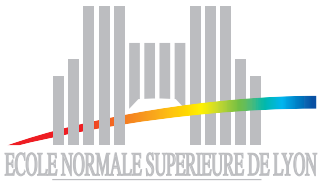
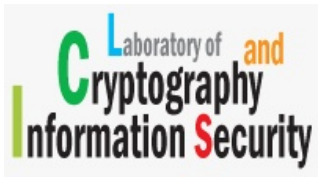
# Multiplieurs parallèles et pipelinés pour le calcul de couplage en caractéristiques 2 et 3

Nicolas Estibals

6 novembre






Contexte

Calcul de couplage

Algorithmes de multiplication sur $\mathbb{F}_{p^m}$

Architecture et implémentation du multiplieur

Performance du coprocesseur complet

Conclusion

# Introduction *(i/ii)*

- Thématique :
  - Cryptographie sur courbes elliptiques (couplages)
  - Arithmétique des corps finis
  - Matériel
- Étude des algorithmes de multiplication sur $\mathbb{F}_{p^m}$
- Implémentation matérielle sur FPGA



Contexte

Calcul de couplage

Algorithmes de multiplication sur $\mathbb{F}_{p^m}$

Architecture et implémentation du multiplieur

Performance du coprocesseur complet

Conclusion

# Introduction *(ii/ii)*

- Travaux réalisés durant mon stage de Master 1 :
  - au LCIS (Laboratory of Cryptography and Information Security)
  - à l'université de Tsukuba, Japon
  - sous l'encadrement de Jean-Luc Beuchat
- Travaux réalisés en collaboration avec :

| | |
|---|---|
| Jean-Luc Beuchat | LCIS, Université de Tsukuba, Japon |
| Nidia Cortez-Duarte | CSD, IPN, Mexico, Mexique |
| Jérémie Detrey | Équipe CACAO, INRIA Nancy - Grand Est, France |
| Eiji Okamoto | LCIS, Université de Tsukuba, Japon |
| Francisco Rodríguez-Henríquez | CSD, IPN, Mexico, Mexique |



Contexte

Calcul de couplage

Algorithmes de multiplication sur $\mathbb{F}_{p^m}$

Architecture et implémentation du multiplieur

Performance du coprocesseur complet

Conclusion

# Plan de l'exposé


Contexte

Calcul de couplage

Algorithmes de multiplication sur $\mathbb{F}_{p^m}$

Architecture et implémentation du multiplieur

Performance du coprocesseur complet

Conclusion





Contexte

Calcul de couplage

Algorithmes de multiplication sur $\mathbb{F}_{p^m}$

Architecture et implémentation du multiplieur

Performance du coprocesseur complet

Conclusion

Contexte

Calcul de couplage

Algorithmes de multiplication sur $\mathbb{F}_{p^m}$

Architecture et implémentation du multiplieur

Performance du coprocesseur complet

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

| 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, ...)



Contexte

Calcul de couplage

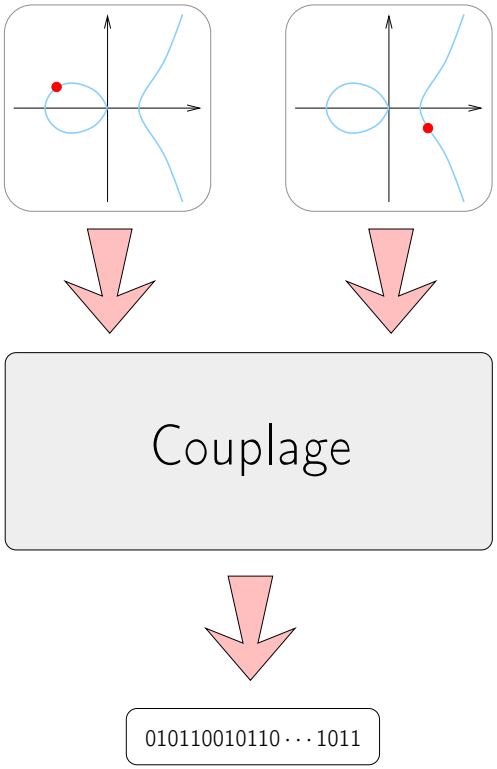
Algorithmes de multiplication sur $\mathbb{F}_{p^m}$

Architecture et implémentation du multiplieur

Performance du coprocesseur complet

Conclusion

# 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 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 :

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

$$\forall P \in G_1^*, \hat{e}(P, P) \neq 1$$

$G_1$ est un sous-groupe des points d'une courbe elliptique sur $\mathbb{F}_{p^m}$,
$G_2$ un sous-groupe d'une extension de $\mathbb{F}_{p^m}$.

# Les couplages en matériel

Calcul d'un couplage :

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

Développer du matériel pour :

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



Contexte

Calcul de couplage

Algorithmes de multiplication sur $\mathbb{F}_{p^m}$

Architecture et implémentation du multiplieur

Performance du coprocesseur complet

Conclusion

# Motivations

Coprocesseur calculant un couplage :

- Architecture et algorithme adaptables :
  - Caractéristiques 2 et 3
  - Différents niveaux de sécurité
- Rapide

Multiplieur performant :

