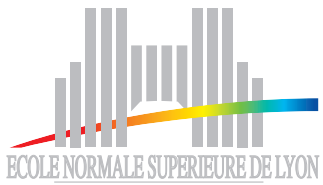
Génération automatique de circuits pour le calcul de couplages cryptographiques en matériel

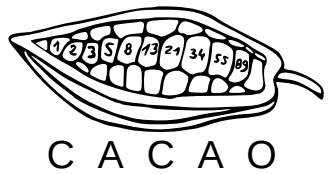
Nicolas Estibals

février – juin 2009

Encadrants :

Jérémie Detrey (Équipe-projet INRIA CACAO, LORIA, Nancy)
Jean-Luc Beuchat (LCIS, Université de Tsukuba, Japon)





Introduction

- ECC (*Elliptic Curve Cryptography*)
  - Introduite par Koblitz et Miller en 1985
  - Vs. RSA (réduction de la taille des clefs RSA-3072 $\approx$ ECC-256)
  - Recommandée et standardisée (NIST, NSA...)
- Couplages
  - Introduits en 1993 comme une attaque contre certaines courbes
  - Protocoles cryptographiques : signature numérique courte, chiffrement basé sur l'identité...
  - En cours de standardisation

Introduction

- Arithmétique spécifique
  - Arithmétique sur les courbes
  - Arithmétique sur les corps finis
- Matériel
  - Coprocesseur cryptographique
  - Matériel embarqué (carte à puce, RFID...)
- Coprocesseur arithmétique pour corps finis
- Programmation d'un coprocesseur
  - Longue, pénible, sujette à l'introduction de bugs
  - Spécifique au coprocesseur (exploration architecturale impossible)
  - Spécifique aux paramètres de la primitive cryptographique (niveau de sécurité...)
- Besoin d'un outil automatique : compilateur

Plan de l'exposé

Plan de l'exposé

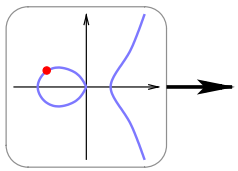
Couplage de Tate et exponentiation finale

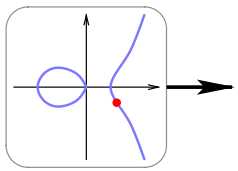
- Couplage de Tate réduit :

$$\hat{e}(P, Q)$$

  - P et Q deux points d'une courbe elliptique supersingulière sur $\mathbb{F}_{p^m}$ ($p = 2$ ou 3, $m \sim 200$)

$$E : y^2 = x^3 + Ax + B$$





Couplage de Tate et exponentiation finale

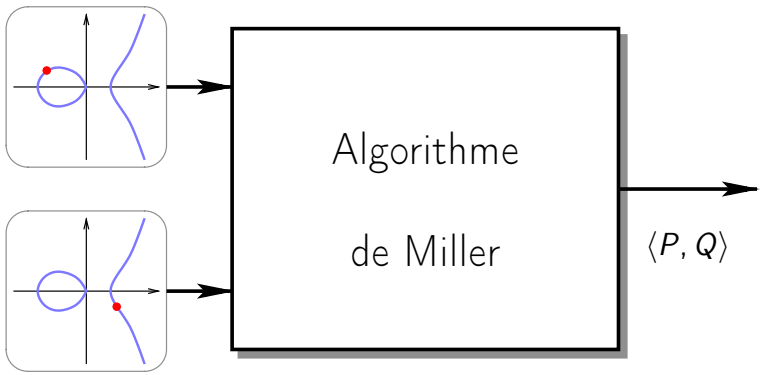
- Couplage de Tate réduit :

$$\hat{e}(P,Q) = \langle P,Q\rangle^{M}$$

  - P et Q deux points d'une courbe elliptique supersingulière sur $\mathbb{F}_{p^m}$ ($p = 2$ ou 3, $m \sim 200$)

$$E : y^2 = x^3 + Ax + B$$

  - $\langle P,Q\rangle \in \mathbb{F}^*_{p^{km}}$: couplage de Tate (non réduit)



Couplage de Tate et exponentiation finale

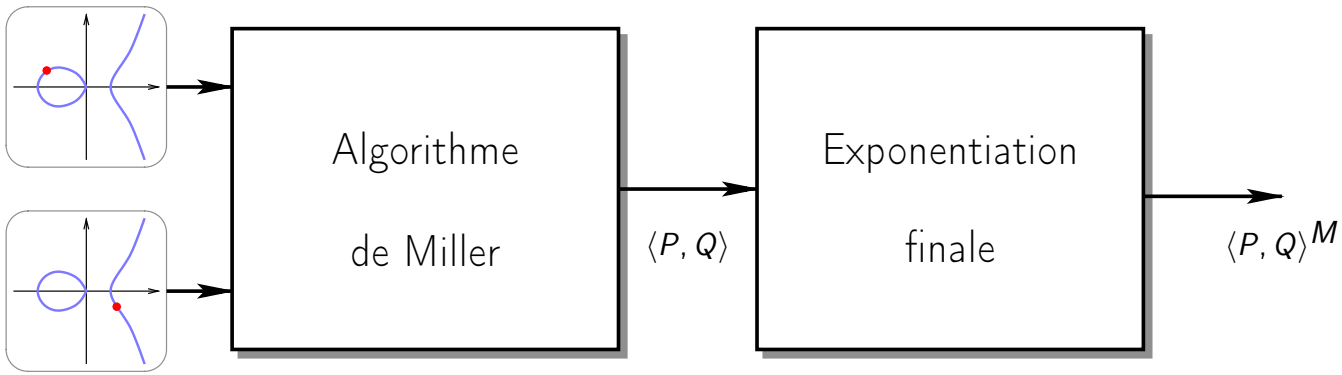
- Couplage de Tate réduit :

$$\hat{e}(P,Q) = \langle P,Q\rangle^{M}$$

  - P et Q deux points d'une courbe elliptique supersingulière sur $\mathbb{F}_{p^m}$ ($p = 2$ ou 3, $m \sim 200$)

$$E : y^2 = x^3 + Ax + B$$

  - $\langle P,Q\rangle \in \mathbb{F}^*_{p^{km}}$: couplage de Tate (non réduit)
  - $\langle P,Q\rangle^{M}$ couplage de Tate réduit



Calcul de l'exponentiation finale

- Exponentiation sur $\mathbb{F}^*_{p^{km}}$
  - Exposant :
    - $\mathbb{F}_{2^m}$: $M = (2^{2m} - 1)(2^m \pm 2^{\frac{m+1}{2}} + 1)$
    - $\mathbb{F}_{3^m}$: $M = (3^{3m} - 1)(3^m + 1)(3^m \pm 3^{\frac{m+1}{2}} + 1)$
  - Calculs sur l'extension
    - $\mathbb{F}^*_{p^{km}}$ construit par une tour d'extensions
    - Opérations sur $\mathbb{F}_{p^m}$: additions, multiplications, Frobenius ($x \mapsto x^p$)
- Algorithme d'exponentiation rapide en base p (coût linéaire en m)

Calcul de l'exponentiation finale

- Exponentiation sur $\mathbb{F}^*_{p^{km}}$
  - Exposant de forme particulière :
    - $\mathbb{F}_{2^m}$: $M = (2^{2m} - 1)(2^m \pm 2^{\frac{m+1}{2}} + 1)$
    - $\mathbb{F}_{3^m}$: $M = (3^{3m} - 1)(3^m + 1)(3^m \pm 3^{\frac{m+1}{2}} + 1)$
  - Calculs sur l'extension
    - $\mathbb{F}^*_{p^{km}}$ construit par une tour d'extensions
    - Opérations sur $\mathbb{F}_{p^m}$: additions, multiplications, Frobenius ($x \mapsto x^p$)
- Algorithme d'exponentiation rapide en base p (coût linéaire en m)
- Algorithme *ad hoc*

	Multiplications	Additions	Frobenius
$\mathbb{F}_{2^m}$	$26 + \Theta(\log_2 m)$	51 ou 53	$3m + 3$
$\mathbb{F}_{3^m}$	$73 + \Theta(\log_2 m)$	176 ou 179	$4m + 1$

Calcul de l'exponentiation finale

- Exponentiation sur $\mathbb{F}^*_{p^{km}}$
  - Exposant de forme particulière :
    - $\mathbb{F}_{2^m}$: $M = (2^{2m} - 1)(2^m \pm 2^{\frac{m+1}{2}} + 1)$
    - $\mathbb{F}_{3^m}$: $M = (3^{3m} - 1)(3^m + 1)(3^m \pm 3^{\frac{m+1}{2}} + 1)$
  - Calculs sur l'extension
    - $\mathbb{F}^*_{p^{km}}$ construit par une tour d'extensions
    - Opérations sur $\mathbb{F}_{p^m}$: additions, multiplications, Frobenius ($x \mapsto x^p$)
- Algorithme d'exponentiation rapide en base p (coût linéaire en m)
- Algorithme *ad hoc*
- Nouvel algorithme : remplacer les Frobenius par leur réciproque ($x \mapsto \sqrt[p]{x}$)

	Multiplications	Additions	Frobenius
$\mathbb{F}_{2^m}$	$26 + \Theta(\log_2 m)$	51 ou 53	$3m + 3$
$\mathbb{F}_{3^m}$	$73 + \Theta(\log_2 m)$	176 ou 179	$4m + 1$

