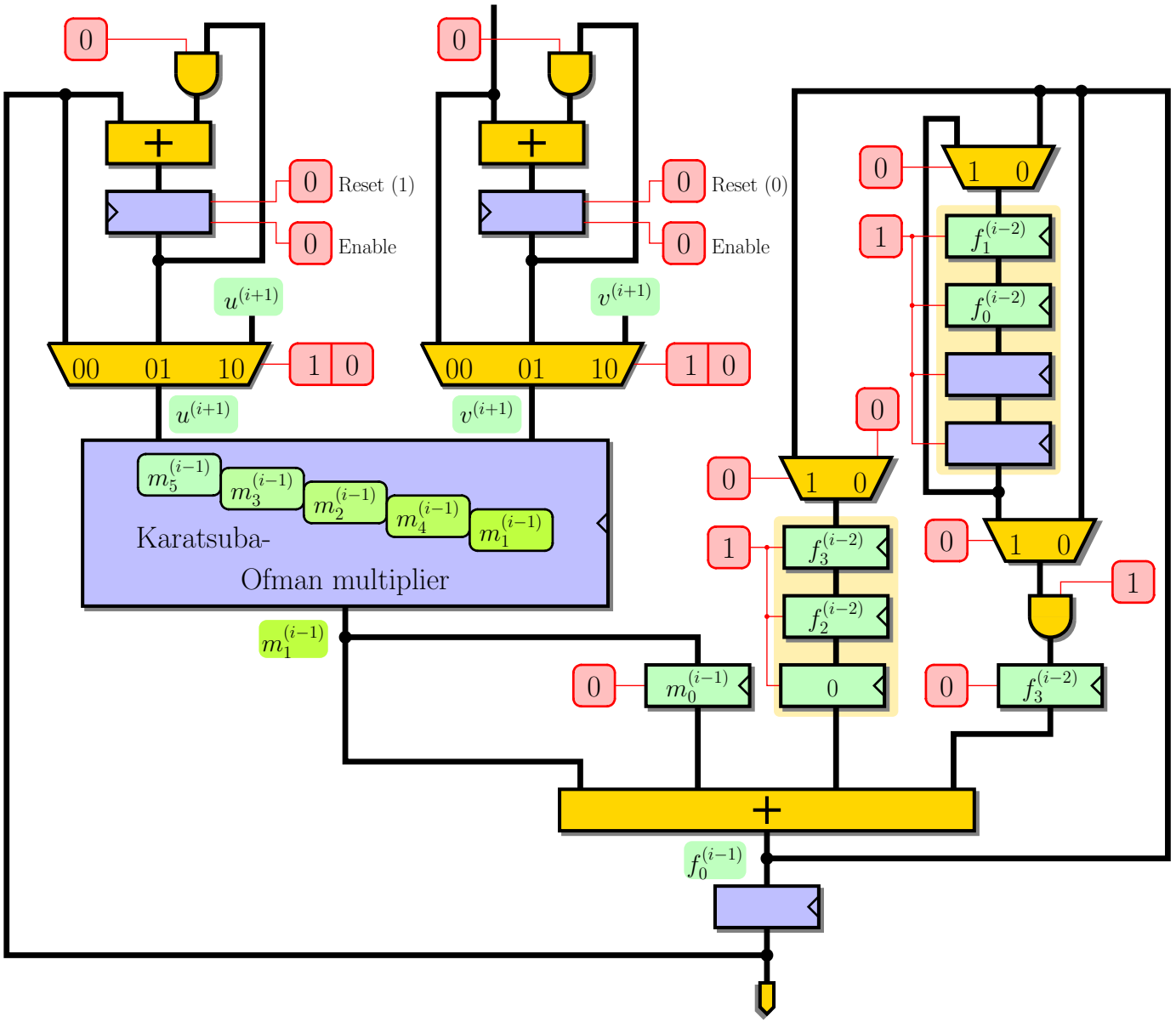
Entrée: $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$ avec $x_P, y_P, x_Q, y_Q \in \mathbb{F}_{2^m}$, $\alpha, \beta, \bar{\delta} \in \mathbb{F}_2$.
Sortie: $\eta_T(P, Q) \in \mathbb{F}^*_{2^{4m}}$.

$u, v, g_0, g_1, g_2 \in \mathbb{F}_{2^m}$,
$F, L, G \in \mathbb{F}_{2^{4m}}$,
t et s sont des symboles formels qui permettent de construire $F_{2^{4m}}$ à partir de $\mathbb{F}_{2^m}$.

