On the construction of elliptic Chudnovsky-type algorithms for multiplication in large extensions of finite fields

Stéphane Ballet, Alexis Bonnecaze, Mila Tukumuli

On the Construction of Elliptic Chudnovsky-Type Algorithms for Multiplication in Large Extensions of Finite Fields

Stéphane Ballet, Alexis Bonnecaze and Mila Tukumuli

Abstract

We indicate a strategy in order to construct bilinear multiplication algorithms of type Chudnovsky in large extensions of any finite field. In particular, using the symmetric version of the generalization of Randriambololona specialized on the elliptic curves, we show that it is possible to construct such algorithms with low bilinear complexity. More precisely, if we only consider the Chudnovsky-type algorithms of type symmetric elliptic, we show that the symmetric bilinear complexity of these algorithms is in $O(n(2q)^{\log_q^*(n)})$ where n corresponds to the extension degree, and $\log_q^*(n)$ is the iterated logarithm. Moreover, we show that the construction of such algorithms can be done in time polynomial in n. Finally, applying this method we present the effective construction, step by step, of such an algorithm of multiplication in the finite field $\mathbb{F}_{3^{57}}$.

Index Terms

Multiplication algorithm, bilinear complexity, elliptic function field, interpolation on algebraic curve, finite field.

I. Introduction

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. Accelerating basic arithmetic operations can provide efficient arithmetic algorithms and thus, can make faster a protocol which executes a lot of multiplications. This situation typically occurs when considering cryptographic protocols. In this paper, we only care about the multiplication operation. There exist numerous multiplication algorithms in the literature, examples are Karatsuba's algorithm for polynomial multiplication, Toom-Cook's algorithm for large integer multiplication, but also Strassen's algorithm for matrix multiplication. We are interested in multiplication algorithms in any extension of finite fields, in particular the focus is on the Chudnovsky-Chudnovsky method [19]. This method, based on interpolation on algebraic curves defined over a finite field allows

Aix Marseille University, CNRS IML FRE 3529, 13288 Marseille cedex 9, France. e-mail: First Name.Last Name@univ-amu.fr

us to obtain multiplication algorithms with low bilinear complexity. Our objective is to construct explicitely such multiplication algorithms for large finite extensions of finite fields. The Chudnovsky-Chudnovsky method and its variants have been extensively studied these last years through the work of Shparlinsky, Tsfasmann, Vladut [28], Baum and Shokrollahi [11], Ballet and Rolland [9], [10], Chaumine [17], Arnaud [1], Cenk-Ozbudak [16] and Cascudo, Cramer, Xing and Yang [14], and recently Randriambololona [25]. Indeed, the studies on the subject are of both theoretical and practical importance: theoretically, the bilinear complexity is linked to the tensor rank and in practice, it is related to the number of gates in an electronic circuit. However, most of the work focused on the improvement of the bounds on the bilinear complexity and the theoretical aspects of the Chudnovsky-type algorithms (in particular the underlying geometry of Riemann-Roch spaces).

A. Multiplication algorithm and tensor rank

In this article, we focus on the construction of algorithms realizing the multiplication in extensions of finite fields with a minimal number (called bilinear complexity) of two-variable multiplications (called bilinear multiplications) without considering the other operations as multiplications by a constant (called scalar multiplications). Let us first recall the notions of multiplication algorithm and associated bilinear complexity in terms of tensor rank as is done in [25].

Definition I.1. *Let K be a field, and $E_0, \dots, E_s$ be finite dimensional k-vector spaces. A non zero element $t \in E_0 \otimes \cdots \otimes E_s$ is said to be an elementary tensor, or a tensor of rank 1, if it can be written in the form $t = e_0 \otimes \cdots \otimes e_s$ for some $e_i \in E_i$. More generally, the rank of an arbitrary $t \in E_0 \otimes \cdots \otimes E_s$ is defined as the minimal length of a decomposition of t as a sum of elementary tensors.*

Definition I.2. *If*

$$\alpha \quad : \quad E_1 \times \cdots \times E_s \longrightarrow E_0$$

is an s-linear map, the s-linear complexity of α is defined as the tensor rank of the element

$$\tilde{\alpha} \in E_0 \otimes E_1^\vee \otimes \cdots \otimes E_s^\vee$$

where $E_i^\vee$ denotes the dual of E_i as vector space over K for any integer i, naturally deduced from α. In particular, the 2-linear complexity is called the bilinear complexity.

Definition I.3. *Let $\mathcal{A}$ be a finite-dimensional K-algebra. We denote by*

$$\mu(\mathcal{A}/K)$$

the bilinear complexity of the multiplication map

$$m_{\mathcal{A}} \quad : \quad \mathcal{A} \times \mathcal{A} \longrightarrow \mathcal{A}$$

considered as a K-bilinear map.