Plan de l'exposé

Opérateurs arithmétiques

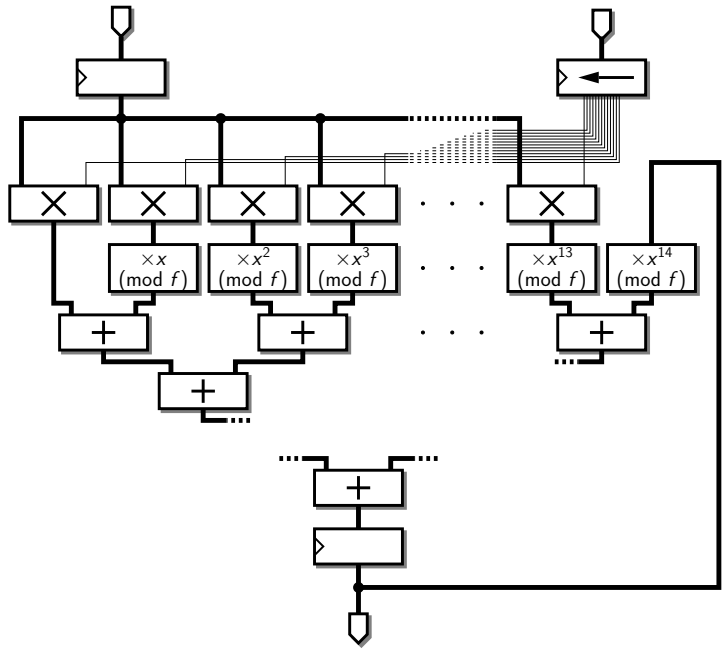
- Représentation de $\mathbb{F}_{p^m}$:
  - $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$
  - $\mathbb{F}_{p^m} \cong \mathbb{F}_p[X]/(f)$ où f polynôme irréductible de degré m
  - $\mathbb{F}_{p^m}$ représenté par les polynômes de degré $\leqslant m-1$ sur $\mathbb{F}_p$
  - m coefficients de $\mathbb{F}_p$ pour un élément de $\mathbb{F}_{p^m}$

Opérateurs arithmétiques

- Représentation de $\mathbb{F}_{p^m}$:
  - $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$
  - $\mathbb{F}_{p^m} \cong \mathbb{F}_p[X]/(f)$ où f polynôme irréductible de degré m
  - $\mathbb{F}_{p^m}$ représenté par les polynômes de degré $\leqslant m-1$ sur $\mathbb{F}_p$
  - m coefficients de $\mathbb{F}_p$ pour un élément de $\mathbb{F}_{p^m}$
- Opérations :
  - Addition : sommer coefficient à coefficient
  - Multiplication : multiplier les polynômes et réduction modulo f
  - Frobenius : combinaison linéaire des coefficients

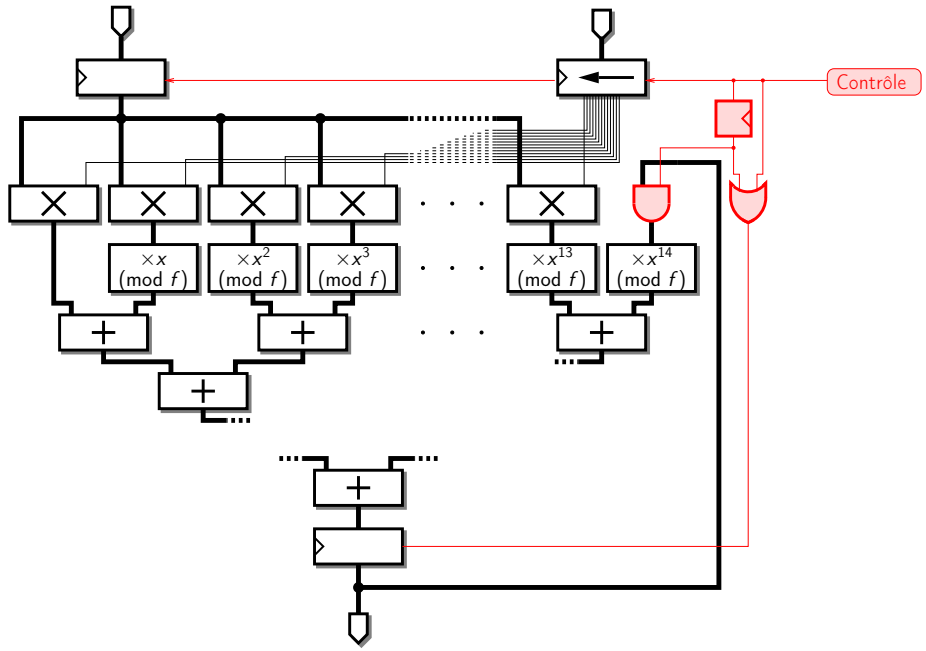
Multiplieur

- Multiplieur parallèle-série
- D coefficients par cycle d'horloge
- Une multiplication en $\lceil m/D \rceil$ cycles



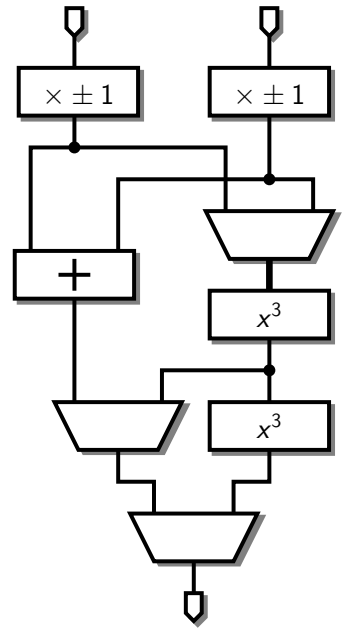
Multiplieur

- Multiplieur parallèle-série
- D coefficients par cycle d'horloge
- Une multiplication en $\lceil m/D \rceil$ cycles



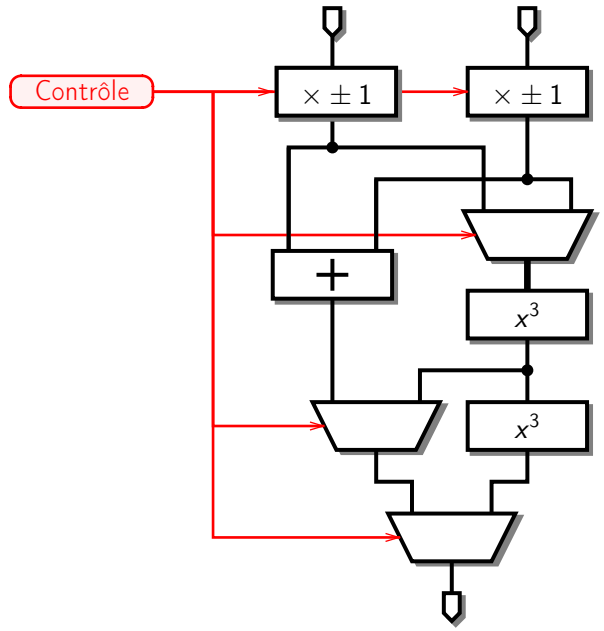
Unité de calcul polyvalente

- Unité de calcul polyvalente : combinaison de plusieurs opérateurs
- Exemple en caractéristique 3

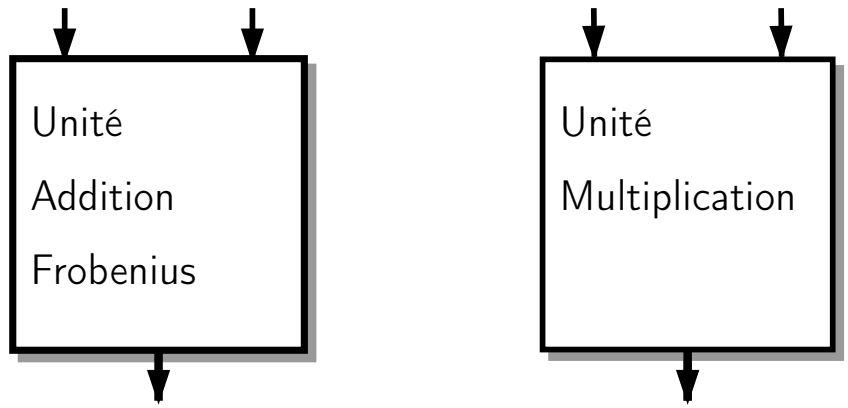


Unité de calcul polyvalente

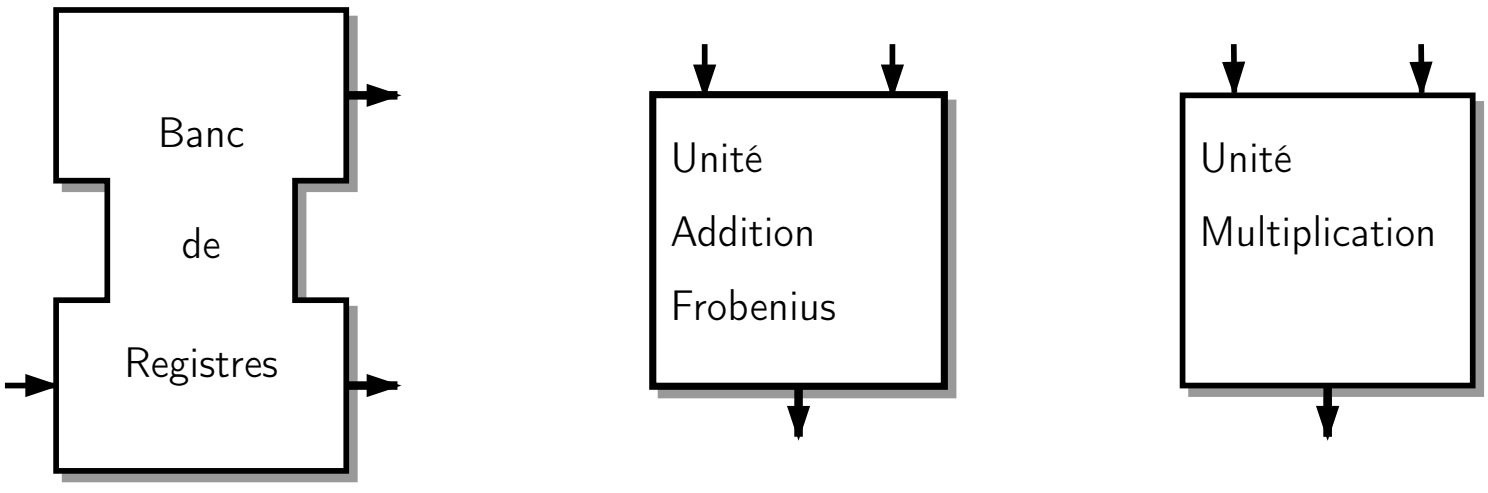
- Unité de calcul polyvalente : combinaison de plusieurs opérateurs
- Exemple en caractéristique 3
- Contrôle : choix de l'opération réalisée