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



Contexte

Calcul de couplage

Algorithmes de multiplication sur $\mathbb{F}_{p^m}$

Architecture et implémentation du multiplieur

Performance du coprocesseur complet

Conclusion

Contexte

Calcul de couplage

Algorithmes de multiplication sur $\mathbb{F}_{p^m}$

Architecture et implémentation du multiplieur

Performance du coprocesseur complet

Conclusion



Contexte

Calcul de couplage

Algorithmes de multiplication sur $\mathbb{F}_{p^m}$

Architecture et implémentation du multiplieur

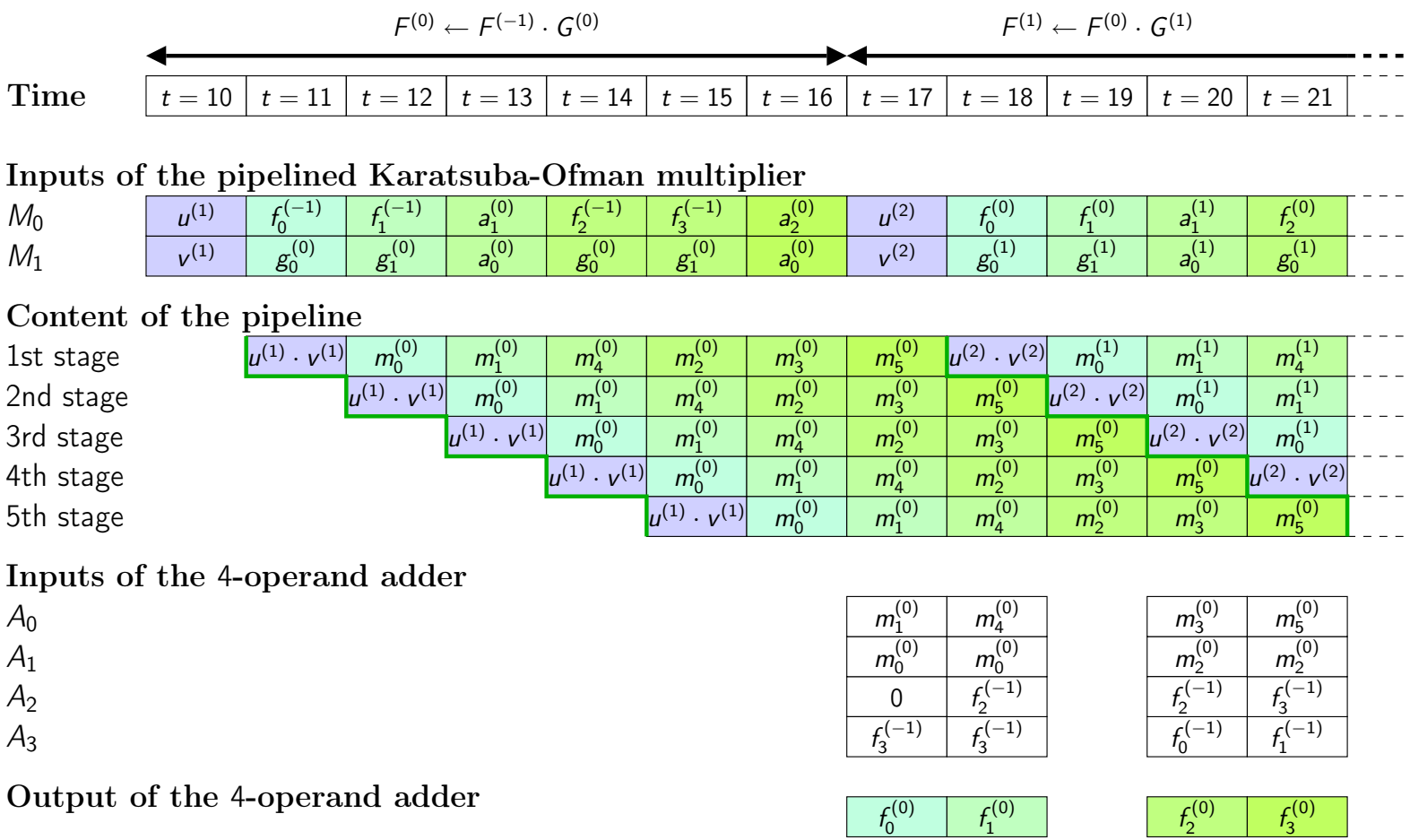
Performance du coprocesseur complet

Conclusion

# Algorithmes de couplage

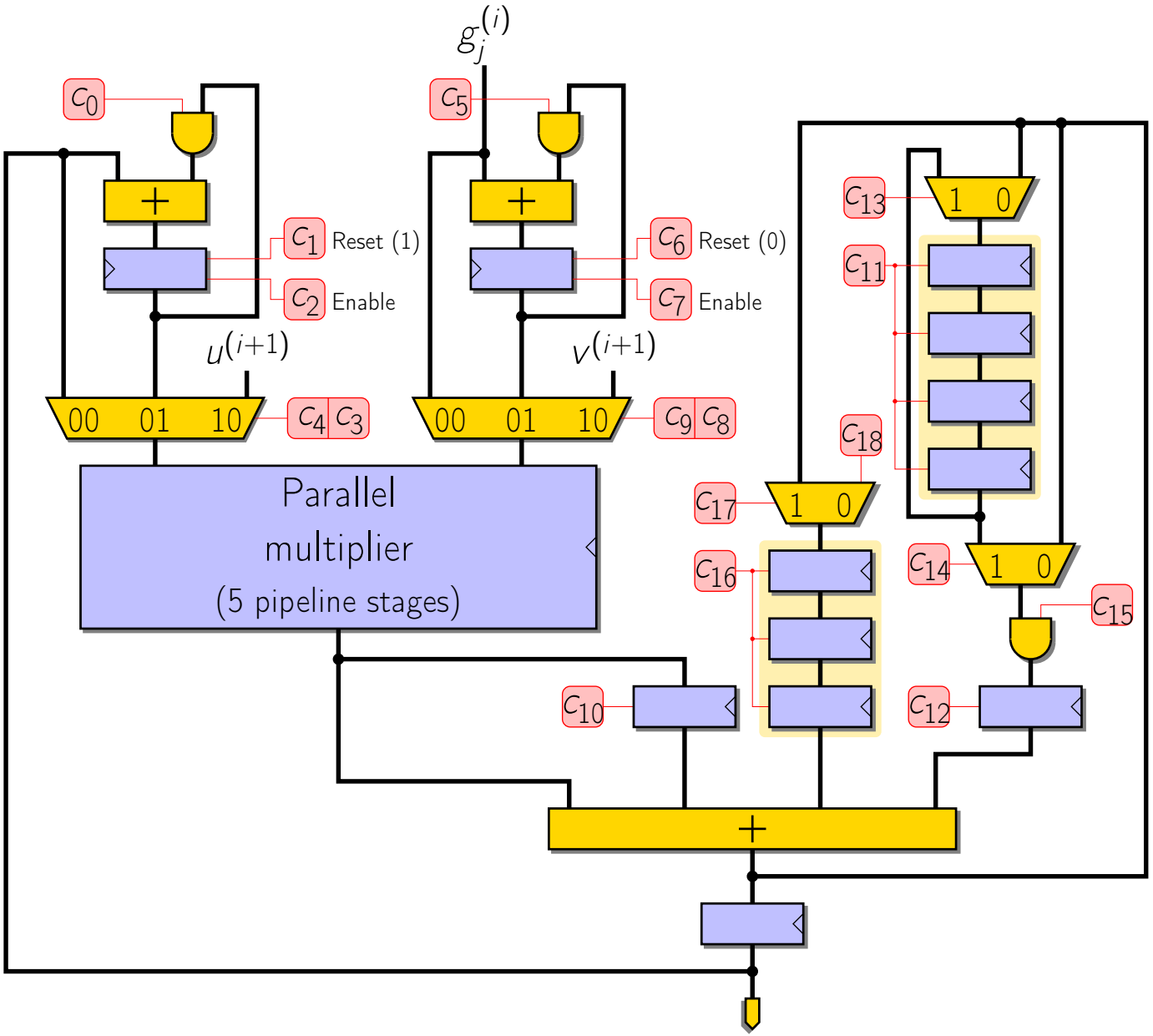
- Weil(1940), Tate(1966) : définitions mais calcul exponentiel
- Miller(1986) : premier algorithme efficace, une boucle avec :
  - Additions, Frobenius sur $\mathbb{F}_{p^m}$ (facile)
  - Multiplications sur $\mathbb{F}_{p^m}$ (difficile)
- Nombreuses variations et améliorations par la suite
- $\eta_T$ meilleur moyen de calculer un couplage de Tate
- Quel multiplieur pour quelles performances ?
- Problème : s'assurer que le pipeline reste plein

# Un ordonnancement serré (caractéristique 2)




$\Rightarrow$ Avec un multiplieur en 5 cycles le pipeline reste rempli

# Design du coprocesseur (caractéristique 2)



Contexte

Calcul de couplage

Algorithmes de multiplication sur $\mathbb{F}_{p^m}$

Architecture et implémentation du multiplieur

Performance du coprocesseur complet

Conclusion



Contexte

Calcul de couplage

Algorithmes de multiplication sur $\mathbb{F}_{p^m}$

Architecture et implémentation du multiplieur

Performance du coprocesseur complet

Conclusion

# De $\mathbb{F}_{p^m}$ à $\mathbb{F}_p[X]$

- Représentation des éléments de $\mathbb{F}_{p^m}$
  $\Rightarrow$ Polynômes sur $\mathbb{F}_p$ modulo un polynôme irréductible
- Représentation canonique
  $\Rightarrow$ Polynôme de degré $m-1$ au plus

# De $\mathbb{F}_{p^m}$ à $\mathbb{F}_p[X]$

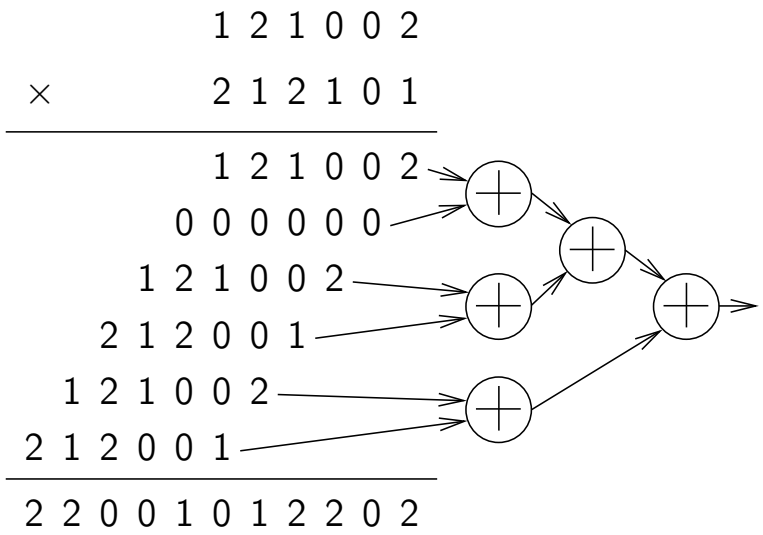
- Représentation des éléments de $\mathbb{F}_{p^m}$
  $\Rightarrow$ Polynômes sur $\mathbb{F}_p$ modulo un polynôme irréductible
- Représentation canonique
  $\Rightarrow$ Polynôme de degré $m-1$ au plus
- Multiplier deux polynômes de degré $m-1$ donne un polynôme de degré $2m-2$ au plus

# De $\mathbb{F}_{p^m}$ à $\mathbb{F}_p[X]$

- Représentation des éléments de $\mathbb{F}_{p^m}$
  $\Rightarrow$ Polynômes sur $\mathbb{F}_p$ modulo un polynôme irréductible
- Représentation canonique
  $\Rightarrow$ Polynôme de degré $m-1$ au plus
- Multiplier deux polynômes de degré $m-1$ donne un polynôme de degré $2m-2$ au plus
- Choix du polynôme irréductible déterminant
- Polynôme le plus creux possible
  $\Rightarrow$ Réduction modulaire plus simple

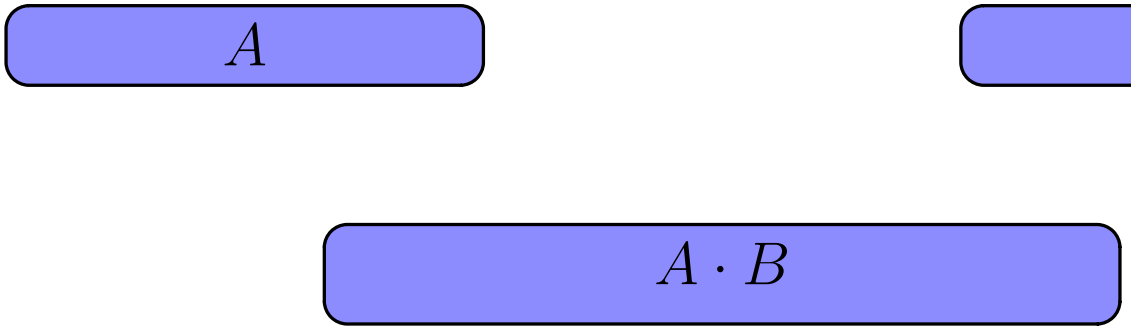
# Algorithme naïf

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



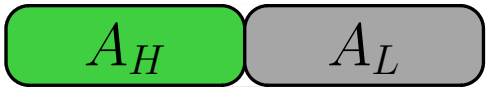

$$(X^5 + 2X^4 + X^3 + 2)$$
$$\times(2X^5 + X^4 + 2X^3 + X^2 + 1)$$
$$= 2X^{10} + 2X^9 + X^6 + X^4 + 2X^3$$
$$+2X^2 + 2$$

