

UNIVERSITÉ DE VERSAILLES

PROJET D'ÉTUDE

MASTER D'ALGÈBRE APPLIQUÉE À LA CRYPTOGRAPHIE

---

# Algorithme de comptage de points de Schoof

---


*Réalisé par:*

Abdourahman SALEH IBRAHIM  
Abdessamad FAZZAT

*Supervisé par:*

Prof. Luca DE FEO

January 7, 2019

versailles.jpg

# Contents

## **Abstract**

Résumé du projet

# **1 Introduction**

Introduction aux courbes elliptiques et application à la cryptographie

## 2 Courbes elliptiques

### 2.1 Courbes elliptiques

### 2.2 Loi de groupe

### 2.3 Endomorphisme de Frobenius

### 2.4 Nombre de points

## 3 Arithmétique dans un corps fini

### 3.1 Algorithme d'Euclide

### 3.2 Algorithme d'Euclide étendu

### 3.3 Inversion modulaire

### 3.4 Exponentiation modulaire

### 3.5 Racine carrée modulaire

### 3.6 Théorème Chinois des restes

## 4 Cryptographie sur les courbes elliptiques

### 4.1 Problème du logarithme discret

## 5 Algorithme de Schoof

### 5.1 Polynômes de division

### 5.2 Points de torsion

### 5.3 Une borne sur le nombre de points: Théorème de Hasse

### 5.4 Algorithme de comptage de points de Schoof

### 5.5 Algorithme de Schoof-Elkies-Atkin

## 6 Implémentation de l'algorithme de Schoof

### 6.1 Complexité

## References

- [1] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod  $p$ . *Mathematics of computation* 44.170 (1985):483-494.
- [2] R. Crandall, C. Pomerance. *Prime numbers: a computational perspective*. Vol. 182. Springer Science Business Media, 2006. Côte 512.7 CRA. §7.5.2.
- [3] I. F. Blake, G. Seroussi, N. Smart. *Elliptic curves in cryptography*. Vol. 265. Cambridge university press, 1999. Côte 005.82 BLA. Chapitre VII.
- [4] P. Guillot: *Introduction aux courbes elliptiques pour la cryptographie*.