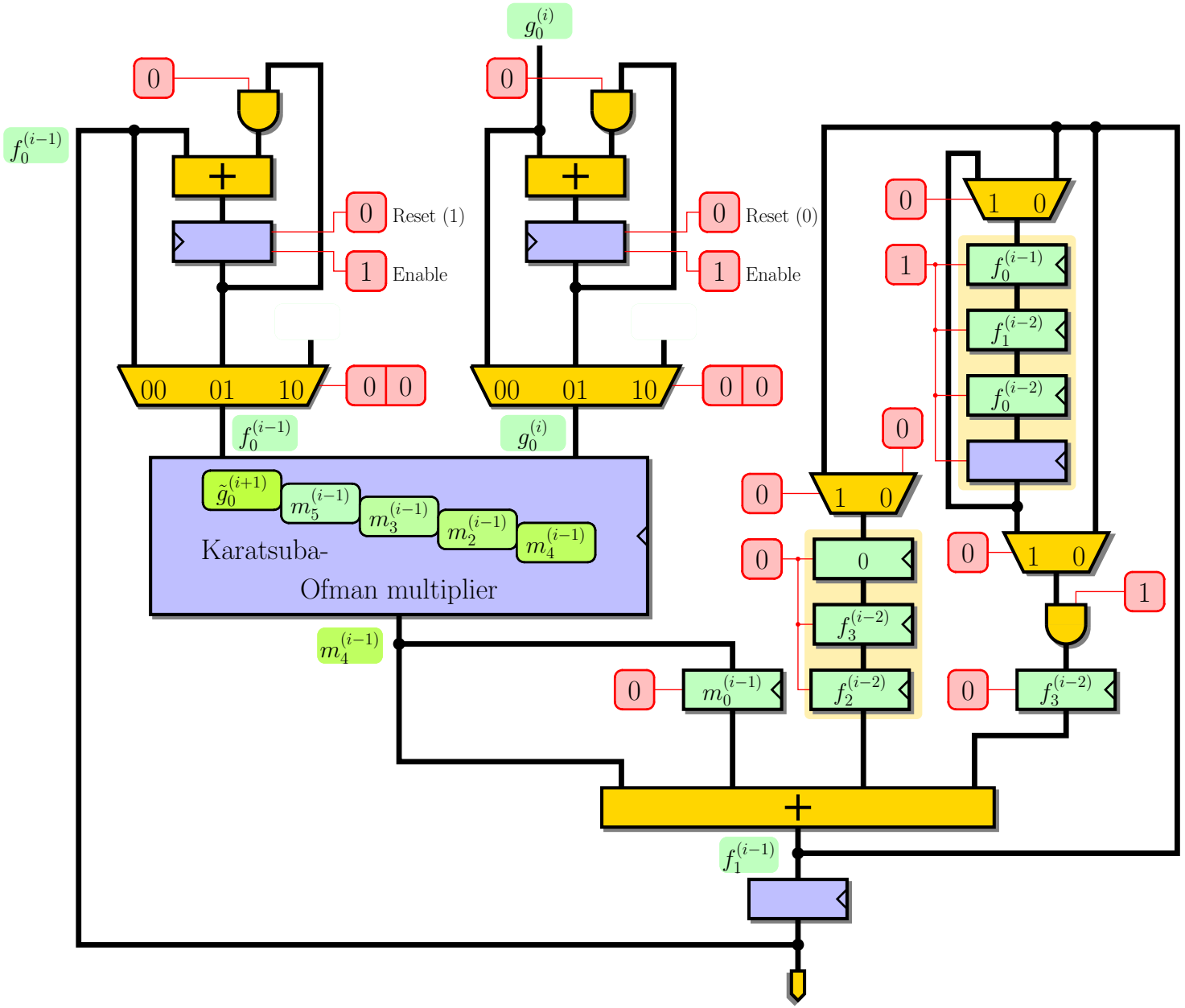
1. $y_P \leftarrow y_P + \bar{\delta}$;
2. $u \leftarrow x_P + \alpha$; $v \leftarrow x_Q + \alpha$;
3. $g_0 \leftarrow \boldsymbol{u \cdot v} + y_P + y_Q + \beta$; (1 multiplication et 2 additions sur $\mathbb{F}_{2^m}$)
4. $g_1 \leftarrow u + x_Q$; $g_2 \leftarrow v + {x_P}^2$;
5. $G \leftarrow g_0 + g_1 s + t$;
6. $L \leftarrow (g_0 + g_2) + (g_1 + 1)s + t$;
7. $F \leftarrow \boldsymbol{L \cdot G}$; (2 multiplications et 5 additions sur $\mathbb{F}_{2^m}$)
8. **for** $j = 1$ to $\frac{m-1}{2}$ **do**
9. $x_P \leftarrow \sqrt{x_P}$; $y_P \leftarrow \sqrt{y_P}$; $x_Q \leftarrow {x_Q}^2$; $y_Q \leftarrow {y_Q}^2$;
10. $u \leftarrow x_P + \alpha$; $v \leftarrow x_Q + \alpha$;
11. $g_0 \leftarrow \boldsymbol{u \cdot v} + y_P + y_Q + \beta$; (1 multiplication et 2 additions sur $\mathbb{F}_{2^m}$)
12. $g_1 \leftarrow u + x_Q$;
13. $G \leftarrow g_0 + g_1 s + t$;
14. $F \leftarrow \boldsymbol{F \cdot G}$; (6 multiplications et 14 additions sur $\mathbb{F}_{2^m}$)
15. **end for**