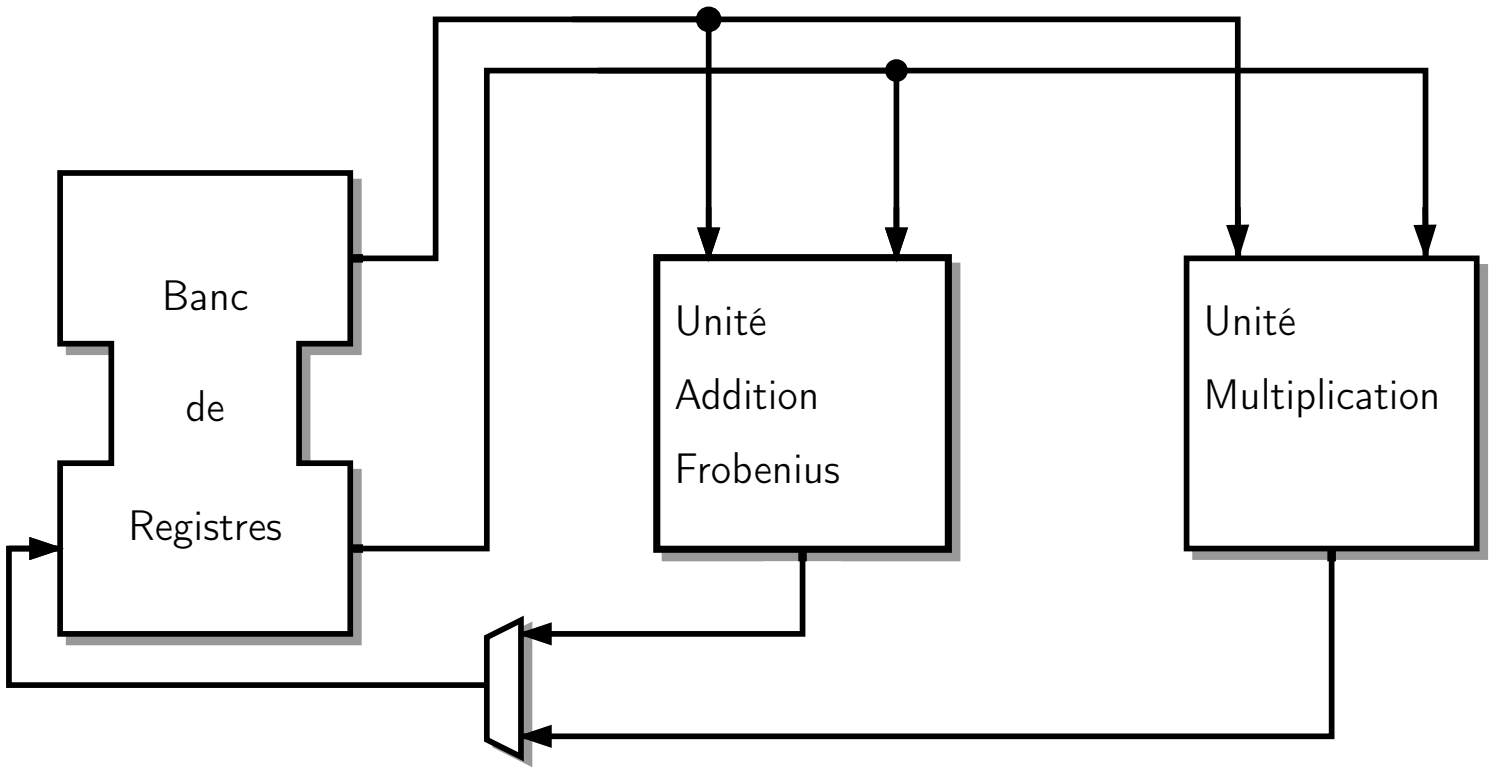
Construire un coprocesseur



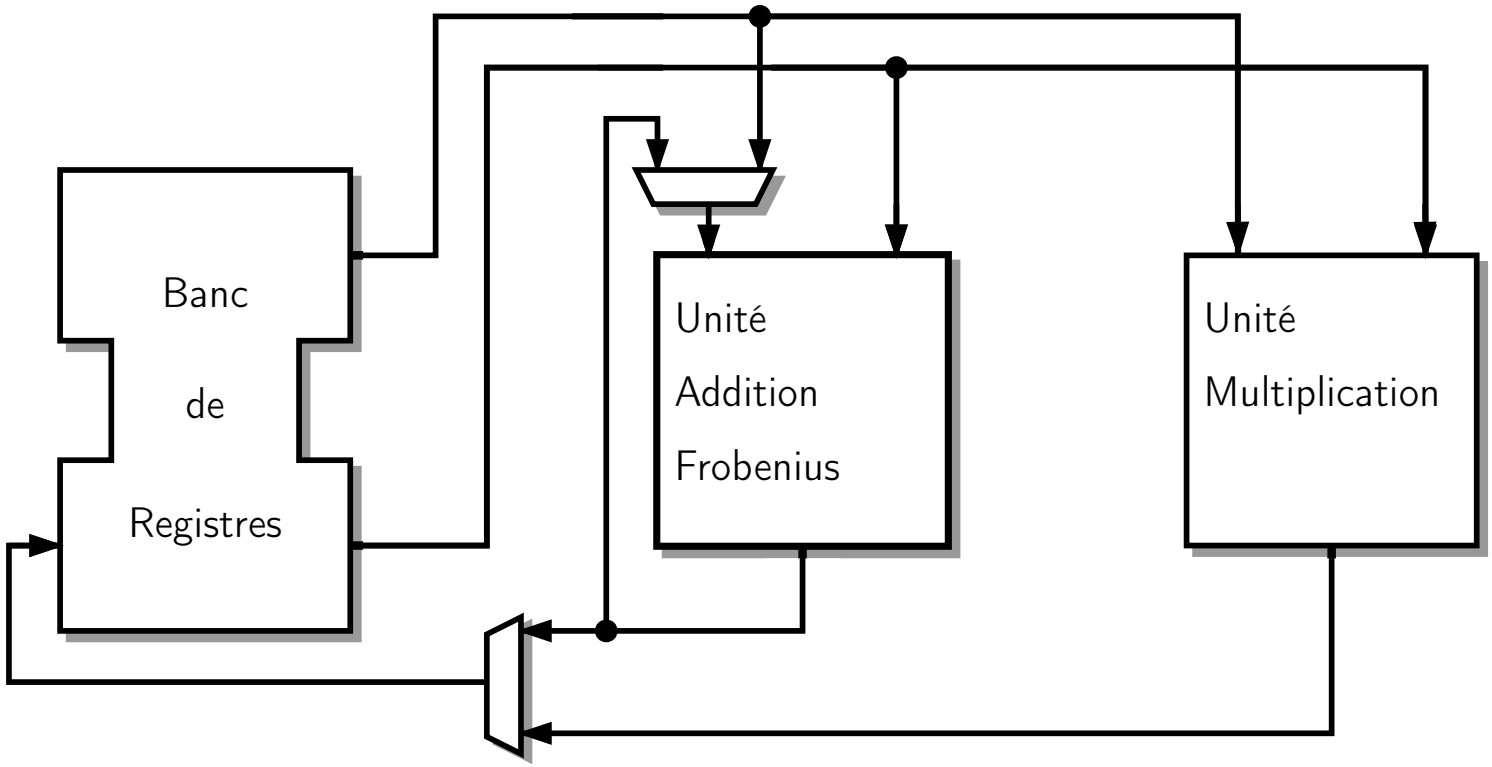
Construire un coprocesseur



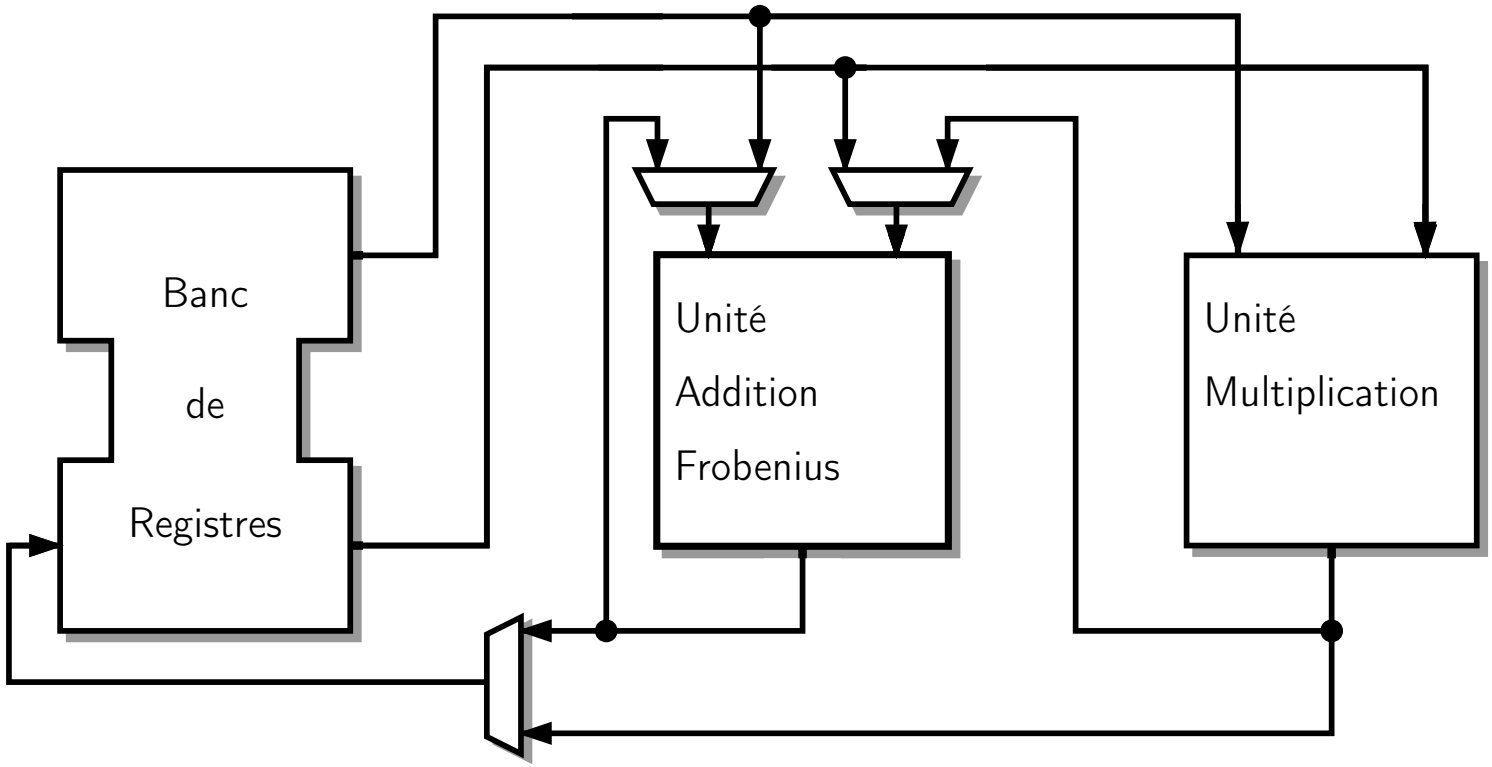
Construire un coprocesseur



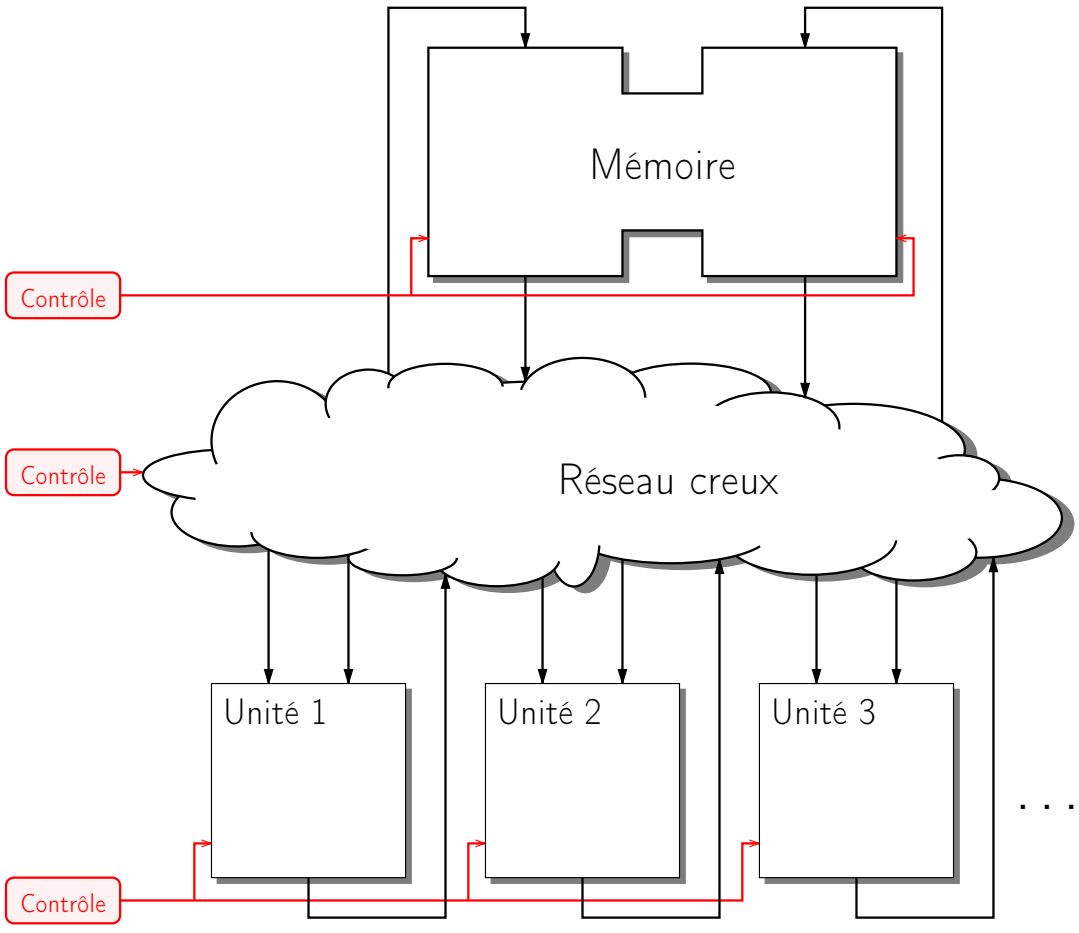
Construire un coprocesseur



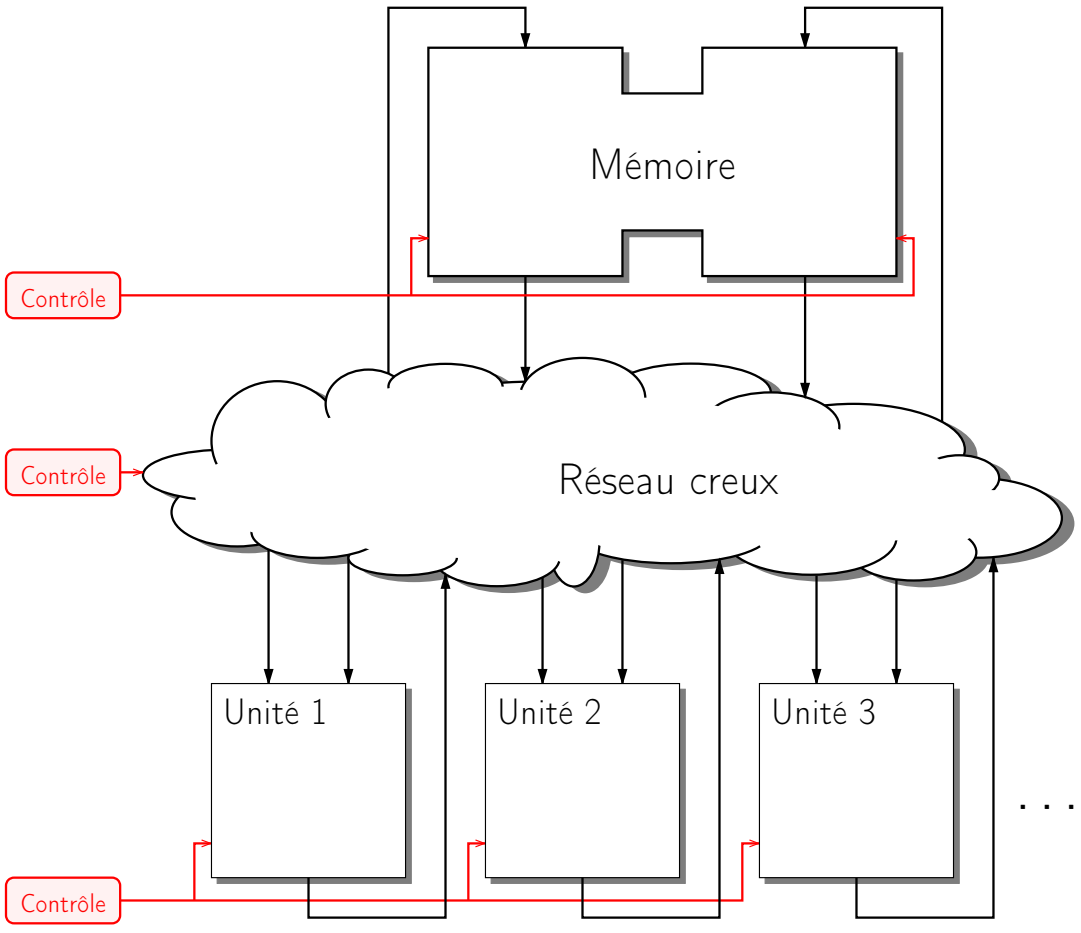
Construire un coprocesseur



Modèle de coprocesseur