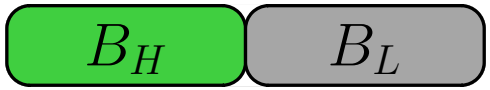
# Algorithme de Karatsuba-Offman



# Algorithme de Karatsuba-Offman

Approche *divide-and-conquer*

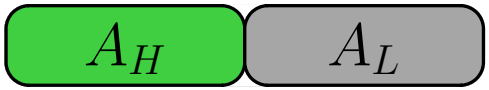


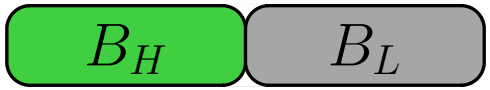




$$A_H B_H X^{2n} + (A_H B_L + A_L B_H) X^n + A_L B_L$$

# Algorithme de Karatsuba-Offman

Approche *divide-and-conquer*



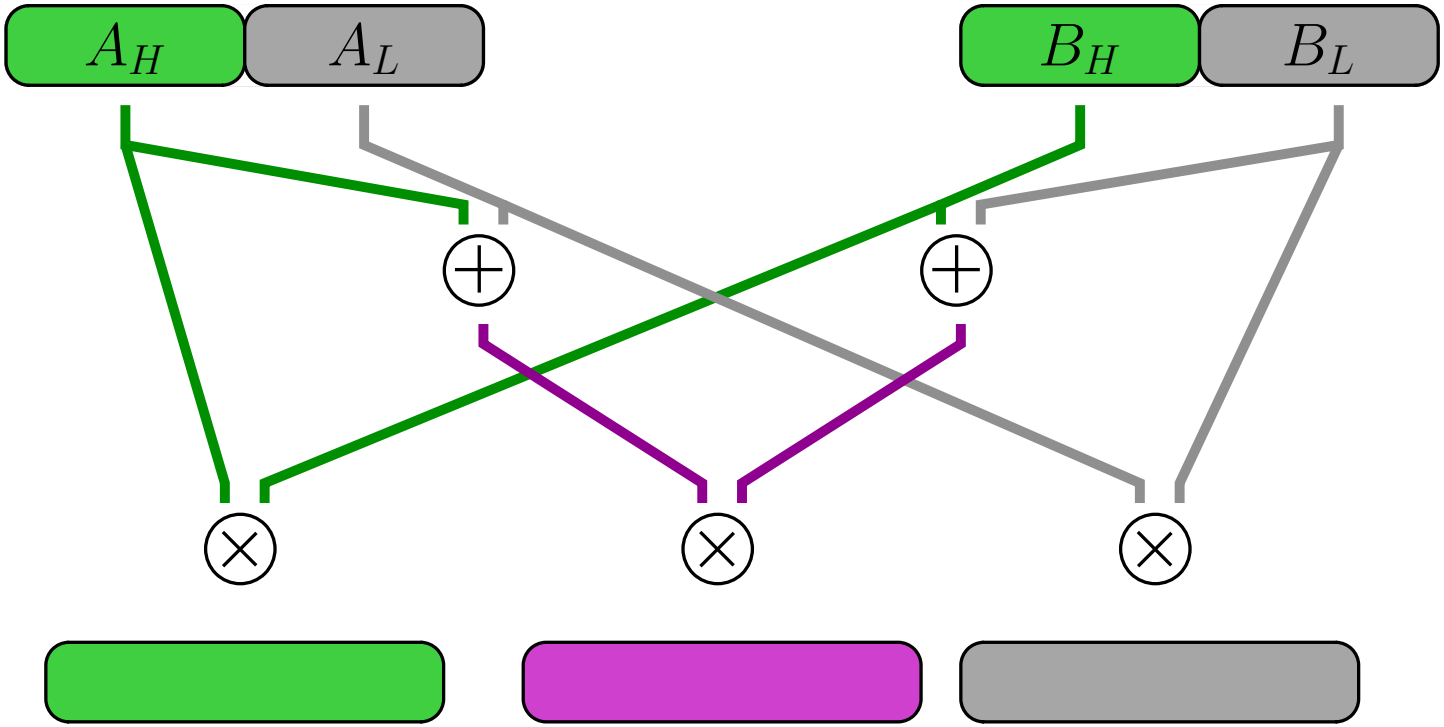

$$A_H B_H X^{2n} + (A_H B_L + A_L B_H) X^n + A_L B_L$$

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

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