◂ Couplage

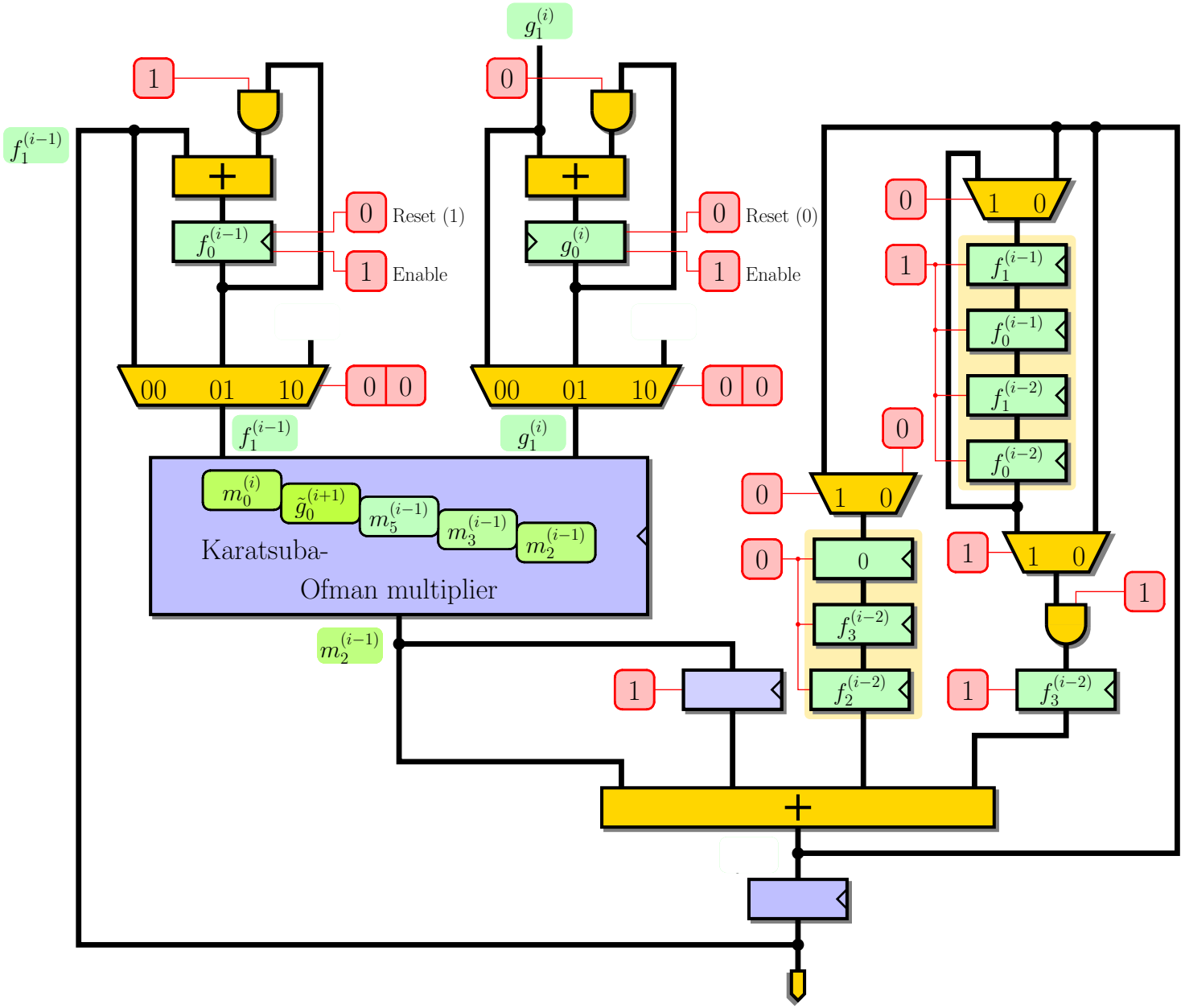
Coprocesseur de couplage en fonctionnement