In particular, if $\mathcal{A} = \mathbb{F}_{q^n}$ and $K = \mathbb{F}_q$, we let:

$$\mu_q(n) = \mu(\mathbb{F}_{q^n}/\mathbb{F}_q).$$

More concretely, $\mu(\mathcal{A}/K)$ is the smallest integer n such that there exist linear forms $\phi_1, \ldots, \phi_n$ and $\psi_1, \ldots, \psi_n \ : \ \mathcal{A} \longrightarrow K$, and elements $w_1, \ldots, w_n \in \mathcal{A}$, such that for all $x, y \in \mathcal{A}$ one has

$$xy = \phi_1(x)\psi_1(y)w_1 + \cdots + \phi_n(x)\psi_n(y)w_n, \tag{1}$$

since such an expression is the same thing as a decomposition

$$T_M = \sum_{i=1}^{n} w_i \otimes \phi_i \otimes \psi_i \in \mathcal{A} \otimes \mathcal{A} \otimes \mathcal{A}^\vee. \tag{2}$$

for the multiplication tensor of $\mathcal{A}$.

Definition I.4. *We call multiplication algorithm of length n for $\mathcal{A}/K$ a collection of ϕ_i, ψ_i, w_i that satisfy* (1) *or equivalently a tensor decomposition*

$$T_M = \sum_{i=1}^{n} w_i \otimes \phi_i \otimes \psi_i \in \mathcal{A} \otimes \mathcal{A} \otimes \mathcal{A}^\vee$$

for the multiplication tensor of $\mathcal{A}$. Such an algorithm is said symmetric if $\phi_i = \psi_i$ for all i (this can happen only if $\mathcal{A}$ is commutative).

Hence, when $\mathcal{A}$ is commutative, it is interesting to study the minimal length of a symmetric multiplication algorithm.

Definition I.5. *If $\mathcal{A}$ is a finite-dimensional K-algebra. The symmetric bilinear complexity*

$$\mu^{sym}(\mathcal{A}/K)$$

is the minimal length of a symmetric multiplication algorithm.
In particular, if $\mathcal{A} = \mathbb{F}_{q^n}$ and $K = \mathbb{F}_q$, we let:

$$\mu_q^{sym}(n) = \mu^{sym}(\mathbb{F}_{q^n}/\mathbb{F}_q).$$

B. Known results

In their seminal papers, Winograd [33] and De Groote [21] have shown that $\mu(\mathbb{F}_{q^n}/\mathbb{F}_q) \geq 2n - 1$, with equality holding if and only if $n \leq \frac{1}{2}q + 1$. Winograd have also proved [33] that optimal multiplication algorithms realizing the lower bound belong to the class of interpolation algorithms. Later, generalizing interpolation algorithms on the projective line over $\mathbb{F}_q$ to algebraic curves of higher genus over $\mathbb{F}_q$, Chudnovsky and Chudnovsky provided a method [19] which enabled to prove the linearity [2] of the bilinear complexity of multiplication in finite extensions of a finite field. Moreover, they proposed the first known multiplication algorithm using interpolation to algebraic function fields (of one variable) over $\mathbb{F}_q$. This is the so-called Chudnovsky and Chudnovsky algorithm, also called Chudnovsky algorithm to simplify. Then, several studies focused on the qualitative improvement of this algorithm

(for example [9], [1], [16], [25]) as well as the improvements of upper bounds (for example [10], [8]) and asymptotic upper bounds (for example [28], [14]) of the bilinear complexity. However, few studies have been devoted to the effective construction of Chudnovsky-type algorithms, and in particular no work has been done when the degree of extensions reaches a cryptographic size. Indeed, the first known effective finite fields multiplication through interpolation on algebraic curves was proposed by Shokrollahi and Baum [11]. They used the Fermat curve $x^3 + y^3 = 1$ to construct multiplication algorithm over $\mathbb{F}_{4^4}$ with 8 bilinear multiplications. In [3], Ballet proposed one over $\mathbb{F}_{16^n}$ where $n \in [13, 14, 15]$, using the hyperelliptic curve $y^2+y = x^5$ with $2n+1$ bilinear multiplications. Notice that these aforementioned two algorithms only use rational points, and multiplicity equals to one. Recently Cenk and Özbudak proposed in [16] an explicit multiplication algorithm in $\mathbb{F}_{3^9}$ with 26 bilinear multiplications. To this end, they used the elliptic curve $y^2 = x^3 + x + 2$ with points of higher degree and higher multiplicity.