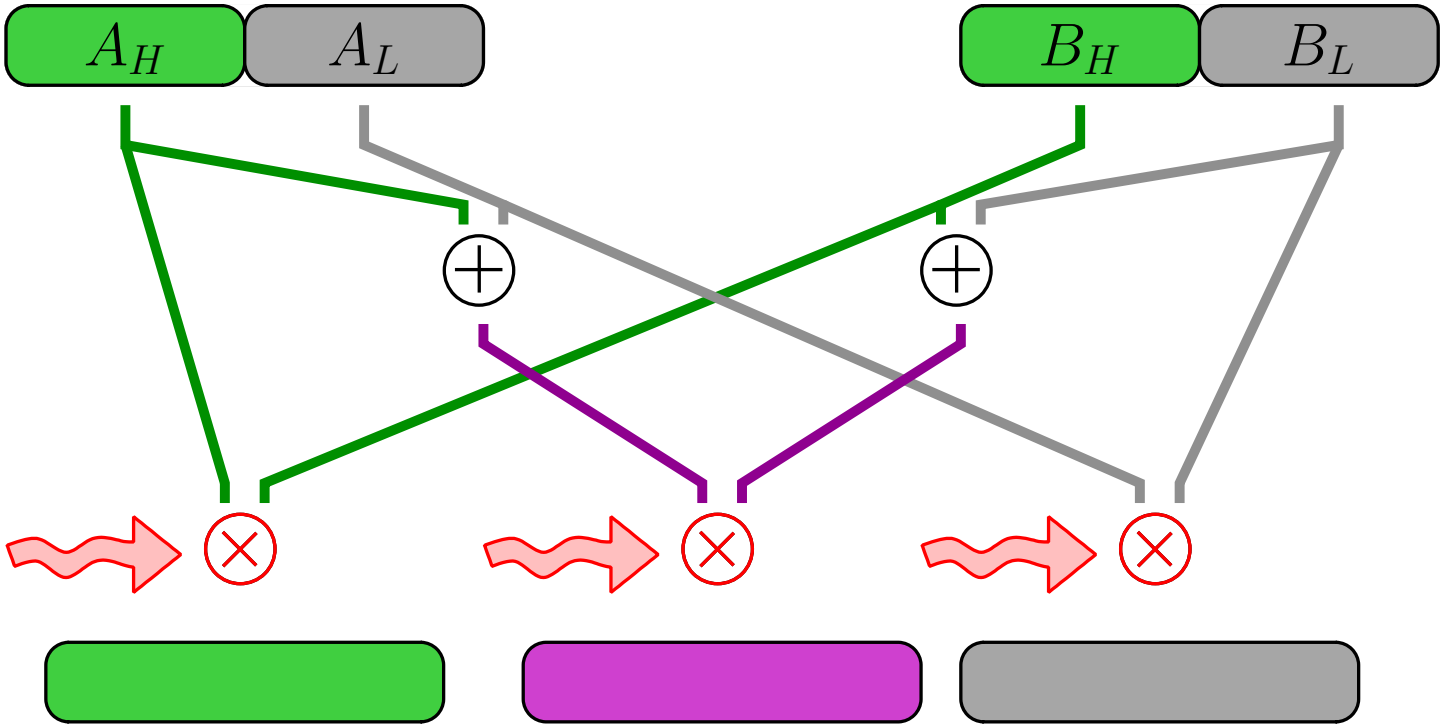
# Algorithme de Karatsuba-Offman

Approche *divide-and-conquer*



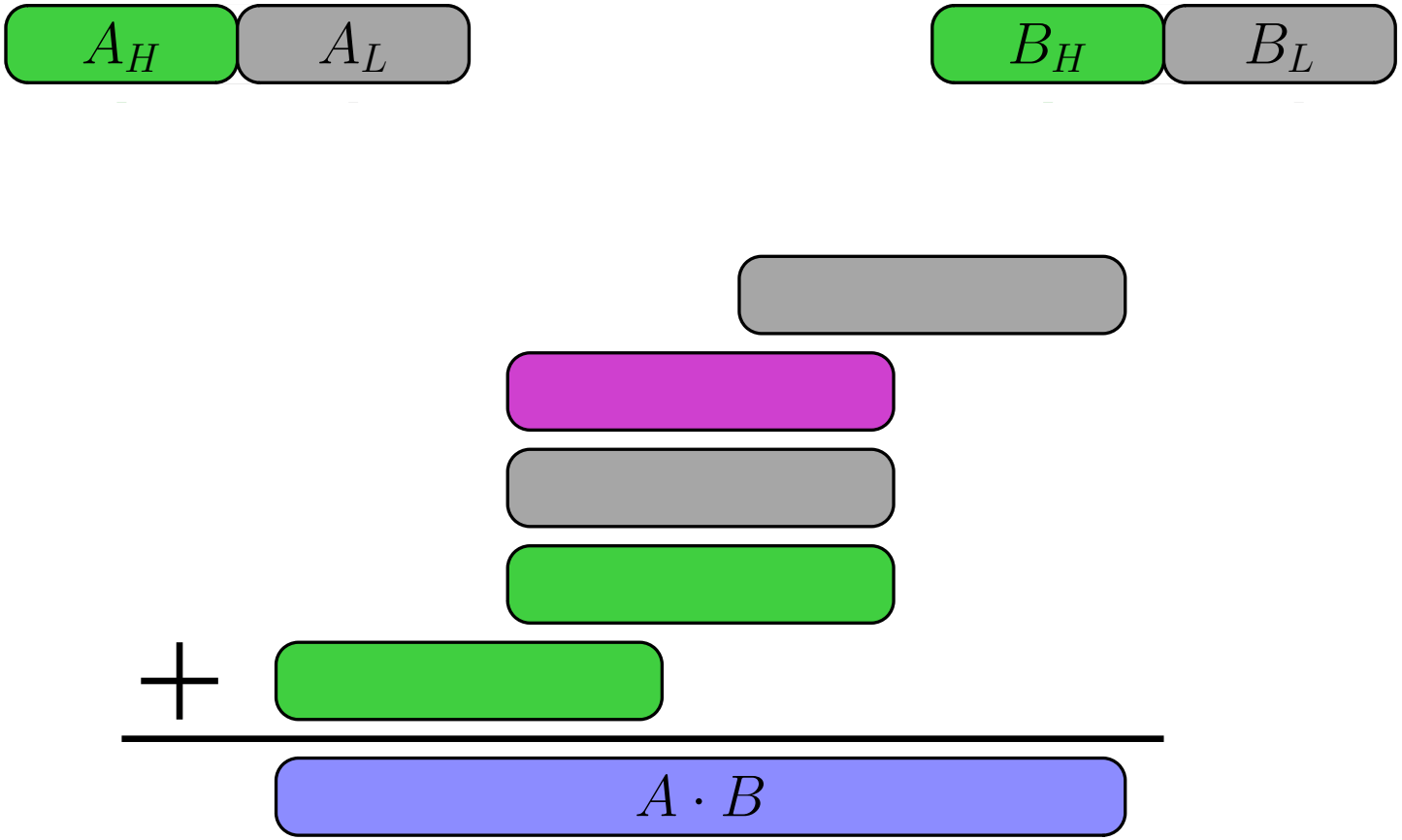
# Algorithme de Karatsuba-Offman

Approche *divide-and-conquer*



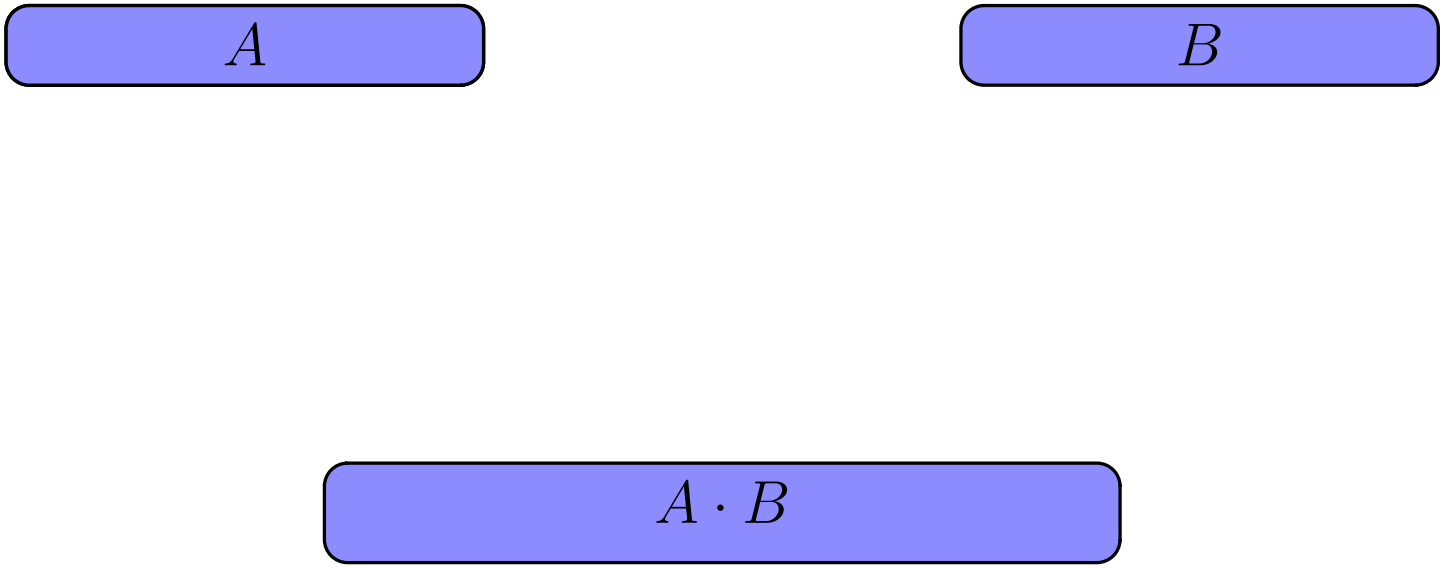
# Algorithme de Karatsuba-Offman

Approche *divide-and-conquer*

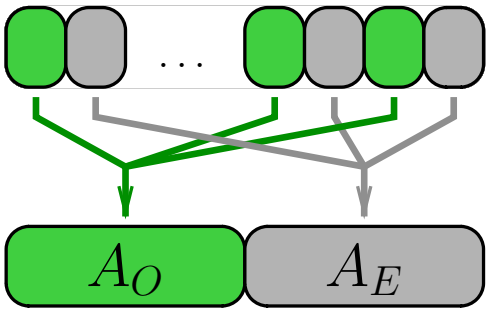


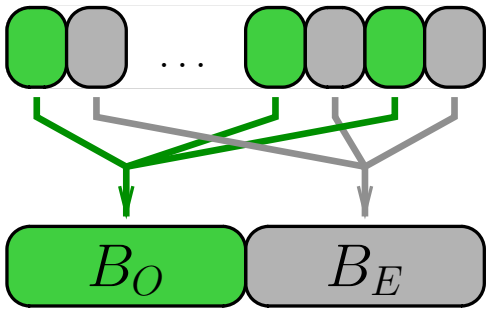

Complexité en $\Theta(n^{1.58})$

# Algorithme de Karatsuba-Offman sans recouvrement



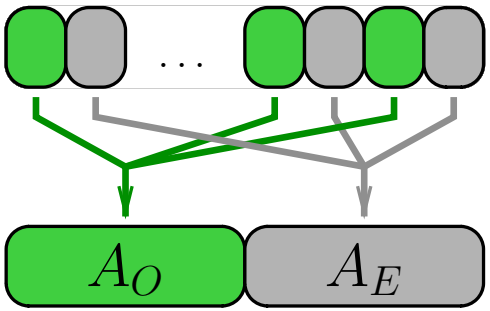
# Algorithme de Karatsuba-Offman sans recouvrement

