Université de Versailles

Projet d'étude

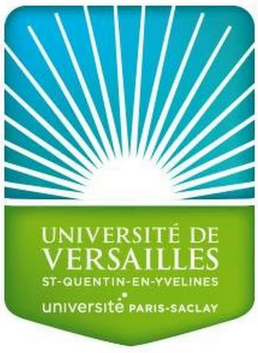
Master d'algèbre appliquée à la cryptographie

Algorithme de comptage de points de Schoof

Réalisé par:
Abdourahman Saleh Ibrahim
Abdessamad Fazzat

Supervisé par:
Prof. Luca De Feo

January 7, 2019



Contents

Abstract

Résumé du projet

1 Introduction

Introduction aux courbes elliptiques et application à la cryptographie

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.