C. Organization of the paper and new results

In Section 2, we fix the notation and we recall the different versions of Chudnovsky-type algorithms. Then in Section 3, we present a strategy in order to construct multiplication algorithms of type Chudnovsky in arbitrary large extensions of finite fields. In particular, we show that from an elliptic curve defined over any finite field $\mathbb{F}_q$, we can exhibit a symmetric version of the generalization of Randriambololona (specialized on the elliptic curves) for any extension of $\mathbb{F}_q$ of degree n, with low bilinear complexity. More precisely, if we only consider the Chudnovsky-type algorithms of type symmetric elliptic, we show that the symmetric bilinear complexity of these algorithms is in $O(n(2q)^{\log_q^*(n)})$. Even if this asymptotic complexity is quasi-linear, it has the advantage of being derived from an infinite family of symmetric algorithms with a fixed genus equal to one. Fixing the genus to one allows us to control the complexity of the construction, meaning that for finite fields of cryptographic size, one can construct in a reasonable time such algorithms. Hence, our strategy leads to fully constructive methods. Indeed, we prove that the complexity of the construction of symmetric elliptic algorithms is in time polynomial in n. Notice that with the usual strategy based upon the construction of algorithms with growing genus, the complexity of construction is not known because it is a hard problem to explicitly construct a point with a high degree [28, Section 4, Remarks 5]. Finally in Section 4, we present new upper bounds for large extensions of $\mathbb{F}_2$ and $\mathbb{F}_3$, and we also propose the effective construction, step by step, of an algorithm of multiplication in $\mathbb{F}_{3^{57}}$.

II. Multiplication algorithms of type

We start with some elementary terminology and results of algebraic function fields. A comprehensive course of the subject can be found in [29].

A. Notation

An algebraic function field $F/\mathbb{F}_q$ of one variable over $\mathbb{F}_q$ is an extension field $F \supseteq \mathbb{F}_q$ such that F is a finite extension of $\mathbb{F}_q(x)$ for some element $x \in F$ which is transcendental over $\mathbb{F}_q$. A valuation ring of the function field $F/\mathbb{F}_q$ is a ring $\mathcal{O} \subseteq F$ such that $\mathbb{F}_q \subset \mathcal{O} \subset F$ and for any $z \in F$, either $z \in \mathcal{O}$ *or* $z^{-1} \in \mathcal{O}$. A place P of

the function field $F/\mathbb{F}_q$ is the maximal ideal of some valuation ring $\mathcal{O}$ of $F/\mathbb{F}_q$. If $\mathcal{O}$ is a valuation ring of $F/\mathbb{F}_q$ and P is its maximal ideal, then $\mathcal{O}$ is uniquely determined by P hence we denote $\mathcal{O}$ by $\mathcal{O}_P$. Every place P can be written as $P = t\mathcal{O}_P$, where t is the local parameter for P. We will denote the set of all places of $F/\mathbb{F}_q$ as $\mathbb{P}_F$. For a place P, $F_P := \mathcal{O}_P/P$ is called the residue class field of P. The map $x \to x(P)$ from F to $F_P \cup \{\infty\}$ is called the residue class map with respect to P. The degree of P is defined by $[F_P : \mathbb{F}_q] := \deg P$. The free abelian group which is generated by the places of $F/\mathbb{F}_q$ is called the divisor group of $F/\mathbb{F}_q$ and it is denoted by $\mathscr{D}_F$, so a divisor is a formal sum $D = \sum_{P\in\mathbb{P}_F} n_P P$, with $n_P \in \mathbb{Z}$ almost all $n_P = 0$, of degree $\deg(D) = \sum_{P\in\mathbb{P}_F} v_P(D).\deg P$ where v_P is a discrete valuation associated to the place P. The support of a divisor D denoted $supp\ D$ is the set of places P with $v_P(D) \neq 0$. For a function $f \in F/\mathbb{F}_q$, we denote by $(f) = \sum_{P\in\mathbb{P}_F} v_P(f).P$ the principal divisor of f. If D is a divisor then $\mathscr{L}(D) = \{f \in F \mid D + (f) \geq 0\} \cup \{0\}$ is the Riemann-Roch space which is a $\mathbb{F}_q$-vector space. The integer $\ell(D) = \dim \mathscr{L}(D)$ is called the dimension of D and $i(D) = \dim D - \deg D + g - 1$ is the index of specialty of D. We say that D is non-special if $i(D) = 0$ and special otherwise.

B. Generalization of Arnaud and Cenk-Ozbudak

A drawback of the original algorithm is that it only uses rational points. In 1999, S. Ballet and R. Rolland generalized in [9] the algorithm using places of degree 1 and 2. The best finalized version of this algorithm in this direction, is the generalization introduced by Arnaud in [1] and improved by Cenk and Özbudak in [16]. This generalization uses several coefficients in the local expansion at each place P_i. The bound for the bilinear complexity involves the complexity notion $\widehat{M_q}(u)$ introduced by Cenk and Özbudak in [16] and defined as follows:

Definition II.1. *We denote by $\widehat{M_q}(u)$ the minimum number of multiplications in $\mathbb{F}_q$ needed to obtain coefficients of the product of two arbitrary u-term polynomials modulo x^u in $\mathbb{F}_q[x]$.*

For instance, we know that for all prime powers q, we have $\widehat{M_q}(2) \leq 3$ by [15]. Now, we introduce the generalized algorithm of type Chudnovsky described in [16].