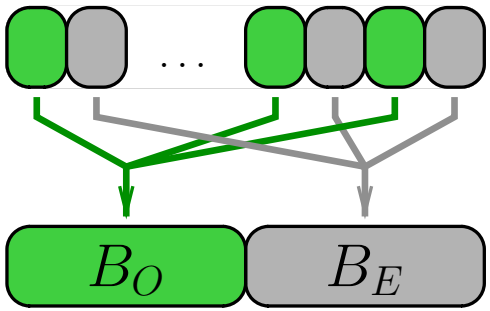



$$(A_0 B_O X^2 + A_E B_E) + X(A_O B_E + A_E B_O)$$

# Algorithme de Karatsuba-Offman sans recouvrement



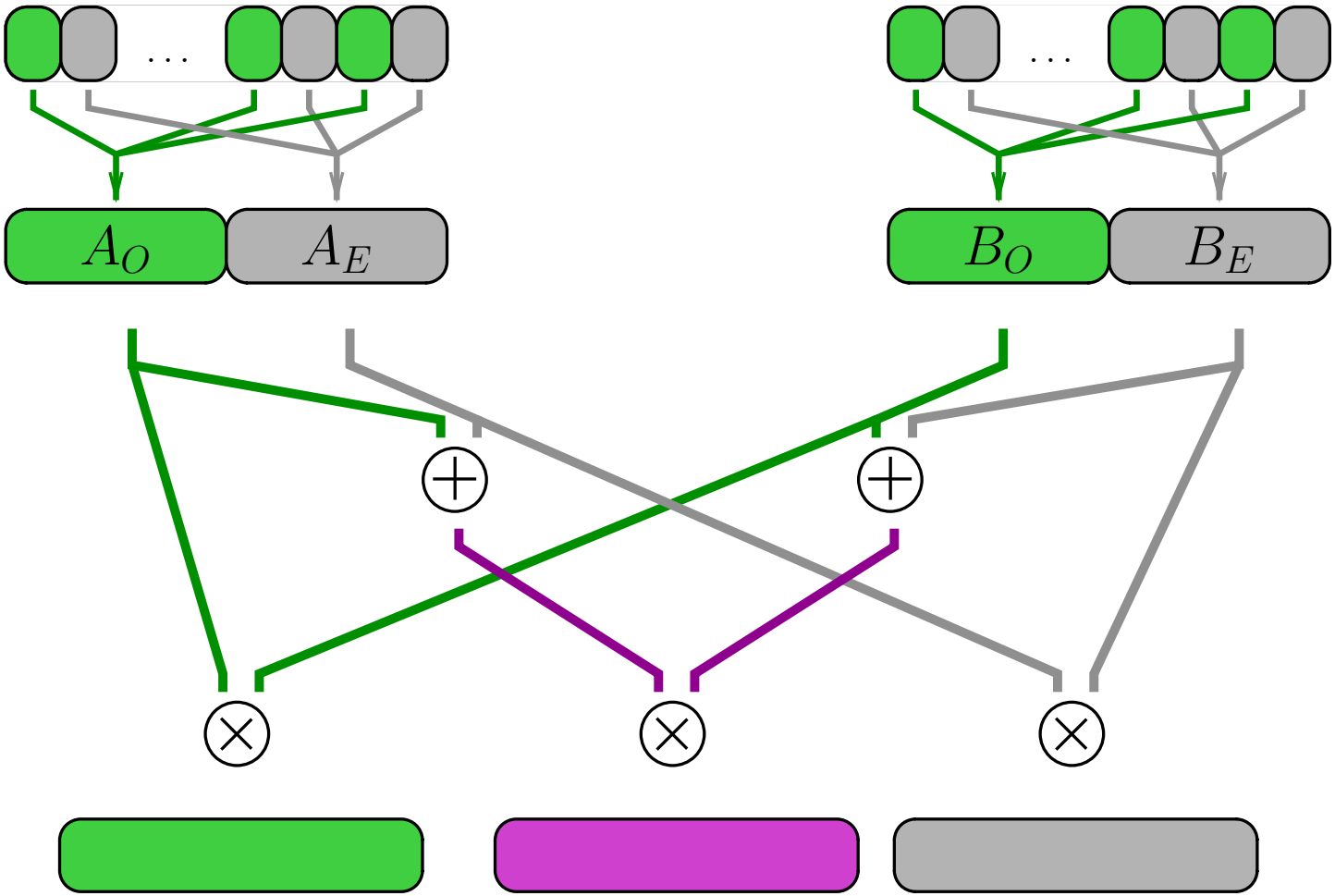




$$(A_0B_OX^2 + A_EB_E) + X(A_OB_E + A_EB_O)$$

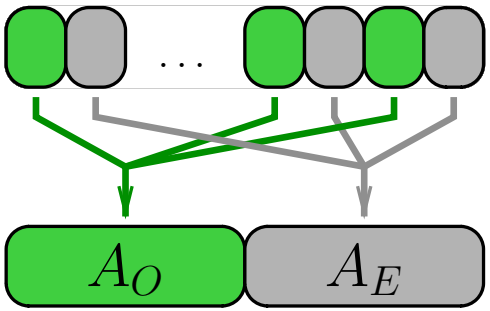
$$ab' + a'b = (a + a')(b + b') - ab - a'b'$$

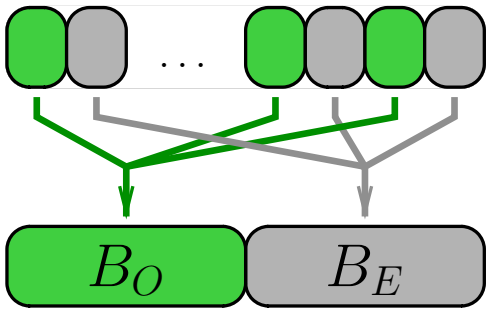
$$(A_0B_OX^2 + A_EB_E) + X((A_O + A_E)(B_O + B_E) - A_OB_O - A_EB_E)$$

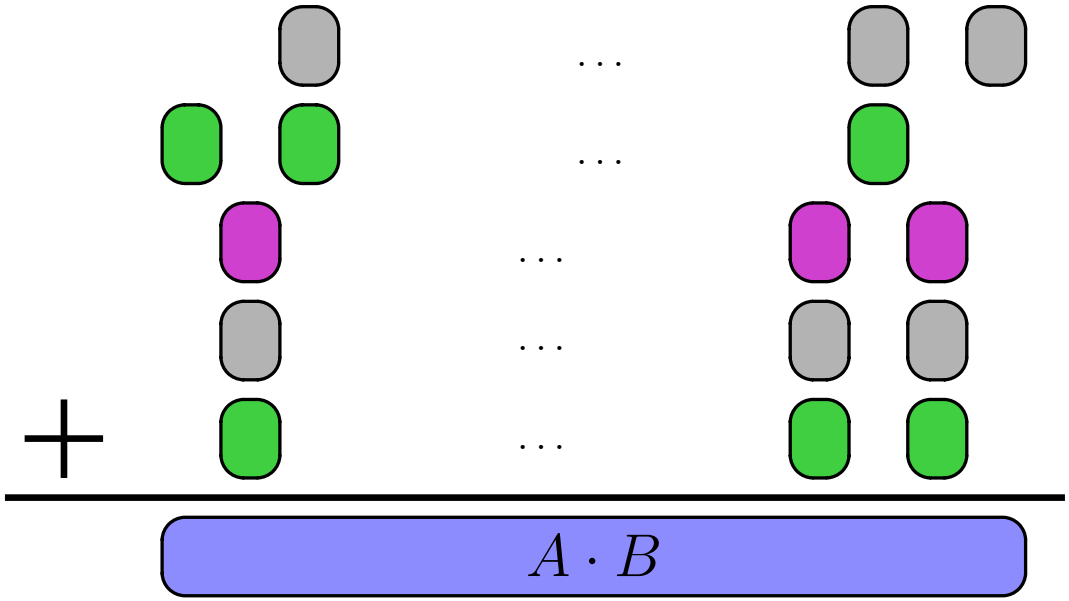
# Algorithme de Karatsuba-Offman sans recouvrement



# Algorithme de Karatsuba-Offman sans recouvrement



# D'autres variations

- Karatsuba-Offman : découpe des opérandes en 3, 5, ... parties
- Toom-Cook : schéma en évaluation-interpolation
- Formule de Montgomery, ...
- Encore à explorer

# Une approche mixte

- 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
- Et quand $m$ grandit encore ?
- Éviter l'ajout de zéros non significatifs



Contexte

Calcul de couplage

Algorithmes de multiplication sur $\mathbb{F}_{p^m}$

Architecture et implémentation du multiplieur

Performance du coprocesseur complet

Conclusion

Contexte

Calcul de couplage

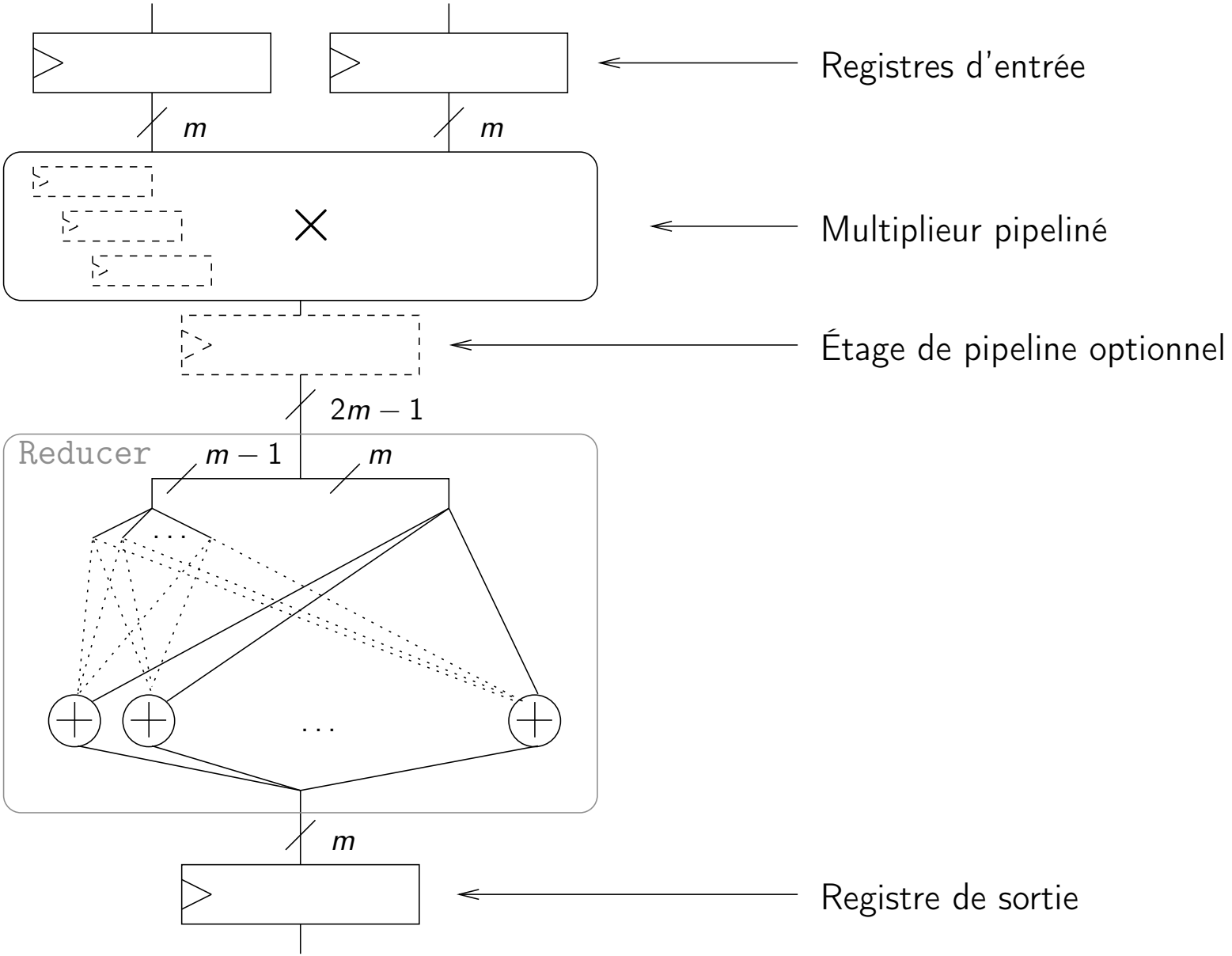
Algorithmes de multiplication sur $\mathbb{F}_{p^m}$

