Projet d'algorithmique : Méthode GLV

Gallant Lambert Vanstone

Pierre Emmanuel CLET, Pierre Augustin BERTHET

Université de Versailles

25 février 2020

Sommaire

1. Introduction
   - Notations
2. Fondement théorique
3. Algorithmes
   - Multiplications simultanées
   - Méthode GLV
4. Implémentation
   - Démarche
   - Protocoles
5. Résultats
6. Conclusion

Sommaire

1. Introduction
   - Notations
2. Fondement théorique
3. Algorithmes
4. Implémentation
5. Résultats
6. Conclusion

Introduction

On travaillera en forme de Weierstrass sur les courbes elliptiques

Notations

- On notera O le point à l'infini
- Le point P
- n l'ordre du point P
- k le multiplicateur
- p le cardinal du corps F_p

Sommaire

1 Introduction

2 Fondement théorique

3 Algorithmes

4 Implémentation

5 Résultats

6 Conclusion

Fondement théorique

Elements théoriques

- Pour tout endomorphisme ϕ dans $E(F_q)$ on a l'existence d'un λ tel que $\lambda P = \phi(P)$
- Ce λ est une racine du polynôme caractéristique de ϕ

Algorithme d'Euclide

On peut trouver k_1 et k_2 les plus petits possibles tels que $k \equiv k_1 + k_2\lambda[n]$

Lemme

Lemme

L'algorithme d'Euclide fournit les équations suivantes :

$s_i n + t_i \lambda = r_i$

Ces équations vérifient les propriétés suivantes :

- $r_i > r_{i+1} \geq 0$
- $|s_i| < |s_{i+1}|$ et $sgn(s_i) = sgn(s_{i+1})$ pour $i \geq 1$
- $|t_i| < |t_{i+1}|$ et $sgn(t_i) = sgn(t_{i+1})$
- $r_i |t_{i+1}| + r_{i+1} |t_i| = n$

Conséquences

Conséquences

Soient v_1 et v_2 tels que $v_1 = (r_{m+1}, -t_{m+1})$ et $v_2 = min((r_m, -t_m), (r_{m+2}, -t_{m+2})$. Alors il existe α et β tels que $\alpha v_1 + \beta v_2$ soit proche du vecteur (k,0).

UVSQ université PARIS-SACLAY

Sommaire

1. Introduction
2. Fondement théorique
3. Algorithmes
   - Multiplications simultanées
   - Méthode GLV
4. Implémentation
5. Résultats

Multiplications simultanées - Projet

Calculer les iP + jQ pour tous les $i, j \in [0, 2^w - 1]$
$u = (u^{d-1}, ..., u^0)$, $v = (v^{d-1}, ..., v^0)$ les décompositions en base 2^w de u et v
$R \leftarrow O$
for $i = t - 1$ down to 0 **do**
  $R \leftarrow 2^w R$
  $R \leftarrow R + (u_i P + v_i Q)$
end for
return R

Algorithm 1: $k_1 P + k_2 Q$ avec k_i sur t bits

Multiplications simultanées

$S \leftarrow P + Q$
$R \leftarrow O$
for $i = t - 1$ down to 0 **do**
  $R \leftarrow 2R$
  $R \leftarrow R + (u^i P + v^i Q)$
end for
return R

Algorithm 2: $k_1 P + k_2 Q$ avec k_i sur t bits

Méthode GLV

- Corps finis
- Opérations
- Projets
- Application
- Main

Sommaire

1 Introduction

2 Fondement théorique

3 Algorithmes

4 Implémentation
- Démarche
- Protocoles

5 Résultats

Démarche

1. Partie théorique
2. Recherche d'algorithmes dans la littérature
3. Implémentations des algorithmes (visée générale)
4. Spécialisation de ces algorithmes par rapport au projet
5. Implémentation d'exemples trouvés dans la littérature et optimisation partielle

Protocoles

1. Choix aléatoires de courbes, points et endomorphismes
2. Choix de courbes présentes dans la littérature, avec un endomorphisme simple et son λ associé

Sommaire

1 Introduction

2 Fondement théorique

3 Algorithmes

4 Implémentation

5 Résultats

6 Conclusion

Résultats

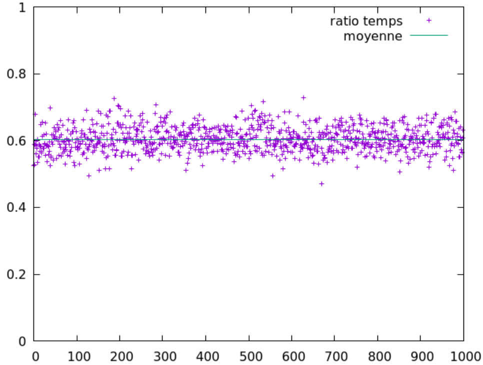

Figure – $E : y^2 = x^3 + 3$

Résultats - suite

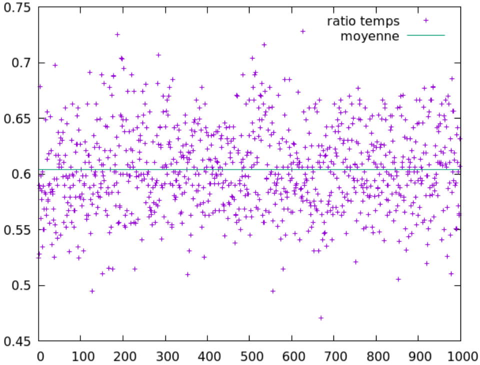

Figure – $E : y^2 = x^3 + 3$

Résultats - suite

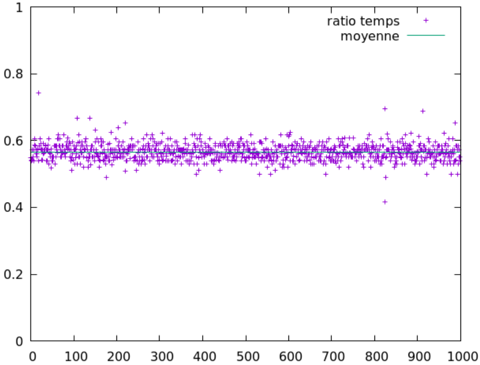

Figure – $E : y^2 = x^3 - 2$

Résultats - suite

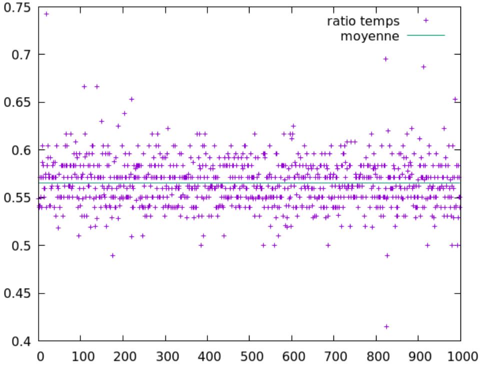

Figure – $E : y^2 = x^3 - 2$

Sommaire

1 Introduction

2 Fondement théorique

3 Algorithmes

4 Implémentation

5 Résultats

6 Conclusion

Conclusion

On a les points suivants :

- POUR : on a bien une accélération, avec une vitesse presque doublée
- CONTRE : la méthode ne s'applique pas à toutes les courbes et nécessite un travail conséquent en amont

Bibliographie

- "Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms", Gallant Lambert Vanstone
- "A Guide to Elliptic Curves Cryptography",Hankerson Menezes Vanstone, Springer
- "Courbes elliptiques", cours 2020, Krir, Université de Versailles