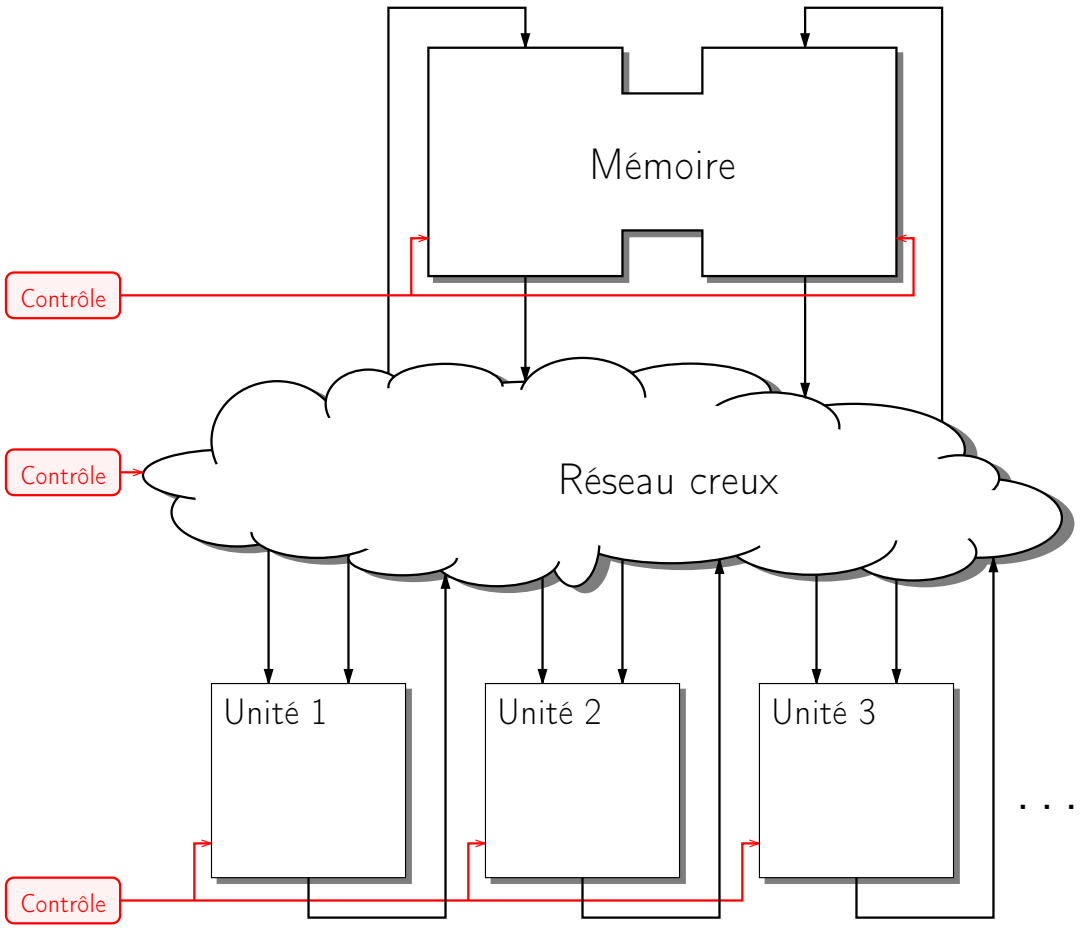


Modèle de coprocesseur



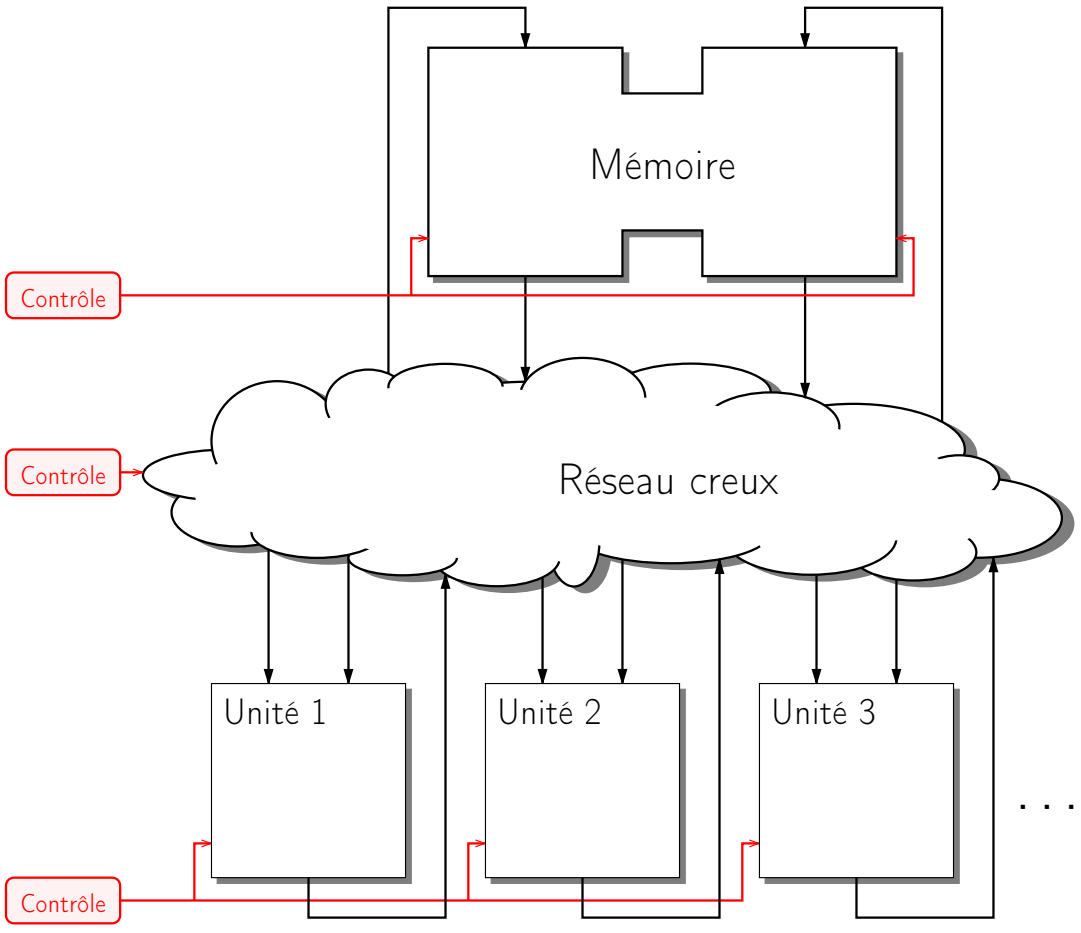
- Contrôle lu dans une mémoire morte par un petit automate

Modèle de coprocesseur



- Contrôle lu dans une mémoire morte par un petit automate
- Description formelle du coprocesseur :
  - Ensemble des fonctionnalités
  - Ensemble des liens du réseau