Coprocesseur de couplage en fonctionnement

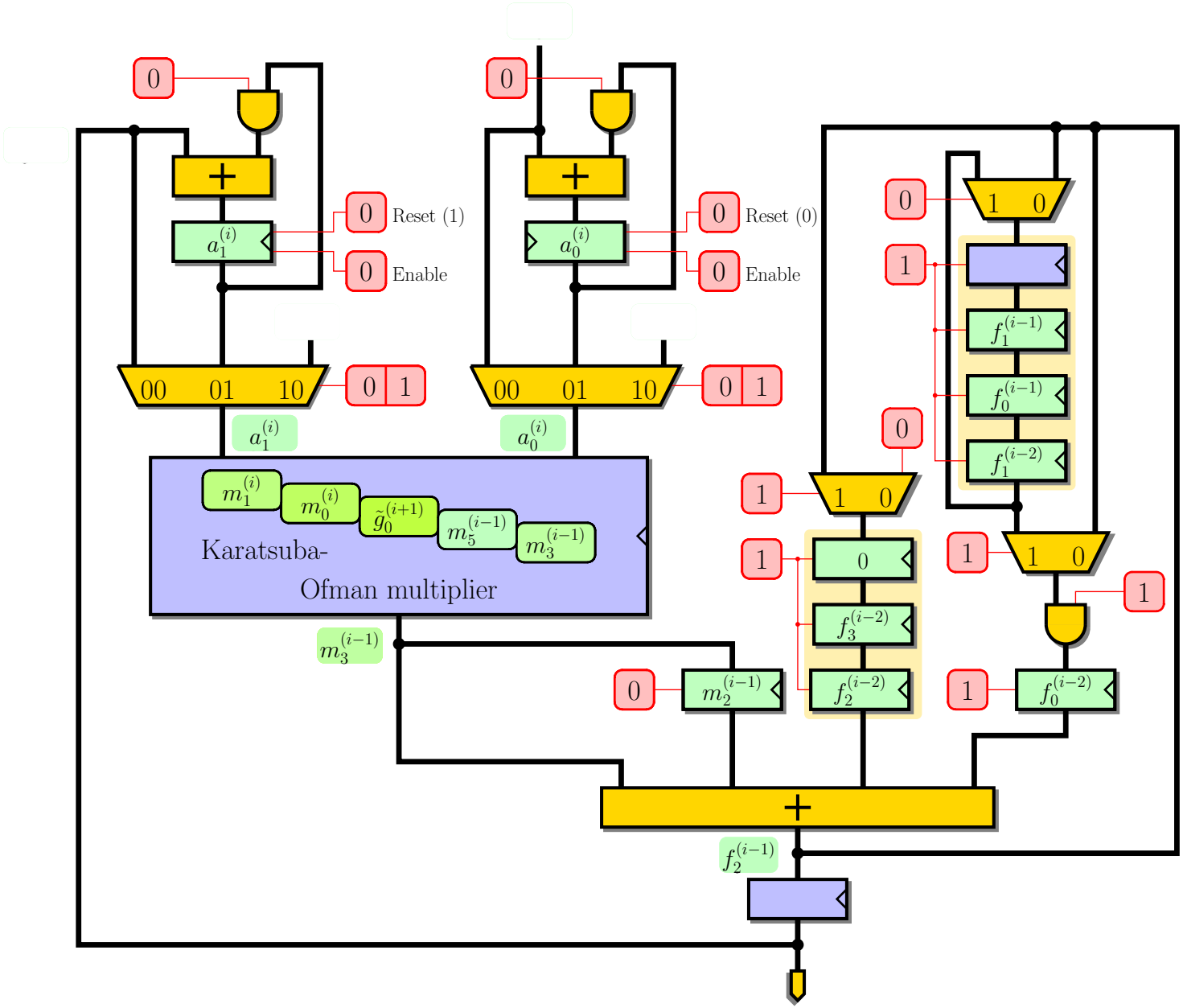


Coprocesseur de couplage en fonctionnement