Theorem II.2. *Let*

- *q be a prime power,*
- *$F/\mathbb{F}_q$ be an algebraic function field,*
- *Q be a degree n place of $F/\mathbb{F}_q$,*
- *$\mathcal{D}$ be a divisor of $F/\mathbb{F}_q$,*
- *$\mathcal{P} = \{P_1, \ldots, P_N\}$ be a set of N places of arbitrary degree,*
- *$u_1, \ldots, u_N$ be positive integers.*

We suppose that Q and all the places in $\mathcal{P}$ are not in the support of $\mathcal{D}$ and that:

a) the map

$$Ev_Q : \begin{cases} \mathcal{L}(\mathcal{D}) & \to & \mathbb{F}_{q^n} \simeq F_Q \\ f & \longmapsto & f(Q) \end{cases}$$

is onto,

b) the map

$$Ev_{\mathcal{P}} : \left\{ \begin{array}{ccc} \mathcal{L}(2\mathcal{D}) & \longrightarrow & \left(\mathbb{F}_{q^{\deg P_1}}\right)^{u_1} \times \cdots \times \left(\mathbb{F}_{q^{\deg P_N}}\right)^{u_N} \\ f & \longmapsto & \big(\varphi_1(f), \varphi_2(f), \ldots, \varphi_N(f)\big) \end{array} \right.$$

is injective, where the application φ_i is defined by

$$\varphi_i : \left\{ \begin{array}{ccc} \mathcal{L}(2\mathcal{D}) & \longrightarrow & \left(\mathbb{F}_{q^{\deg P_i}}\right)^{u_i} \\ f & \longmapsto & \big(f(P_i), f'(P_i), \ldots, f^{(u_i-1)}(P_i)\big) \end{array} \right.$$

with $f = f(P_i) + f'(P_i)t_i + f''(P_i)t_i^2 + \cdots + f^{(k)}(P_i)t_i^k + \ldots$, the local expansion at P_i of f in $\mathcal{L}(2\mathcal{D})$, with respect to the local parameter t_i. Note that we set $f^{(0)} = f$.

Then

$$\mu_q^{sym}(n) \leq \sum_{i=1}^{N} \mu_q^{sym}(\deg P_i)\widehat{M}_{q^{\deg P_i}}(u_i).$$

C. Generalization of Randriambololona

In 2012, Randriambololona introduced in [25] a possibly asymmetric generalization of this algorithm. Furthermore, he introduced a new quantity $\mu_q(\deg P_i, u_i)$ to deal with both, the degree and the multiplicity, at the same time.

Definition II.3. *For any integers $n, l \geq 1$ we consider the $\mathbb{F}_q$-algebra of polynomials in one indeterminate with coefficients in $\mathbb{F}_{q^n}$, truncated at order l:*

$$\mathcal{A}_q(n, l) = \mathbb{F}_{q^n}[t]/(t^l)$$

of dimension

$$dim_{\mathbb{F}_q}\mathcal{A}_q(n, l) = nl,$$

and we denote by

$$\mu_q(n, l) = \mu(\mathcal{A}_q(n, l)/\mathbb{F}_q)$$

its bilinear complexity over $\mathbb{F}_q$ and by

$$\mu_q^{sym}(n, l) = \mu^{sym}(\mathcal{A}_q(n, l)/\mathbb{F}_q)$$

its symmetric bilinear complexity over $\mathbb{F}_q$.

Remark II.4. *When $l = 1$, we have $\mu_q(n, 1) = \mu_q(n)$ which corresponds to the bilinear complexity of multiplication in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$; and when $n = 1$, we have $\mu_q(1, l) = \widehat{M}_{q^{\deg P_i}}(l)$ which represents the quantity defined by Cenk and Ozbudak [16].*

We recall here the presentation of Randriambololona's generalization [25] which corresponds to the asymmetric version of Chudnovsky type algorithms. By a thickened point in the algebraic curve X defined over $\mathbb{F}_q$, we mean

any closed subscheme of X supported on a closed point (of arbitrary degree). If Q is a closed point in X, we denote by $\mathcal{I}_Q$ the sheaf of ideals defining it and for any integer $l \geq 1$, we let $Q^{[l]}$ be the closed subscheme of X defined by the sheaf of ideals $(\mathcal{I}_Q)^l$. Then $Q^{[l]}$ is the thickened point supported on Q. If D is a divisor on X, we denote by $\mathcal{L}(D) = \Gamma(X, \mathcal{O}_X(D))$ its Riemann-Roch space.