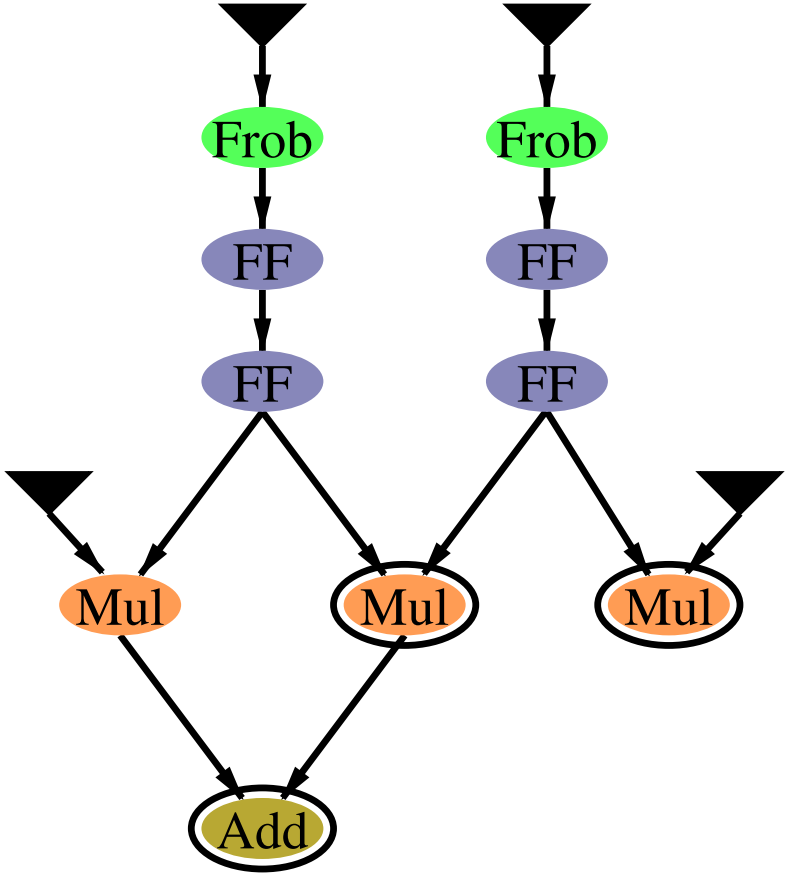
Modèle de coprocesseur



- Contrôle lu dans une mémoire morte par un petit automate
- Description formelle du coprocesseur :
  - Ensemble des fonctionnalités
  - Ensemble des liens du réseau
  - Séquences de contrôle les réalisant

Plan de l'exposé

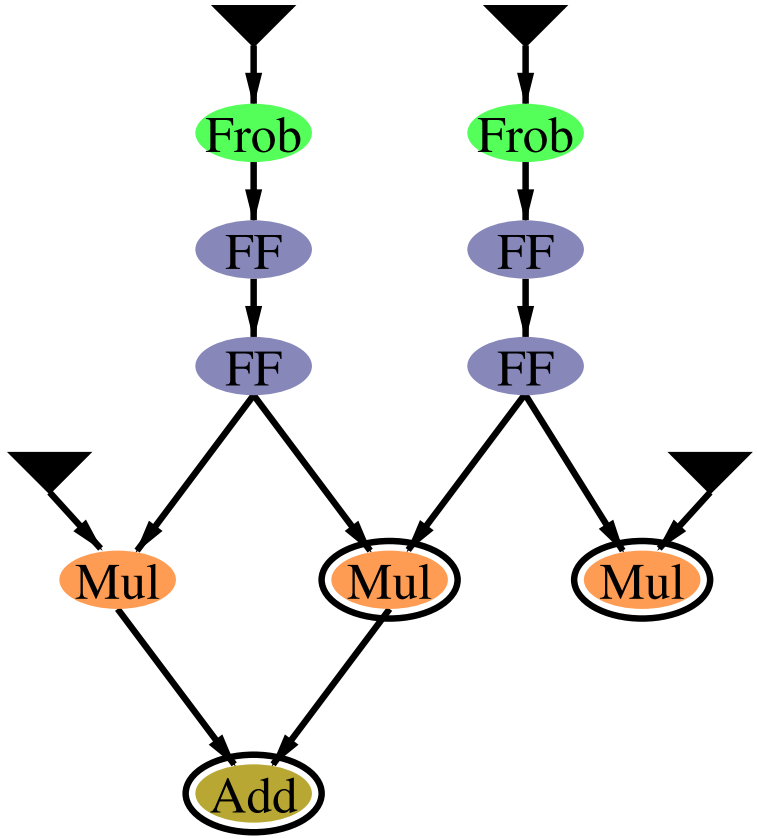
Description de l'algorithme arithmétique