Architecture et implémentation du multiplieur

Performance du coprocesseur complet

Conclusion

# Architecture du multiplieur




Multiplieurs parallèles pipelinés sur corps fini

Nicolas Estibals

Contexte

Calcul de couplage

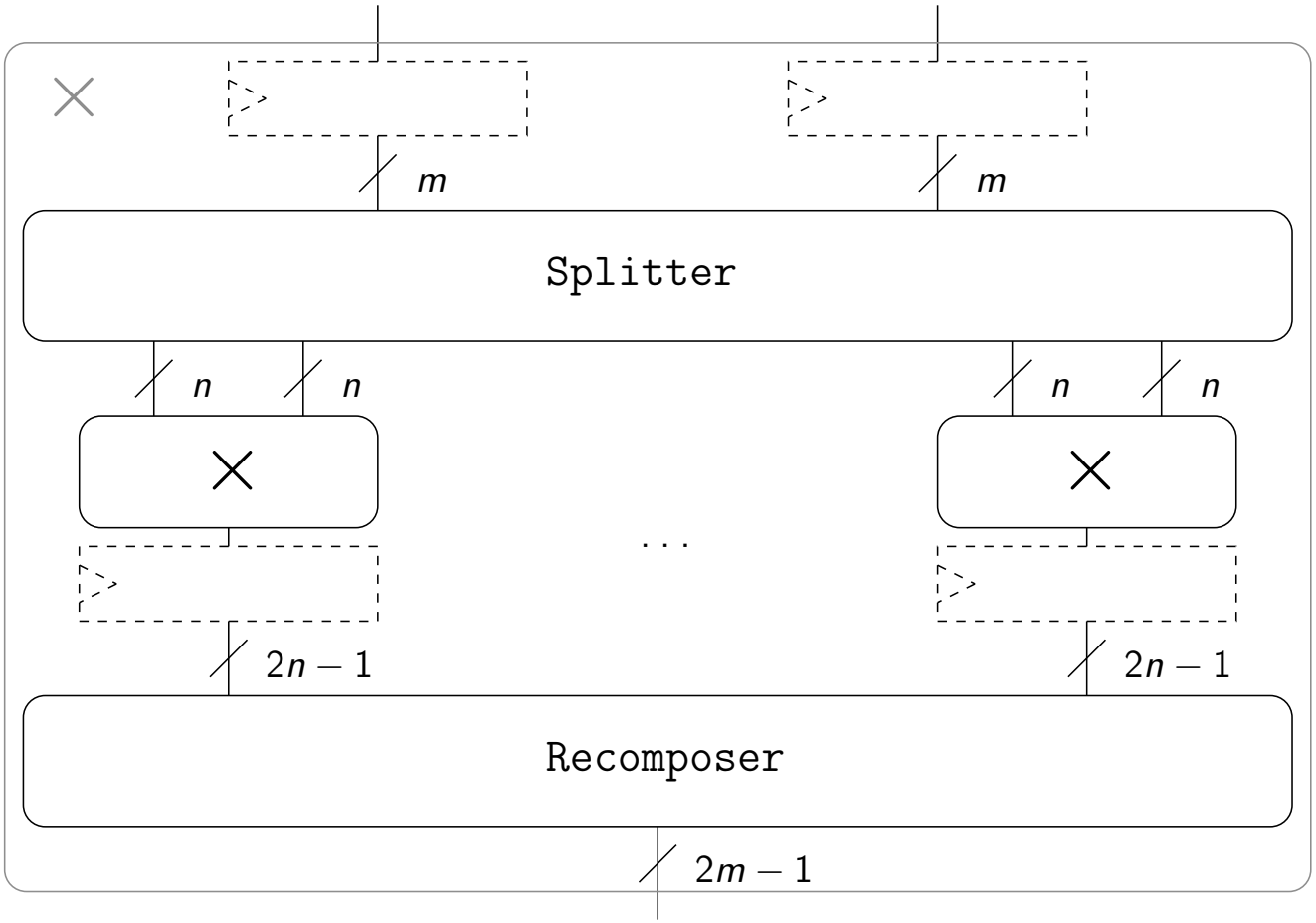
Algorithmes de multiplication sur $\mathbb{F}_{p^m}$

Architecture et implémentation du multiplieur

Performance du coprocesseur complet

Conclusion

# Architecture d'un étage de récursion pour le multiplieur



# Un générateur d'architecture *(i/ii)*

- Besoin d'implémentation en caractéristique 2 et 3, pour différentes tailles
- Tester différentes implémentations
- Tester différents niveaux de pipeline
- Tester différents compromis temps-surface

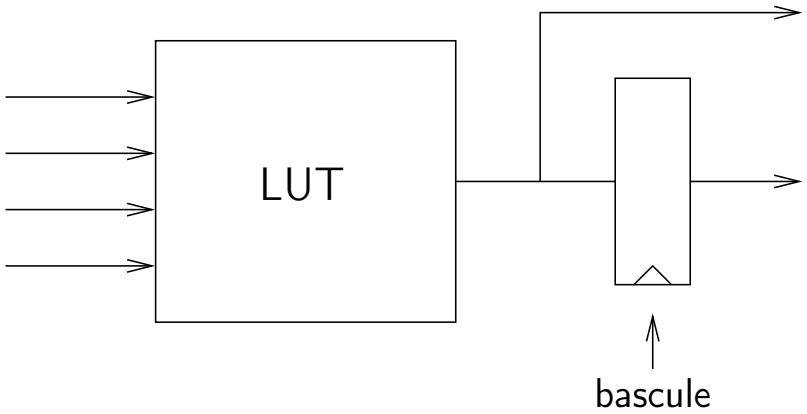
$\Rightarrow$ Générateur d'architecture

# Un générateur d'architecture *(ii/ii)*

- Générateur écrit en `Python`
- Description des architectures en `VHDL`
- Génère des tests
- Choix de l'algorithme pour chaque étage de la récursion
- Choix de la place des registres
- Outils pour l'implémentation rapide de nouveaux algorithmes :
  - Modèle du `VHDL`,
  - Représentation formelle des signaux (indépendante de la caractéristique),
  - Traduction automatique des sommes, ...