Theorem II.5. *Let $\mathcal{C}$ be a curve of genus g over $\mathbb{F}_q$, and let $n, l \geq 1$ be two integers. Suppose that $\mathcal{C}$ admits a closed point Q of degree $\deg Q = n$. Let G be an effective divisor on $\mathcal{C}$, and write*

$$G = u_1 P_1 + \cdots + u_N P_N$$

where the P_i are pairwise distinct closed points, of degree $\deg P_i = d_i$. Suppose there exist two divisors D_1, D_2 on $\mathcal{C}$ such that:

(i) The natural evaluation map

$$\mathcal{L}(D_1 + D_2) \longrightarrow \prod_{i=1}^{N} \mathcal{O}_{\mathcal{C}}(D_1 + D_2) \mid_{P_i^{[u_i]}}$$

is injective.

(ii) The natural evaluation maps

$$\mathcal{L}(D_1) \longrightarrow \mathcal{O}_{\mathcal{C}}(D_1) \mid_{Q^{[l]}} \qquad \mathcal{L}(D_2) \longrightarrow \mathcal{O}_{\mathcal{C}}(D_2) \mid_{Q^{[l]}}$$

are surjective.

Then

$$\mu_q(n, l) \leq \sum_{i=1}^{N} \mu_q(d_i, u_i).$$

In fact, we also have $\mu_q(n, l) \leq \mu(\prod_{i=1}^{N} \mathcal{A}_q(d_i, u_i)/\mathbb{F}_q)$. Moreover, if $D_1 = D_2$, all these inequalities also hold for the symmetric bilinear complexity μ_q^{sym}.

Sufficient numerical criteria for the hypotheses above to hold can be given as follows. A sufficient condition for the existence of Q of degree n on $\mathcal{C}$ is that $2g + 1 \leq q^{(n-1)/2}(q^{1/2} - 1)$, while sufficient conditions for (i) and (ii) are:

(i') The divisor $D_1 + D_2 - G$ is zero-dimensional:

$$l(D_1 + D_2 - G) = 0.$$

(ii') The divisors $D_1 - lQ$ and $D_2 - lQ$ are non-special:

$$i(D_1 - lQ) = i(D_2 - lQ) = 0.$$

More precisely, (i) and (i') are equivalent, while (ii') only implies (ii) a priori.

The improvement suggested by Randriambololona in relation with bilinear complexity leads to the following inequality

$$\mu_q(\deg P_i, u_i) \leq \mu_q(\deg P_i) \widehat{M}_{q^{\deg P_i}}(u_i),$$

where $\mu_q(\deg P_i, 1) = \mu_q(\deg P_i)$ is the bilinear complexity of multiplication in $\mathbb{F}_{q^{\deg P_i}}$ over $\mathbb{F}_q$, and $\mu_q(1, u_i) = \widehat{M}_{q^{\deg P_i}}(u_i)$ is the complexity previously defined in Definition II.1. We present in Table I the best known bounds for $\mu_q(n)$ for small values of n (cf. [23], [16], [12]).

TABLE I
BOUNDS FOR $\mu_q(n)$ AND $\widehat{M}_q(n)$ FOR $1 \leq n \leq 8$, AND $q = 2, 3$.

n	2	3	4	5	6	7	8
$\mu_2(n,1) = \mu_2(n)$	3	6	9	13	15	22	24
$\mu_3(n,1) = \mu_3(n)$	3	6	9	11	15	19	21
$\widehat{M}_q(n)$	3	5	8	11	15	19	24

III. CONSTRUCTION OF CERTAIN ALGORITHMS OF TYPE CHUDNOVSKY

A. Strategies of construction

So far, the strategy to obtain upper bounds for bilinear complexity of multiplication in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, has always been to apply algorithms of type Chudnovsky on infinite families (specially some towers) of algebraic function fields defined over a fixed finite field $\mathbb{F}_q$, with genus growing to infinity and for few fixed degrees of places. Unfortunately this strategy has a weak point since growing the genus could hugely increase the complexity of the construction. However, there exists another strategy which corresponds to using the degree of freedom that remains: the degree of places. Technically, this approach consists in fixing the genus while increasing the degree of places. This new way, implied in the generalization of Arnaud and Cenk-Ozbudak, has never been investigated and requires introducing new complexity notions.

Our purpose here is to develop this strategy in the case of elliptic function fields. The choice of algebraic curves of genus one was made for two main reasons:

1) Elliptic curves are heavily used to construct cryptographic primitives. Indeed, using the same elliptic curve for both the multiplication and the cryptographic algorithms could improve the efficiency in secure embedded systems.
2) The effective construction of such elliptic algorithms can be completed within a reasonable time. More precisely, we prove that the complexity of the construction of a symmetric elliptic bilinear multiplication algorithm in $\mathbb{F}_{q^n}$ is in time polynomial in n.

Our main tool will be a result obtained by Randriambololona in [25, Proposition 4.3] which generalizes results of Shokrollahi [27], Chaumine [17], and Cenk-Ozbudak [16].