- Sous forme de graphe orienté acyclique
- Un nœud par opération

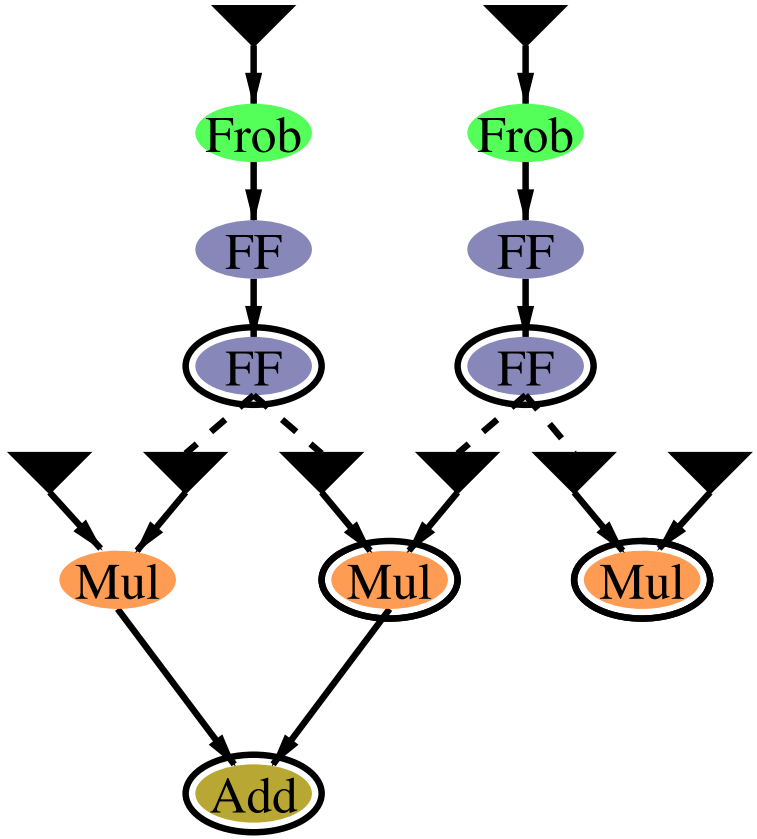
Transformations sur le graphe

- Insertion de *spills* : écriture puis lecture en mémoire



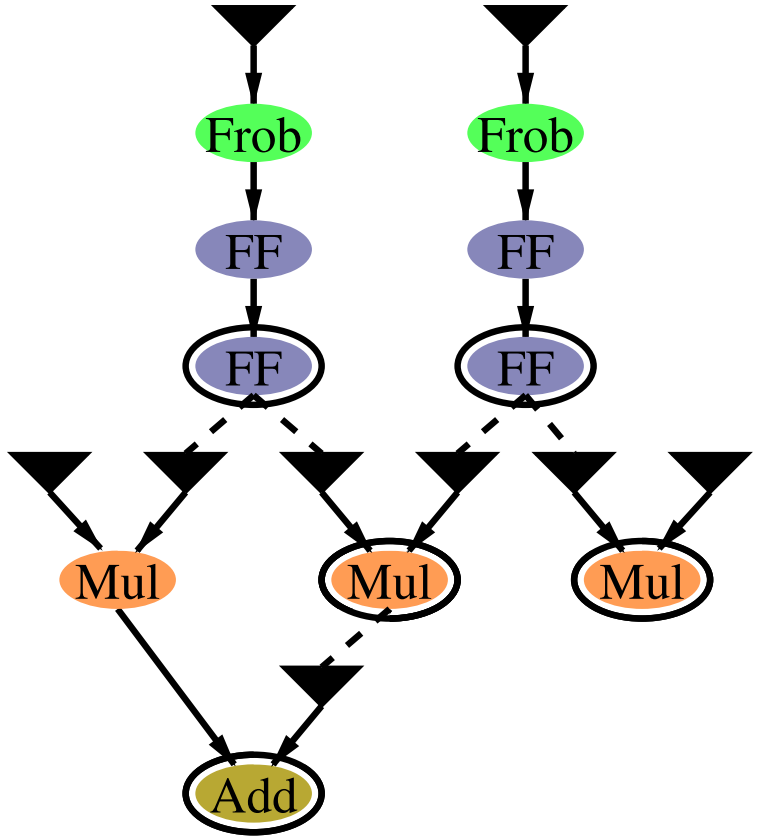
Transformations sur le graphe

- Insertion de *spills* : écriture puis lecture en mémoire
- Liens impossibles



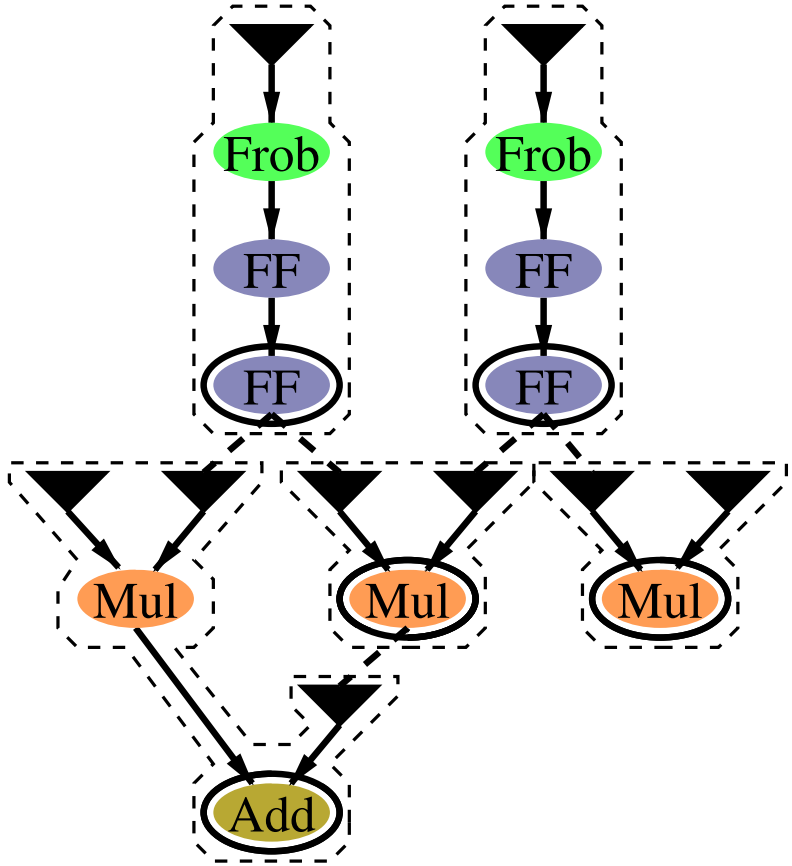
Transformations sur le graphe

- Insertion de *spills* : écriture puis lecture en mémoire
- Liens impossibles
- Collisions de ressources



Transformations sur le graphe

- Insertion de *spills* : écriture puis lecture en mémoire
- Liens impossibles
- Collisions de ressources
- ...



$\hookrightarrow$ Obtention d'un graphe de sous-arbres

Compilation

- Algorithme d'ordonnancement de listes remontant
  - Choisir un sous-arbre A prêt à ordonnancer
  - Soit t la date où il doit être réalisé
  - Essayer de placer A à la date t
    - Si OK, marquer les parents prêts à ordonnancer
    - Sinon avancer la date t et remettre A dans la liste des sous-arbres prêts à ordonnancer
  - Recommencer tant qu'il reste des sous-arbres à ordonnancer

Compilation

- Algorithme d'ordonnancement de listes remontant
  - Choisir un sous-arbre A prêt à ordonnancer
  - Soit t la date où il doit être réalisé
  - Essayer de placer A à la date t
    - Si OK, marquer les parents prêts à ordonnancer
    - Sinon avancer la date t et remettre A dans la liste des sous-arbres prêts à ordonnancer
  - Recommencer tant qu'il reste des sous-arbres à ordonnancer
- Sélection du sous-arbre :
  - Priorité sur les nœuds
  - Rapprocher ce qu'il reste à ordonnancer

Compilation

- Algorithme d'ordonnancement de listes remontant
  - Choisir un sous-arbre A prêt à ordonnancer
  - Soit t la date où il doit être réalisé
  - Essayer de placer A à la date t
    - Si OK, marquer les parents prêts à ordonnancer
    - Sinon avancer la date t et remettre A dans la liste des sous-arbres prêts à ordonnancer
  - Recommencer tant qu'il reste des sous-arbres à ordonnancer
- Sélection du sous-arbre :
  - Priorité sur les nœuds
  - Rapprocher ce qu'il reste à ordonnancer
- Allocation de registres gloutonne

Plan de l'exposé

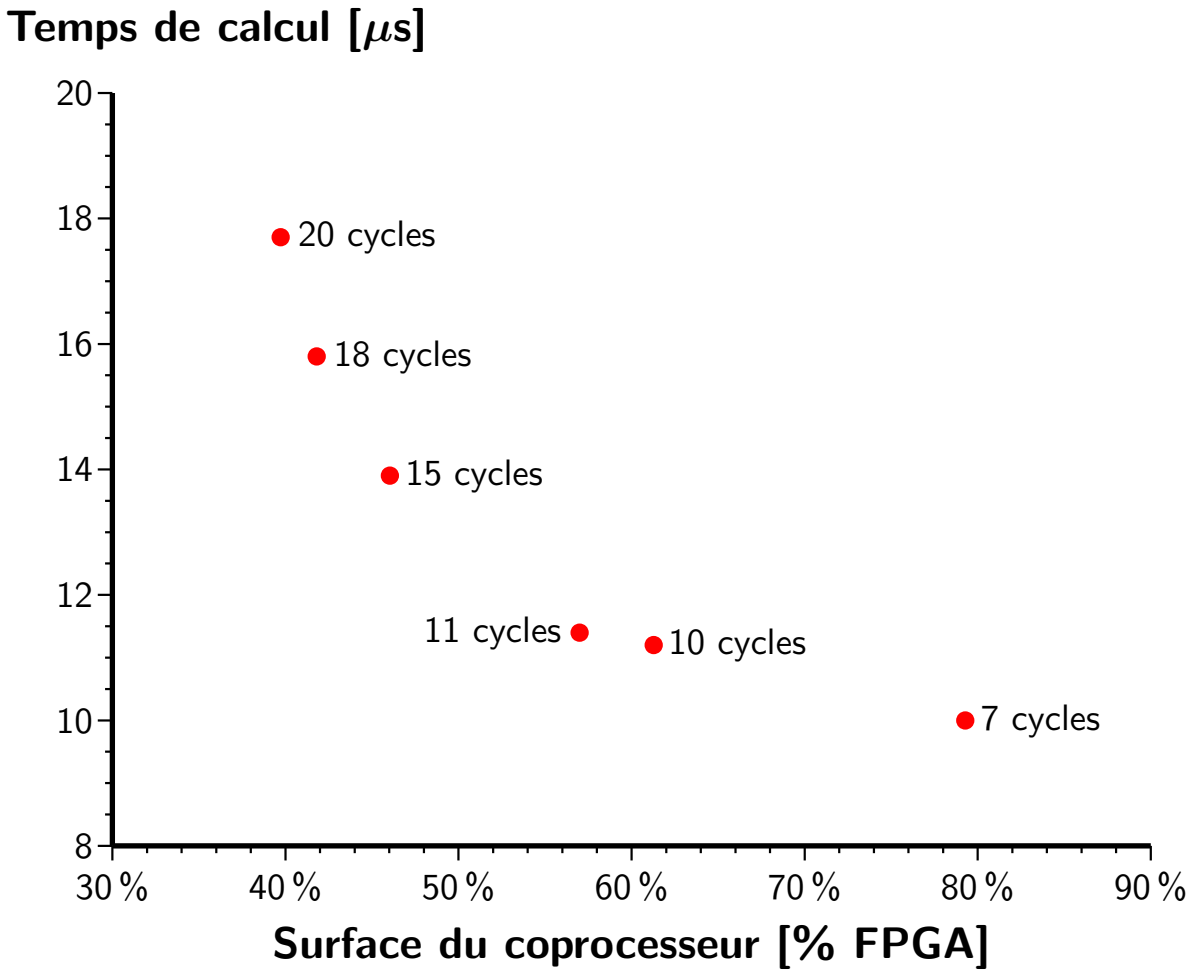
Comparaison des heuristiques

$\mathbb{F}_{p^m}$	Heuristique de compilation	Nombre de cycles	Utilisation du multiplieur
$\mathbb{F}_{3^{193}}$	Manuel	1427	86%
	Priorité	1578	79%
	Rapprochement maximum	1472	85%