# Implémentation sur FPGA (Virtex II pro)

- $\mathbb{F}_2$ représenté par un bit
- $\mathbb{F}_3$ représenté sur deux bits (*borrow-save*)




Sur FPGA, brique de base $\longrightarrow$ LUT

- Toutes les portes à 4 entrées 1 sortie
- Même coût pour additionner 2,3 ou 4 éléments de $\mathbb{F}_2$
- Deux LUT pour sommer deux éléments de $\mathbb{F}_3$

# Performance des architectures générées en caractéristique 2

| Algorithme | $\mathbb{F}_{p^m}$ | Temps ($ns$) | Fréquence (MHz) | Surface (slices) | Produit temps-surface ($\mu s$·slices) |
|---|---|---|---|---|---|
| $\mathcal{K}_{2,239}$, $\mathcal{K}_{2,120}$, $\mathcal{K}_{2,60}$, $\mathcal{K}_{2,30}$, $\mathcal{K}_{2,15}$, Naïf | $\mathbb{F}_{2^{239}}$ | 7.477 | 134 | 9028 | 67.5 |
| $\mathcal{K}'_{2,239}$, $\mathcal{K}'_{2,120}$, $\mathcal{K}'_{2,60}$, $\mathcal{K}'_{2,30}$, $\mathcal{K}'_{2,15}$, Naïf | $\mathbb{F}_{2^{239}}$ | 7.533 | 133 | 10897 | 82.1 |
| $\mathcal{K}_{2,239}$, $\mathcal{K}_{2,120}$, $\mathcal{K}_{2,60}$, $\mathcal{K}_{2,30}$, Naïf | $\mathbb{F}_{2^{239}}$ | 6.783 | 147 | 11792 | 80.0 |
| $\mathcal{K}_{3,239}$, $\mathcal{K}_{2,80}$, $\mathcal{K}_{2,40}$, $\mathcal{K}_{2,20}$, Naïf | $\mathbb{F}_{2^{239}}$ | 6.801 | 147 | 9237 | 62.8 |
| $\mathcal{K}'_{3,239}$, $\mathcal{K}_{2,80}$, $\mathcal{K}_{2,40}$, $\mathcal{K}_{2,20}$, Naïf | $\mathbb{F}_{2^{239}}$ | 6.798 | 147 | 9218 | 62.7 |
| $\mathcal{K}_{2,313}$, $\mathcal{K}_{2,157}$, $\mathcal{K}_{2,79}$, $\mathcal{K}_{2,40}$, $\mathcal{K}_{2,20}$, Naïf | $\mathbb{F}_{2^{313}}$ | 8.143 | 123 | 13708 | 112 |
| $\mathcal{K}'_{3,313}$, $\mathcal{K}_{2,105}$, $\mathcal{K}_{2,53}$, $\mathcal{K}_{2,27}$, $\mathcal{K}_{2,14}$, Naïf | $\mathbb{F}_{2^{313}}$ | 8.882 | 113 | 14567 | 129 |

Pipeliné sur 5 étages

# Performance des architectures générées en caractéristique 3

| Algorithme | $\mathbb{F}_{p^m}$ | Temps ($ns$) | Fréquence (MHz) | Surface (slices) | Produit temps-surface ($\mu s$·slices) |
|---|---|---|---|---|---|
| $\mathcal{K}_{2,97}$, $\mathcal{K}_{2,49}$, $\mathcal{K}_{2,25}$, $\mathcal{K}_{2,13}$, $\mathcal{K}_{2,7}$, Naïf | $\mathbb{F}_{3^{97}}$ | 7.987 | 125 | 10403 | 83,1 |
| $\mathcal{K}'_{2,97}$, $\mathcal{K}'_{2,49}$, $\mathcal{K}'_{2,25}$, $\mathcal{K}'_{2,13}$, $\mathcal{K}'_{2,7}$, Naïf | $\mathbb{F}_{3^{97}}$ | 7.705 | 130 | 10316 | 79.5 |
| $\mathcal{K}'_{3,97}$, $\mathcal{K}'_{2,33}$, $\mathcal{K}'_{2,17}$, $\mathcal{K}'_{2,9}$, $\mathcal{K}'_{2,5}$, Naïf | $\mathbb{F}_{3^{97}}$ | 7.299 | 137 | 11357 | 82.9 |
| $\mathcal{K}'_{2,167}$, $\mathcal{K}'_{2,84}$, $\mathcal{K}'_{2,42}$, $\mathcal{K}'_{2,21}$, $\mathcal{K}'_{2,11}$, $\mathcal{K}'_{2,6}$, Naïf | $\mathbb{F}_{3^{167}}$ | 8.999 | 111 | 27099 | 244 |
| $\mathcal{K}'_{3,167}$, $\mathcal{K}'_{2,56}$, $\mathcal{K}'_{2,28}$, $\mathcal{K}'_{2,14}$, $\mathcal{K}'_{2,7}$, Naïf | $\mathbb{F}_{3^{167}}$ | 10.05 | 100 | 26313 | 264 |

Pipeliné sur 7 étages

# Comparaison avec d'autres multiplieurs de la littérature

| Algorithme | $\mathbb{F}_{p^m}$ | FPGA | Temps ($ns$) | Fréq. (MHz) | Surface (slices) | $A \cdot T$ ($\mu s$·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 |

Contexte

Calcul de couplage

Algorithmes de multiplication sur $\mathbb{F}_{p^m}$

Architecture et implémentation du multiplieur

Performance du coprocesseur complet

Conclusion

# Comparaison avec la littérature

| Algorithme | $\mathbb{F}_{p^m}$ | FPGA | Temps ($\mu s$) | Surface (slices) | $A \cdot T$ ($ms$·slices) |
|---|---|---|---|---|---|
| Beuchat *et al.* (2007) | $\mathbb{F}_{2^{239}}$ | `Virtex II pro` | 127 | **2736** | 347 |
| Shu *et al.* (2006) | $\mathbb{F}_{2^{239}}$ | `Virtex II pro` | 41 | 25287 | 1040 |
| **Notre approche** | $\mathbb{F}_{2^{239}}$ | `Virtex II pro` | **5.2** | 15799 | **82.2** |

# Comparaison avec la littérature

| Algorithme | $\mathbb{F}_{p^m}$ | FPGA | Temps ($\mu s$) | Surface (slices) | $A \cdot T$ ($ms$·slices) |
|---|---|---|---|---|---|
| Beuchat *et al.* (2007) | $\mathbb{F}_{2^{239}}$ | `Virtex II pro` | 127 | **2736** | 347 |
| Shu *et al.* (2006) | $\mathbb{F}_{2^{239}}$ | `Virtex II pro` | 41 | 25287 | 1040 |
| **Notre approche** | $\mathbb{F}_{2^{239}}$ | `Virtex II pro` | **5.2** | 15799 | **82.2** |
| Ronan *et al.* (2006) | $\mathbb{F}_{2^{313}}$ | `Virtex II pro` | 124 | 41078 | 5090 |
| Beuchat *et al.* (2008) | $\mathbb{F}_{2^{313}}$ | `Virtex II pro` | 213 | **3731** | 794 |
| **Notre approche** | $\mathbb{F}_{2^{313}}$ | `Virtex II pro` | **7.8** | 22356 | **174** |

# Comparaison avec la littérature

| Algorithme | $\mathbb{F}_{p^m}$ | FPGA | Temps ($\mu s$) | Surface (slices) | $A \cdot T$ ($ms$·slices) |
|---|---|---|---|---|---|
| Beuchat *et al.* (2007) | $\mathbb{F}_{2^{239}}$ | `Virtex II pro` | 127 | **2736** | 347 |
| Shu *et al.* (2006) | $\mathbb{F}_{2^{239}}$ | `Virtex II pro` | 41 | 25287 | 1040 |
| **Notre approche** | $\mathbb{F}_{2^{239}}$ | `Virtex II pro` | **5.2** | 15799 | **82.2** |
| Ronan *et al.* (2006) | $\mathbb{F}_{2^{313}}$ | `Virtex II pro` | 124 | 41078 | 5090 |
| Beuchat *et al.* (2008) | $\mathbb{F}_{2^{313}}$ | `Virtex II pro` | 213 | **3731** | 794 |
| **Notre approche** | $\mathbb{F}_{2^{313}}$ | `Virtex II pro` | **7.8** | 22356 | **174** |
| Jiang (2007) | $\mathbb{F}_{3^{97}}$ | `Virtex 4` | 21 | 74105 | 1560 |
| **Notre approche** | $\mathbb{F}_{3^{97}}$ | `Virtex 4` | **4.25** | **18360** | **78** |
| Beuchat *et al.* (2008) | $\mathbb{F}_{3^{97}}$ | `Virtex II pro` | 117 | **2711** | 317 |
| **Notre approche** | $\mathbb{F}_{3^{97}}$ | `Virtex II pro` | **8.5** | 18360 | **156** |

Contexte

Calcul de couplage

Algorithmes de multiplication sur $\mathbb{F}_{p^m}$

Architecture et implémentation du multiplieur

Performance du coprocesseur complet

Conclusion

# Conclusion *(i/ii)*

- Faire le pari de la parallélisation
- Adapter le calcul de couplage
- Étude d'algorithmes de multiplication parallèle
- Implémentation matérielle pipelinée
- Générateur de multiplieurs en caractéristiques 2 et 3

# Conclusion *(ii/ii)*

Ces travaux m'ont beaucoup apporté :

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

# Perspectives

- D'autres algorithmes de multiplication :
  - Toom-Cook
  - Formules de Montgomery
  - ...
- Étude sur des extensions plus grandes
- Arithmétique en caractéristique $p$

# Merci pour votre attention

Des Questions ?