Let $\mathcal{C}/\mathbb{F}_q$ be an elliptic curve defined over $\mathbb{F}_q$ with a chosen point P_∞. The set $\mathcal{C}(\mathbb{F}_q)$ of rational points over $\mathbb{F}_q$ admits a structure of finite abelian group with identity element P_∞ and a cardinal $N_1(\mathcal{C}(\mathbb{F}_q))$. Moreover, there is a

map $\sigma : Div(\mathcal{C}) \longrightarrow \mathcal{C}(\mathbb{F}_q)$ uniquely defined by the condition that each divisor D of degree d is linearly equivalent to the divisor $\sigma(D) + (d-1)P_\infty$. This map σ is a group morphism, it passes to linear equivalence, and induces an isomorphism of the degree 0 class group $Cl^0(\mathcal{C})$. First, let us recall the result obtained by Randriambololona in [25, Proposition 4.3]. In fact, this result is very general since it gives upper bounds on $\mu_q(n,l)$ and $\mu_q^{sym}(n,l)$, while we are interested only in $\mu_q^{sym}(n)$, so we cite only part b) c) and d) of this Proposition restricted to this special case:

Proposition III.1. *Let $\mathcal{C}$ be an elliptic curve over $\mathbb{F}_q$, n be an integer. Suppose that $\mathcal{C}$ admits a closed point Q of degree n. Let G be an effective divisor on $\mathcal{C}$, and write*

$$G = u_1 P_1 + \cdots + u_N P_N$$

where P_i are pairwise distinct closed points, of degree $\deg P_i$, so

$$\deg G = \sum_{i=1}^{N} \deg P_i . u_i .$$

Then

$$\mu_{q,\mathcal{C}}(n,1) \leq \sum_{i=1}^{N} \mu_q(\deg P_i, u_i), \tag{3}$$

provided if one of the following conditions is satisfied:

1) *$\mathcal{C}$ admits at least two points of degree one and $\deg G \geq 2n$, and either not all of these points are of 2-torsion, or $\sigma(G) \neq P_\infty$.*
2) *$\deg G \geq 2n+1$ and $\mathcal{C}$ admits at least two points of degree one, all of which are of 2-torsion.*
3) *$\mathcal{C}$ admits only one point of degree one and $\deg G \geq 2n+3$.*

Remark III.2. *In the applications we will be interested mostly in constructing multiplication algorithms for extensions of $\mathbb{F}_2$ and $\mathbb{F}_3$, so it will be useful to list all elliptic curves over these fields (up to isomorphism) and to specify which case of Proposition II.1 applies to each. In fact this could be done also for any q, and it is easy to see that the case that should apply most of the time is case 1). Indeed, it is known that the 2-torsion subgroup of an elliptic curve can only be $\{0\}$, $\mathbb{Z}/2\mathbb{Z}$, or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (in characteristic $\neq 2$), and because of the Hasse bound, as soon as $q \neq 2,3,4,5,7,9$, hence except for finitely many curves, the group of rational points is not entirely of 2-torsion, as asked in condition 1). These finitely many exceptional curves are easily found by direct enumeration:*

a) *Up to isomorphism, the only elliptic curves over $\mathbb{F}_q$ with group of points reduced to $\{0\}$ are*

$$y^2 + y + (x^3 + x + 1) = 0, \quad \textit{if} \quad q = 2,$$
$$y^2 - (x^3 + 2x + 2) = 0, \quad \textit{if} \quad q = 3,$$
$$y^2 + y + (x^3 + a) = 0, \quad \textit{if} \quad q = 4 \textit{ and } \mathbb{F}_4 = \mathbb{F}_2(a),$$

so for these curves we use case 3) of Proposition III.1.

b) Up to isomorphism, the only elliptic curves over $\mathbb{F}_q$ with group of points equal to $\mathbb{Z}/2\mathbb{Z}$ are

$$y^2+xy+x^3+x^2+1=0 \ \ \textit{if} \ \ q=2,$$
$$y^2-(x^3+2x^2+2)=0 \ \ \textit{if} \ \ q=3,$$
$$y^2+xy+(x^3+ax^2+1)=0 \ \ \textit{if} \ \ q=4 \textit{ and } \mathbb{F}_4=\mathbb{F}_2(a),$$
$$y^2-(x^3+2x)=0 \ \ \textit{if} \ \ q=5,$$

so for these curves we use 1) of Proposition III.1 if $\sigma(G)\neq P_\infty$, and we use 2) else.

c) Up to isomorphism, the only elliptic curves over $\mathbb{F}_q$ with group of points equal to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ are

$$y^2+y+2x^3+x+1=0 \ \ \textit{if} \ \ q=3,$$
$$y^2+4x^3+4x=0 \ \ \textit{if} \ \ q=5,$$
$$y^2+6x^3+1=0 \ \ \textit{if} \ \ q=7,$$
$$y^2+(x+1)y+2x^3+x^2+ax+1=0 \ \ \textit{if} \ \ q=9 \textit{ and } \mathbb{F}_9=\mathbb{F}_3(a),$$

so for these curves we use 1) of Proposition III.1 if $\sigma(G)\neq P_\infty$, and we use 2) else.