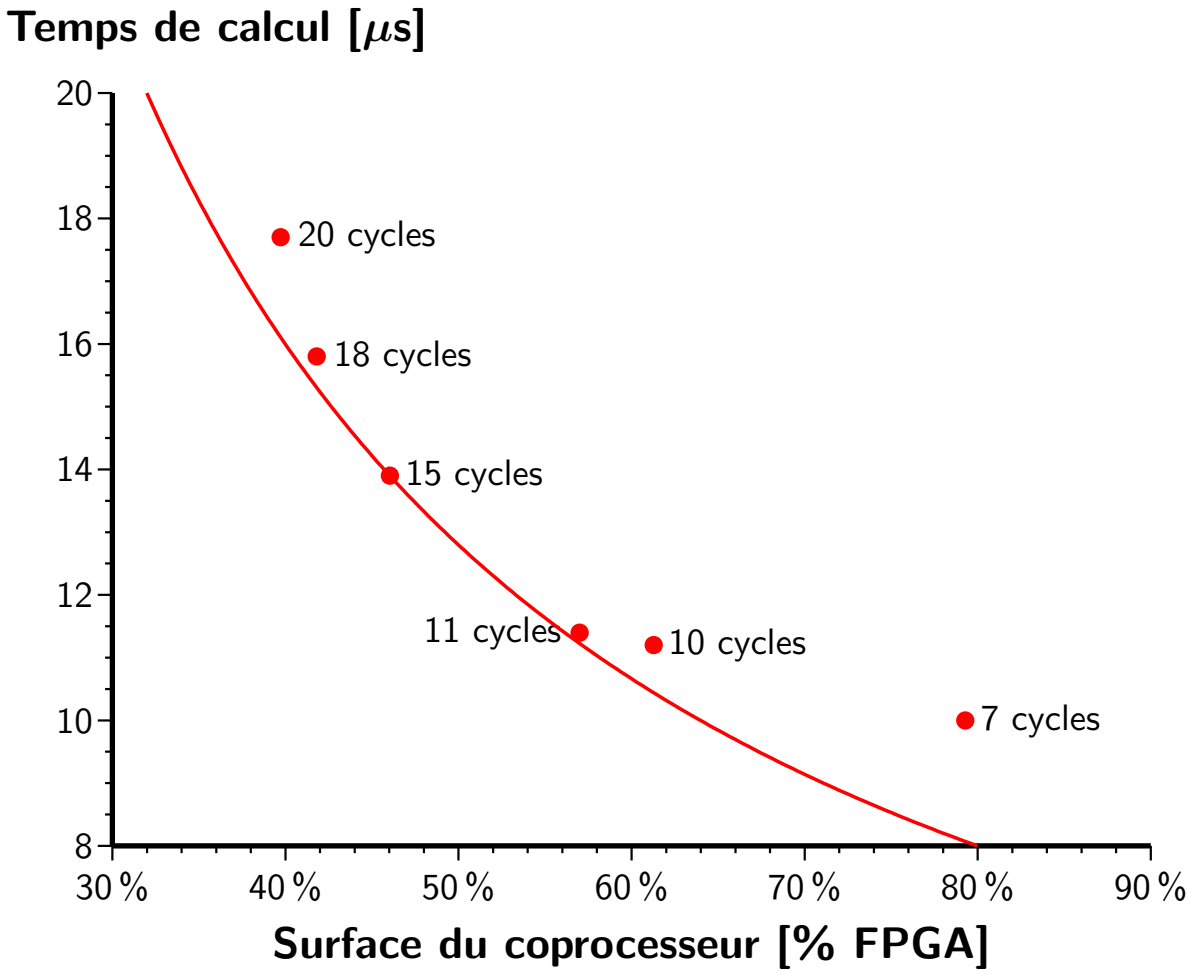
Comparaison des heuristiques

$\mathbb{F}_{p^m}$	Heuristique de compilation	Nombre de cycles	Utilisation du multiplieur
$\mathbb{F}_{3^{193}}$	Manuel	1427	86%
	Priorité	1578	79%
	Rapprochement maximum	1472	85%
$\mathbb{F}_{3^{97}}$	Manuel	654	88%
	Priorité	819	70%
	Rapprochement maximum	816	70%