Contexte

Calcul de couplage

Algorithmes de multiplication sur $\mathbb{F}_{p^m}$

Architecture et implémentation du multiplieur

Performance du coprocesseur complet

Conclusion

# Algorithme $\eta_T$ en caractéristique 2

**Entrée:** $P = (x_P, y_P)$, $Q = (x_Q, y_Q) \in E(\mathbb{F}_{2^m})[\ell]$.

**Sortie:** $\eta_T(P,Q)^M \in \mathbb{F}^*_{2^{4m}}$.

$x_P^{(0)} \leftarrow x_P$ ; $y_P^{(0)} \leftarrow y_P + \bar{\delta}$ ;

$x_Q^{(0)} \leftarrow x_Q$ ; $y_Q^{(0)} \leftarrow y_Q$ ;

$u^{(0)} \leftarrow x_P^{(0)} + \alpha$ ; $v^{(0)} \leftarrow x_Q^{(0)} + \alpha$ ;

$w^{(0)} \leftarrow y_P^{(0)} + y_Q^{(0)} + \beta$ ;

$g_0^{(0)} \leftarrow u^{(0)} \cdot v^{(0)} + w^{(0)}$ ;

$g_1^{(0)} \leftarrow u^{(0)} + v^{(0)} + \alpha$ ; $g_2^{(0)} \leftarrow v^{(0)} + \left(x_P^{(0)}\right)^2$ ;

$x_P^{(1)} \leftarrow \sqrt{x_P^{(0)}}$ ; $y_P^{(1)} \leftarrow \sqrt{y_P^{(0)}}$ ;

$x_Q^{(1)} \leftarrow \left(x_Q^{(0)}\right)^2$ ; $y_Q^{(1)} \leftarrow \left(y_Q^{(0)}\right)^2$ ;

$u^{(1)} \leftarrow x_P^{(1)} + \alpha$ ; $v^{(1)} \leftarrow x_Q^{(1)} + \alpha$ ;

$w^{(1)} \leftarrow y_P^{(1)} + y_Q^{(1)} + \beta$ ;

$F^{(-1)} \leftarrow \left(g_0^{(0)} + g_2^{(0)}\right) + \left(g_1^{(0)} + 1\right) s + t$ ;

**for** $i = 0$ to $\frac{m-1}{2}$ **do**

$G^{(i)} \leftarrow g_0^{(i)} + g_1^{(i)} s + t$ ;

$F^{(i)} \leftarrow F^{(i-1)} \cdot G^{(i)}$ ;

$g_0^{(i+1)} \leftarrow u^{(i+1)} \cdot v^{(i+1)} + w^{(i+1)}$ ;

$g_1^{(i+1)} \leftarrow u^{(i+1)} + v^{(i+1)} + \alpha$ ;

$x_P^{(i+2)} \leftarrow \sqrt{x_P^{(i+1)}}$ ; $y_P^{(i+2)} \leftarrow \sqrt{y_P^{(i+1)}}$ ;

$x_Q^{(i+2)} \leftarrow \left(x_Q^{(i+1)}\right)^2$ ; $y_Q^{(i+2)} \leftarrow \left(y_Q^{(i+1)}\right)^2$ ;

$u^{(i+2)} \leftarrow x_P^{(i+2)} + \alpha$ ; $v^{(i+2)} \leftarrow x_Q^{(i+2)} + \alpha$ ;

$w^{(i+2)} \leftarrow y_P^{(i+2)} + y_Q^{(i+2)} + \beta$ ;

**end for**

**Return** $\left(F^{((m-1)/2)}\right)^M$ ;

◂ Choix de l'algorithme

# Algorithme $\eta_T$ en caractéristique 3

**Entrée:** $P = (x_P, y_P)$, $Q = (x_Q, y_Q) \in E(\mathbb{F}_{3^m})[\ell]$.
**Sortie:** $\eta_T(P, Q)^M \in \mathbb{F}^*_{3^{6m}}$.

1. $x_P^{(0)} \leftarrow x_p - \nu b$ ; $y_p^{(0)} \leftarrow -\mu b y_P$ ;
2. $x_Q^{(0)} \leftarrow x_Q$ ; $y_Q^{(0)} \leftarrow -\lambda y_Q$ ;
3. $t^{(0)} \leftarrow x_P^{(0)} + x_Q^{(0)}$ ;
4. $R^{(-1)} \leftarrow \lambda y_P^{(0)} \cdot t^{(0)} - \lambda y_Q^{(0)} \sigma - \lambda y_P^{(0)}$ ;
5. **for** $i = 0$ to $(m-1)/2$ **do**
6. $\quad S^{(i)} \leftarrow -\left(t^{(i)}\right)^2 + y_P^{(i)} y_Q^{(i)} \sigma - t^{(i)} \rho - \rho^2$ ;
7. $\quad R^{(i)} \leftarrow R^{(i-1)} \cdot S^{(i)}$ ;
8. $\quad x_P^{(i+1)} \leftarrow \sqrt[3]{x_P^{(i)}}$ ; $y_P^{(i+1)} \leftarrow \sqrt[3]{y_P^{(i)}}$ ;
9. $\quad x_Q^{(i+1)} \leftarrow \left(x_Q^{(i)}\right)^3$ ; $y_Q^{(i+1)} \leftarrow \left(y_Q^{(i)}\right)^3$ ;
10. $\quad t^{(i+1)} \leftarrow x_P^{(i)} + x_Q^{(i)}$ ;
11. **end for**
12. **Return** $\left(R^{((m-1)/2)}\right)^M$ ;

◂ Choix de l'algorithme

# Algorithmes de Karatsuba-Offman

| Algorithme | Séparation | Appels récursifs | Reconstruction |
|---|---|---|---|
| $\mathcal{K}_{2,m}$ | $A \rightarrow A_L + X^{\lceil m/2 \rceil} A_H$<br>$B \rightarrow B_L + X^{\lceil m/2 \rceil} B_H$<br>$A_M \leftarrow A_H + A_L$<br>$B_M \leftarrow B_H + B_L$ | $p_H \leftarrow A_H * B_H$<br>$p_M \leftarrow A_M * B_M$<br>$p_L \leftarrow A_L * B_L$ | $S \leftarrow p_H X^{2\lceil m/2 \rceil}$<br>$+ (p_M - p_H - p_L) X^{\lceil m/2 \rceil}$<br>$+ p_L$ |
| $\mathcal{K}_{3,m}$ | $A \rightarrow A_0 + X^{\lceil m/3 \rceil} A_1 + X^{2\lceil m/3 \rceil} A_2$<br>$B \rightarrow B_0 + X^{\lceil m/3 \rceil} B_1 + X^{2\lceil m/3 \rceil} B_2$<br>$A_{S_0} \leftarrow A_1 + A_2$<br>$A_{S_1} \leftarrow A_0 + A_2$<br>$A_{S_2} \leftarrow A_1 + A_0$<br>$B_{S_0} \leftarrow B_1 + B_2$<br>$B_{S_1} \leftarrow B_0 + B_2$<br>$B_{S_2} \leftarrow B_1 + B_0$ | $p_0 \leftarrow A_0 * B_0$<br>$p_1 \leftarrow A_1 * B_1$<br>$p_2 \leftarrow A_2 * B_2$<br>$p'_0 \leftarrow A_{S_0} * B_{S_0}$<br>$p'_1 \leftarrow A_{S_1} * B_{S_1}$<br>$p'_2 \leftarrow A_{S_2} * B_{S_2}$ | $S \leftarrow p_2 X^{4\lceil m/3 \rceil}$<br>$+ (p'_0 - p_1 - p_2) X^{3\lceil m/3 \rceil}$<br>$+ (p'_1 - p_0 + p_1 - p_2) X^{2\lceil m/3 \rceil}$<br>$+ (p'_2 - p_1 - p_0) X^{\lceil m/3 \rceil}$<br>$+ p_0$ |

# Algorithmes de Karatsuba-Offman sans recouvrement

| Algorithme | Séparation | Appels récursifs | Reconstruction |
|---|---|---|---|
| $\mathcal{K}'_{2,(m)}$ | $A \rightarrow A_E(X^2) + XA_O(X^2)$<br>$B \rightarrow B_E(X^2) + XB_O(X^2)$<br>$A_M \leftarrow A_O + A_E$<br>$B_M \leftarrow B_O + B_E$ | $p_O \leftarrow A_O * B_O$<br>$p_M \leftarrow A_M * B_M$<br>$p_E \leftarrow A_E * B_E$ | $S \leftarrow (p_E + Xp_O)(X^2)$<br>$+ X(p_M - p_E - p_O)(X^2)$ |
| $\mathcal{K}'_{3,(m)}$ | $A \rightarrow A_0(X^3) + XA_1(X^3) + X^2A_2(X^3)$<br>$B \rightarrow B_0(X^3) + XB_1(X^3) + X^2B_2(X^3)$<br>$A_{S_0} \leftarrow A_1 + A_2$<br>$A_{S_1} \leftarrow A_0 + A_2$<br>$A_{S_2} \leftarrow A_1 + A_0$<br>$B_{S_0} \leftarrow B_1 + B_2$<br>$B_{S_1} \leftarrow B_0 + B_2$<br>$B_{S_2} \leftarrow B_1 + B_0$ | $p_0 \leftarrow A_0 * B_0$<br>$p_1 \leftarrow A_1 * B_1$<br>$p_2 \leftarrow A_2 * B_2$<br>$p'_0 \leftarrow A_{S_0} * B_{S_0}$<br>$p'_1 \leftarrow A_{S_1} * B_{S_1}$<br>$p'_2 \leftarrow A_{S_2} * B_{S_2}$ | $S \leftarrow (p_0 + X(p'_0 - p_1 - p_2))(X^3)$<br>$+ X(p'_2 - p_0 - p_1 + Xp_2)(X^3)$<br>$+ X^2(p_1 + p'_1 - p_2 - p_0)(X^3)$ |