d) For all other curves, there is at least one point of degree one that is not of 2-torsion, so we can use case 1) of Proposition III.1. Particularly for $q=2$, elliptic curves are

$$y^2+y+x^3=0$$
$$y^2+y+x^3+x=0$$
$$y^2+xy+x^3+1=0,$$

and for $q=3$, we obtain

$$y^2+2x^3+2x=0$$
$$y^2+2x^3+x+2=0$$
$$y^2+2x^3+2x^2+2=0$$
$$y^2+2x^3+2x^2+1=0$$
$$y^2+2x^3+x^2+2=0.$$

Also one can easily check that these curves all admit a closed point of degree n as soon as $n\geq 7$ if $q=2$, $n\geq 4$, if $q=3$ and $n\geq 3$ if $q\geq 4$.

B. Recursive elliptic algorithms

Now we are interested in the following quantities:

Definition III.3. *For any integer n, let*

$$\mu_{q,1}^{sym}(n)$$

denote an upper bound on $\mu_q^{sym}(n)$ obtained by applying Proposition III.1, possibly recursively with various elliptic curves, and starting from the values in Table I.

Likewise, given an elliptic curve $C/\mathbb{F}_q$, let

$$\mu_{q,C}^{sym}(n)$$

denote an upper bound on $\mu_q^{sym}(n)$ obtained by applying Proposition III.1, possibly recursively but only with the curve C, and starting from the values in Table I.

Definition III.4. *The iterated logarithm of n, written $\log_q^*(n)$ defined by the following recursive function:*

$$\log_q^*(n) = \begin{cases} 0 & \text{if } n \leq 1 \\ 1 + \log_q^*(\log_q(n)) & \text{otherwise,} \end{cases}$$

corresponds to the number of times the logarithm function must be iteratively applied to n before the result is less than or equal to 1.

Theorem III.5. *Let q be a prime power and let $\mathcal{C}$ be an elliptic curve defined over $\mathbb{F}_q$. Then, for any integer n such that $n \geq 7$ if $q = 2$, $n \geq 4$ if $q = 3$ and $n \geq 3$ if $q \geq 4$, there exists a symmetric elliptic bilinear algorithm of type Theorem II.5 constructed from the curve $\mathcal{C}$ such that*

$$\mu_{q,\mathcal{C}}^{sym}(n) \ \in \ O\left(n(2q)^{\log_q^*(n)}\right).$$

Notice that $(2q)^{\log_q^*(n)}$ is a very slowly growing function, as illustrated in Table II.

TABLE II
VALUES FOR $(2q)^{\log_q^*(n)}$ FOR $q = 2$ AND $n \leq 2^{65536}$.

n	$\log^*(n)$	$(2q)^{\log_q^*(n)}$
$(1, 2]$	1	4
$(2, 4]$	2	16
$(4, 16]$	3	64
$(16, 65536]$	4	256
$(65536, 2^{65536}]$	5	1024

Proof: Without loss of generality, let C be an elliptic curve which the model does not appear in case a) and b) of Remark III.2. Let G be the divisor on C such that

$$G = u_1 P_1 + \cdots + u_N P_N.$$

Concentrating on the worst case, we can assume that

- we do not use derivative evaluation, that is $u_i = 1 \ \text{ for } \ 1 \leq i \leq N$,
- we only use places of a fixed degree, that is $\deg(P_1) = \cdots = \deg(P_N) = d_1$.

With these assumptions $G = P_1 + \cdots + P_{B_{d_1}}$, where B_{d_1} denotes the number of places of degree d_1. From Remark III.2, if C is one of the elliptic curve of case d) and $\deg(G) = d_1 B_{d_1} \geq 2n$, then

$$\mu_{q,\mathcal{C}}^{sym}(n) \leq \sum_{i=1}^{B_{d_1}} \mu_{q,\mathcal{C}}^{sym}(\deg P_i) = B_{d_1} \mu_{q,\mathcal{C}}^{sym}(d_1). \tag{4}$$

From [29, Corollary 5.2.10] applied to elliptic curves, we know that B_{d_1} verifies

$$\frac{q^{d_1}}{d_1} - 9\frac{q^{d_1/2}}{d_1} < B_{d_1} < \frac{q^{d_1}}{d_1} + 9\frac{q^{d_1/2}}{d_1}.$$