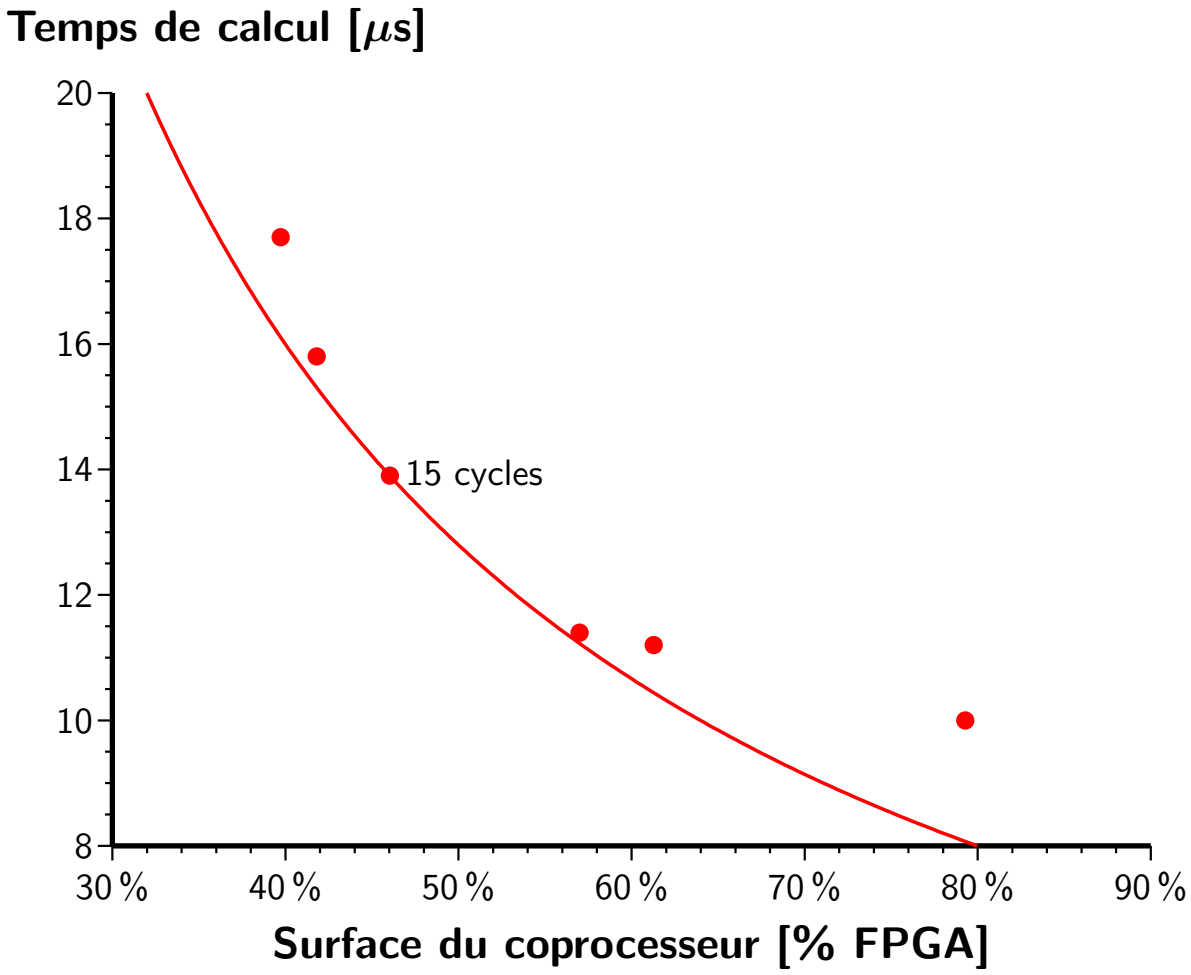
Variations architecturales



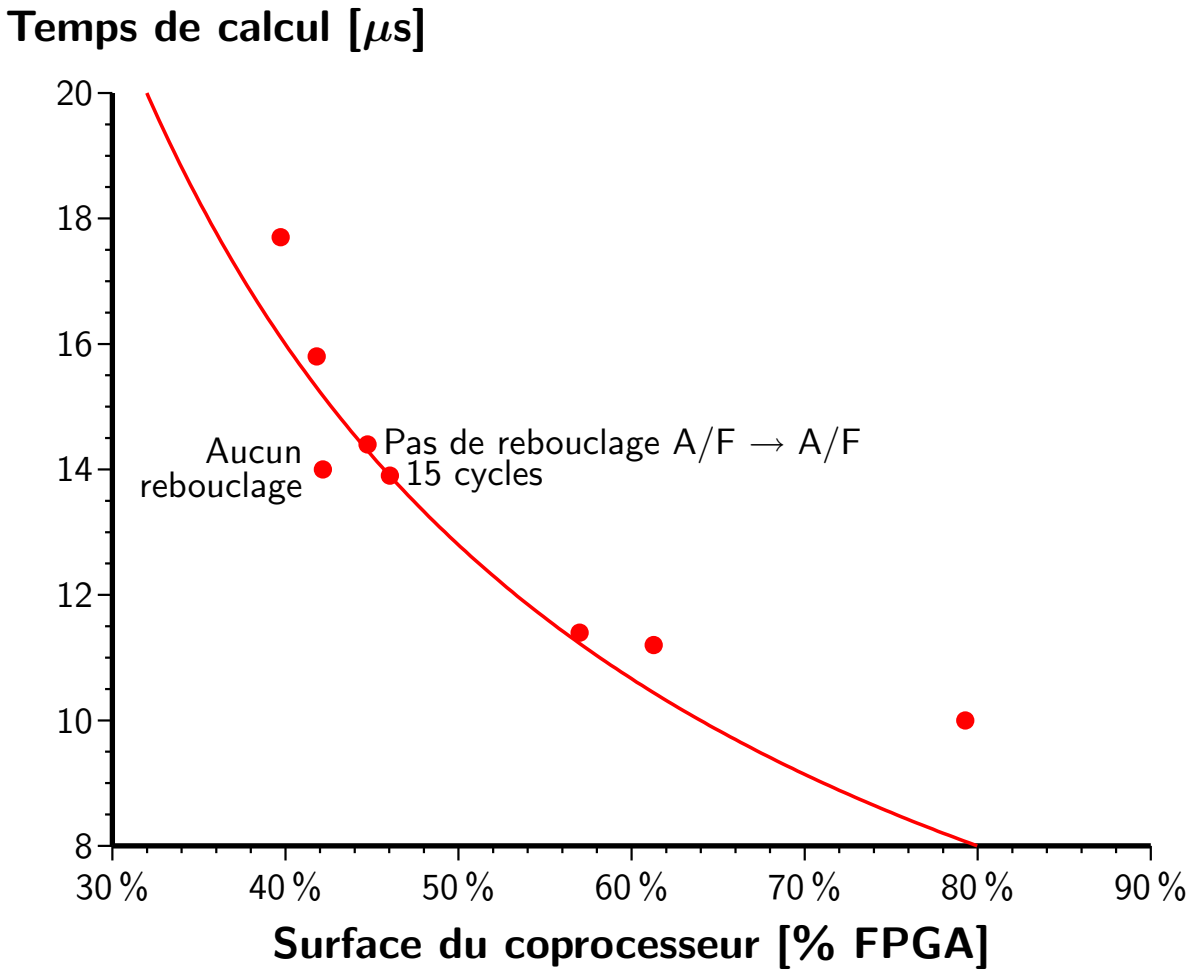
Variations architecturales



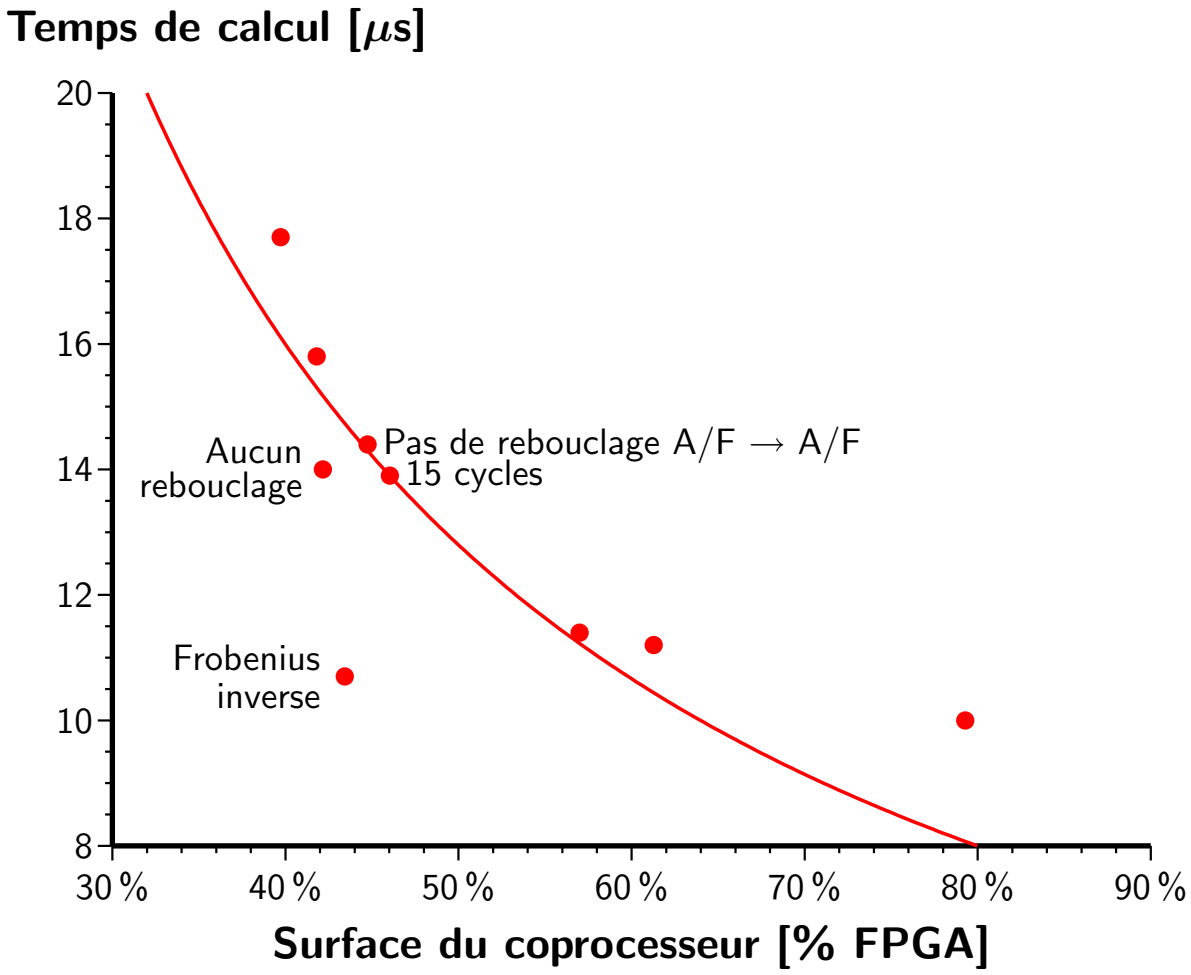
Variations architecturales



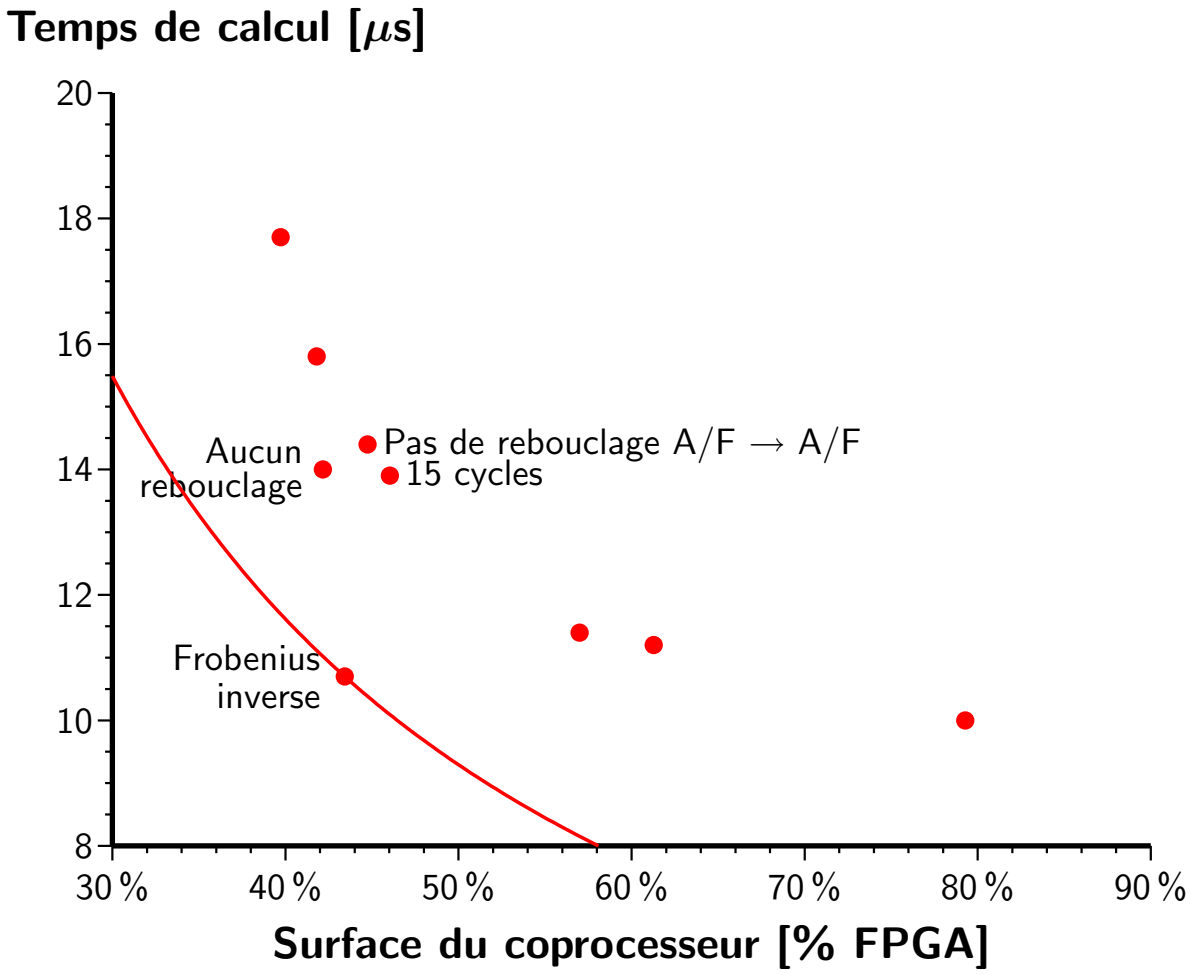
Variations architecturales



Variations architecturales



Variations architecturales



Plan de l'exposé

Conclusion

- Contributions :
  - Conception d'un modèle de coprocesseur arithmétique
  - Réalisation d'un compilateur pour cette architecture
  - Amélioration de l'algorithme d'exponentiation finale
- Perspectives :
  - D'autres heuristiques de compilation : A^*, recuit simulé, etc.
  - D'autres algorithmes :
    - Intégralité du couplage de Tate
      Travaux en cours, parmi les meilleurs compromis temps-surface de la littérature
    - Multiplication scalaire sur une courbe
    - Couplage sur courbes hyperelliptiques, etc.

Merci pour votre attention

Questions ?