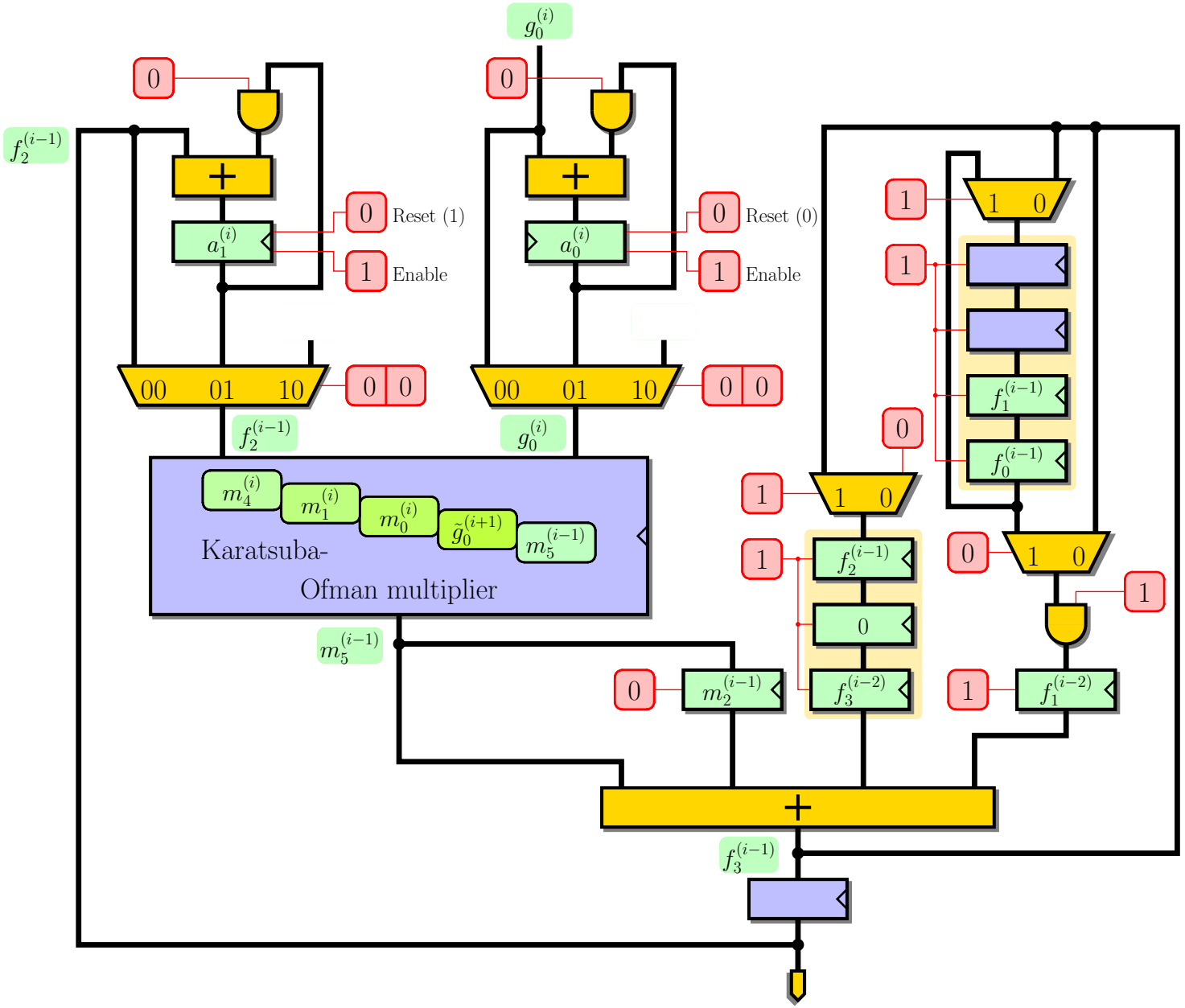


◂ Architecture

Coprocesseur de couplage en fonctionnement

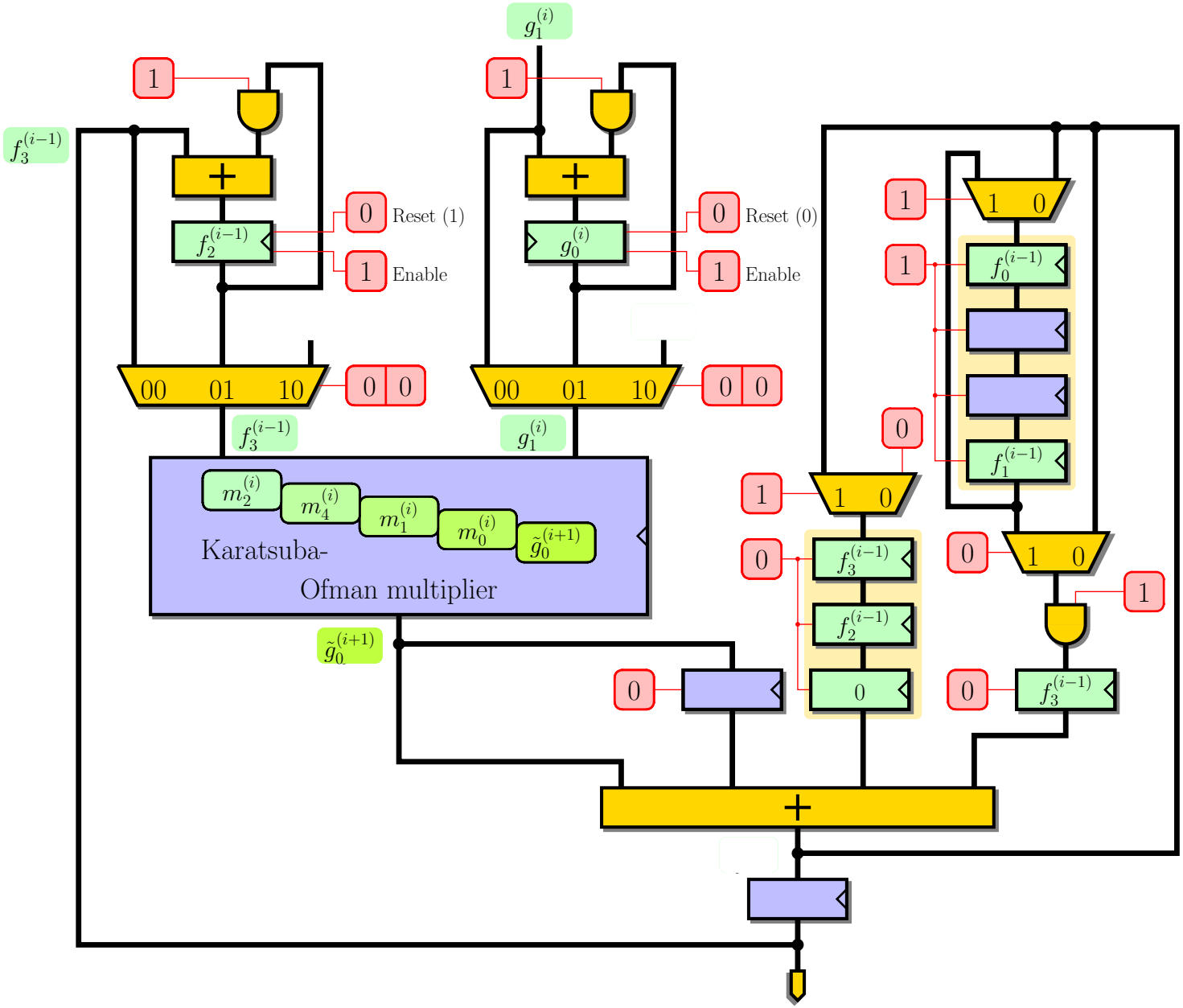


