Chudnovsky Algorithm for Multiplication in $\mathbb{F}_{3^{67}}$

Mila Tukumuli
Aix-Marseille Univ, IML[1] & ERISCS[2], 13009, Marseille, France
Email adress: mila.tukumuli@univ-amu.fr

[1] Institut de Mathématiques de Luminy, case 907, 13288 Marseille cedex 9, France
[2] Etudes et Recherche en Informatique des Systèmes Communicants Sécurisés,
Parc Scientifique de Luminy, ESIL Bâtiment A, 13009 Marseille

Keywords: : Finite fields; Multiplication algorithm; Bilinear complexity; Algebraic function field.

Abstract. A growing number of applications, such as asymmetric cryptography, make use of big integer arithmetic. In this context, it is important to conceive and develop efficient arithmetic algorithms combined with an optimal implementation method. In this work, we concentrate on multiplication algorithms over extensions of finite fields with low bilinear complexity. The so-called Chudnovsky and Chudnovsky method is an algorithm of multiplication based on interpolation on algebraic curves which allows us to:

- find upper bounds for the bilinear complexity of multiplication;
- construct effective bilinear algorithms of multiplication.

The first known effective multiplication through interpolation on algebraic curves was proposed by Shokrollahi and Baum in 1991. They used the Fermat curve $x^3+y^3=1$ to construct a multiplication algorithm over $\mathbb{F}_{4^4}$ with 8 bilinear multiplications. In 2002, Ballet proposed one over $\mathbb{F}_{16^n}$ where $n \in [13, 14, 15]$, using an hyperelliptic curve with $2n+1$ bilinear multiplications. However, these aforementioned two algorithms used rational points with multiplicity 1. Recently Cenk and Özbudak proposed a multiplication algorithm in $\mathbb{F}_{3^9}$ with 26 bilinear multiplications. This construction used the curve $y^2 = x^3 + x + 2$, with points of degree one and two, and derivative evaluations.

This work intends to clarify all the steps of construction of the Chudnovsky algorithm, particularly when the degree of the extension increases. We focus on the underlying difficulties which can arise when considering such a construction in order to make it effective. The ultimate goal is to systematize the process for finite fields used in cryptography. As a case study, we present the steps of construction of a multiplication algorithm in $\mathbb{F}_{3^{67}}$ with 282 bilinear multiplications using the elliptic curve $y^2 = x^3 + x^2 + 2$ over $\mathbb{F}_3$.