Coprocesseur de couplage en fonctionnement



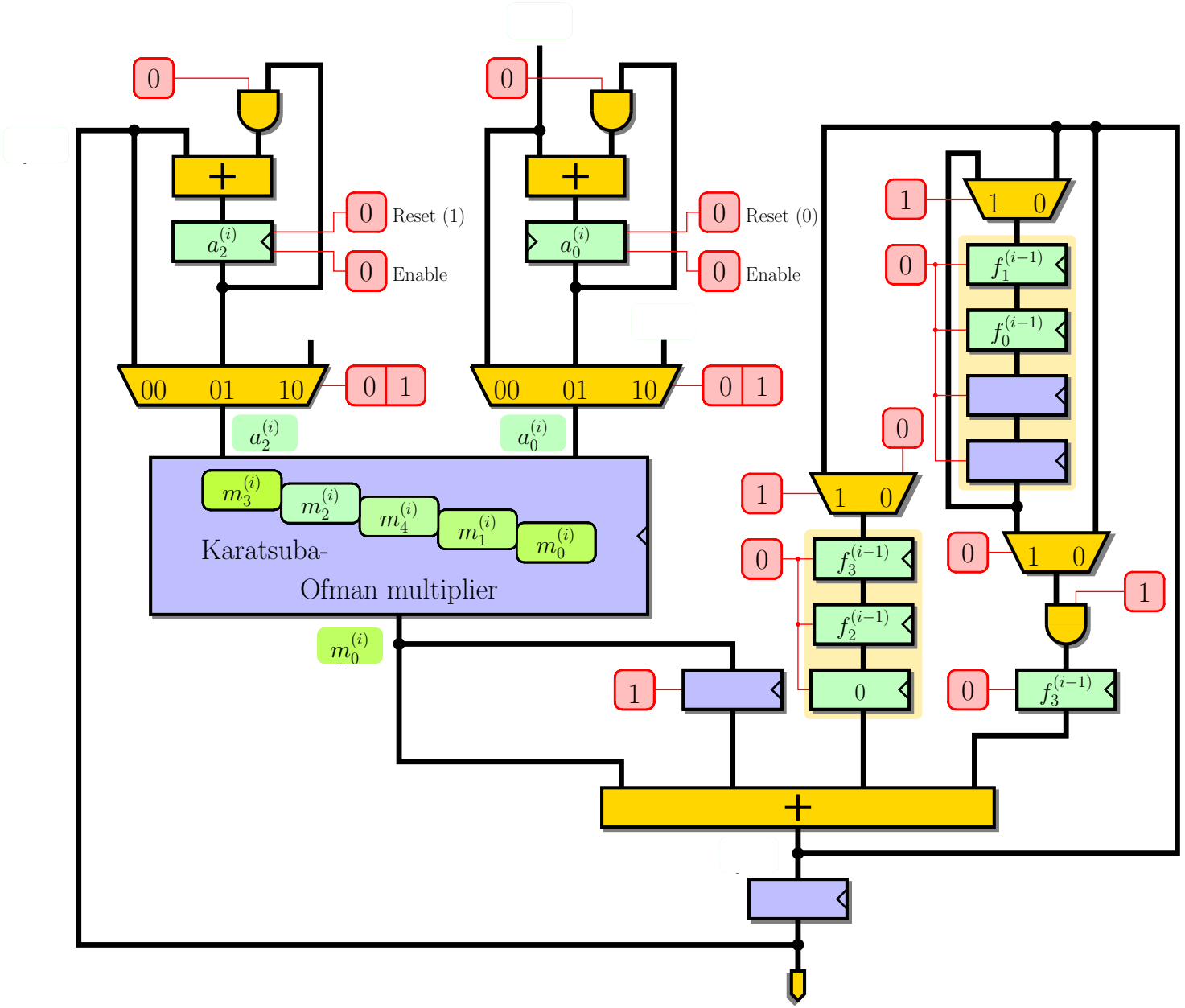
◂ Architecture

Coprocesseur de couplage en fonctionnement

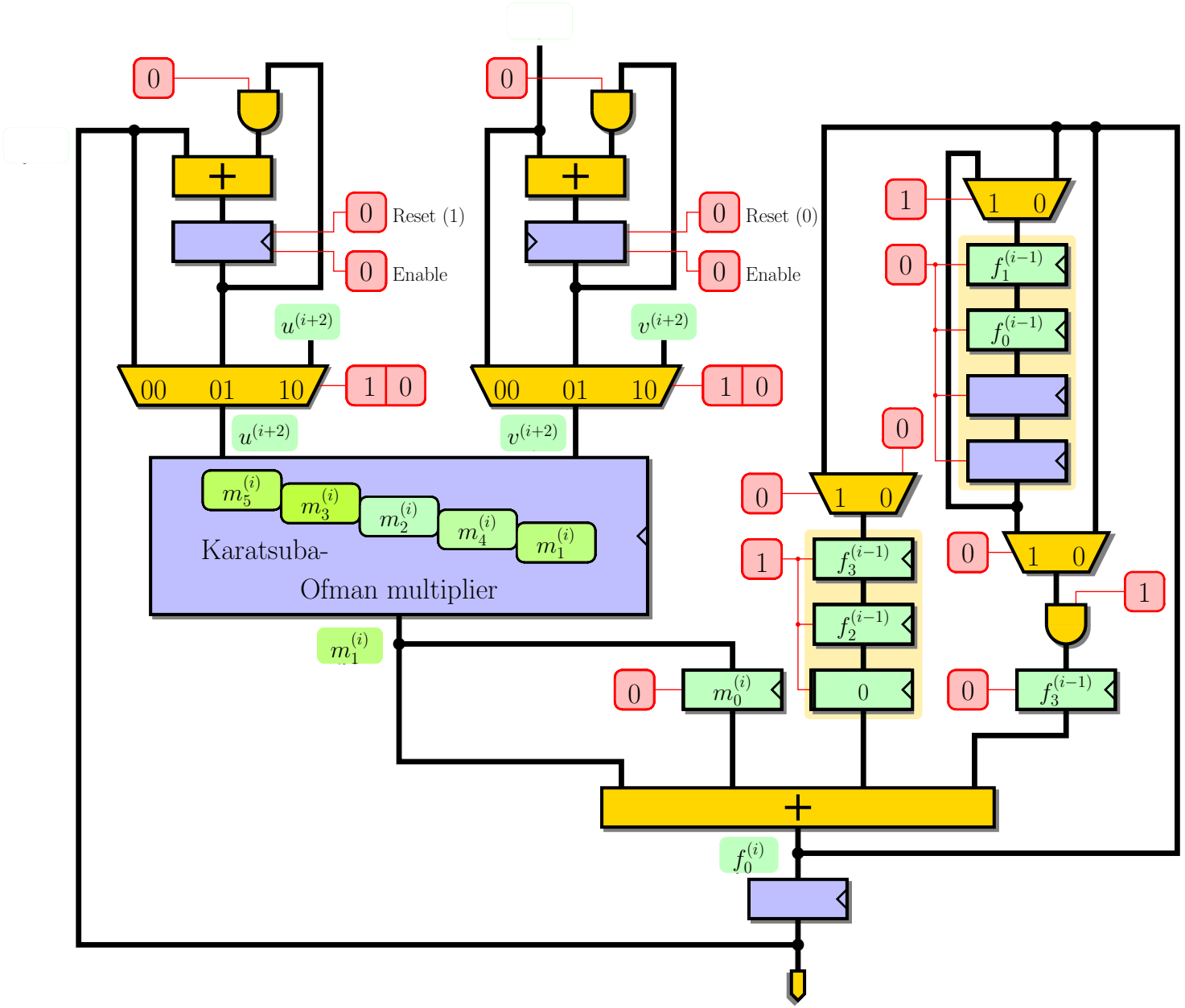


◂ Architecture

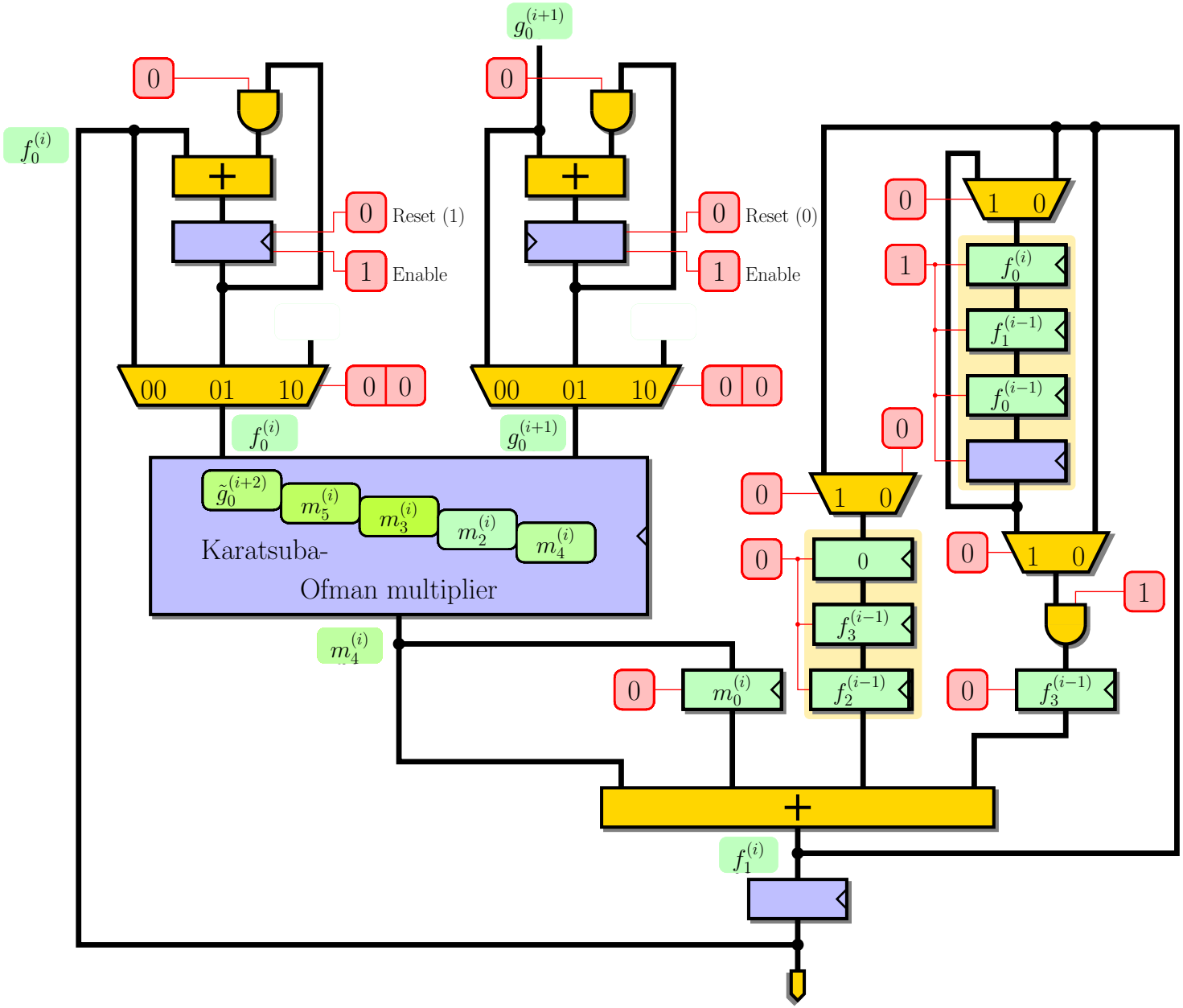
Coprocesseur de couplage en fonctionnement



Coprocesseur de couplage en fonctionnement



Coprocesseur de couplage en fonctionnement



◂ Architecture