Asymptotically, $B_{d_1} \in O\left(\frac{q^{d_1}}{d_1}\right)$ and then $\deg(G) \in O(q^{d_1})$. Let d_1 be the smallest integer such that $q^{d_1} \geq 2n$, then $q^{d_1-1} < 2n$ and we have $d_1 \in O\left(\log_q(2n)\right)$. Thus

$$\mu_{q,\mathcal{C}}^{sym}(n) \in O\left(B_{d_1}\mu_{q,\mathcal{C}}^{sym}(d_1)\right)$$

and then

$$\mu_{q,\mathcal{C}}^{sym}(n) \in O\left(\frac{2nq}{d_1}\mu_{q,\mathcal{C}}^{sym}(d_1)\right).$$

Using recursively the process, we obtain

$$\mu_{q,\mathcal{C}}^{sym}(d_1) \in O\left(\frac{2d_1q}{d_2}\mu_{q,\mathcal{C}}^{sym}(d_2)\right),$$

where $d_2 \in O\left(\log_q(2d_1)\right)$. With this procedure, we have that $\mu_{q,\mathcal{C}}^{sym}(n)$ belongs to

$$O\left(\frac{2nq}{d_1}\cdot\frac{2d_1q}{d_2}\cdot\ \cdots\ \cdot\frac{2d_{k-2}q}{d_{k-1}}\cdot 2d_{k-1}q\frac{\mu_{q,\mathcal{C}}^{sym}(d_k)}{d_k}\right),$$

with $d_i \in O\left(\log_q(2d_{i-1})\right)$, for $1 \leq i \leq k$, and consequently

$$\mu_{q,\mathcal{C}}^{sym}(n) \in O\left(n(2q)^k\cdot\frac{\mu_{q,\mathcal{C}}^{sym}(d_k)}{d_k}\right).$$

Let $k = \log_q^*(2n)$, then we have

$$d_k \in O\left(\underbrace{\log_q(\log_q(\ldots(\log_q}_{k\ terms}(2n))\ldots))\right) \leq 1,$$

and thus

$$\frac{\mu_{q,\mathcal{C}}^{sym}(d_k)}{d_k} \leq 1.$$

Finally

$$\mu_{q,\mathcal{C}}^{sym}(n) \in O\left(n\cdot(2q)^{\log_q^*(n)}\right).$$

■

Corollary III.6. *For any integer n such that $n \geq 7$ if $q = 2$, $n \geq 4$ if $q = 3$ and $n \geq 3$ if $q \geq 4$, there exists a symmetric elliptic bilinear algorithm of type Theorem II.5 constructed from a curve of genus one and from an effective divisor*

$$G = u_1P_1 + \cdots + u_NP_N,$$

on this curve, where the P_i are N pairwise distinct closed points, of degree $\deg P_i = d_i$, and the u_i are strictly positive integers, such that

$$\mu_{q,1}^{sym}(n) \in O\left(n\cdot(2q)^{\log_q^*(n)}\right).$$

Proof: The proof is similar to the proof of Theorem III.5. Indeed, for a fixed genus g, the number B_d of places of degree d, as claimed in [29, Corollary 5.2.10], is such that

$$\frac{q^d}{d} - (2+7g)\frac{q^{d/2}}{d} < B_d < \frac{q^d}{d} + (2+7g)\frac{q^{d/2}}{d}.$$

Thus, for each curve of genus g, B_d is asymptotically the same. Consequently, changing the model of the elliptic curve does not change the proof, and does not change asymptotically the bilinear complexity. ■

Elliptic curves have already been used to bound the bilinear complexity of multiplication (see for example the work of Shokrollahi [27], Ballet [4], and Chaumine [17]). Recently, Couveignes and Lercier [18] proposed a multiplication algorithm for finite field extensions $\mathbb{F}_{q^n}$, using normal elliptic bases. Their multiplication tensor consists in 5 convolution products, 2 component-wise products, 1 addition and 3 subtractions. Note that convolution products can be computed at the expense of $O\left(n \log n \log |\log(n)|\right)$ operations in $\mathbb{F}_q$. Asymptotically, the tensor they produce is not competitive with ours from the point of view of bilinear complexity.

C. Complexity of the construction

Studies on bilinear complexity are well advanced, however we do not know a single polynomial construction of bilinear multiplication algorithm with linear or quasi-linear multiplicative complexity. In the case of bilinear multiplication algorithm with linear multiplicative complexity, namely the case of the usual strategy based upon the construction with growing genus, we cannot give information about the complexity of construction. Indeed, it is completely unclear how to construct explicitly points of high degree [28, Section 4, Remarks 5]. However, using the new strategy with elliptic curves, we show that we can polynomially construct symmetric elliptic bilinear multiplication algorithms with quasi-linear multiplicative complexity.

Lemma III.7. *Let E be an elliptic curve defined over $\mathbb{F}_q$ and let $F/\mathbb{F}_q$ be the associated elliptic function field. Then we can construct a degree n place of $F/\mathbb{F}_q$ in time polynomial in n.*

Proof: In order to construct a degree n place Q of the elliptic function field $F/\mathbb{F}_q$, firstly we have to construct a rational point $\mathscr{P} = (x_{\mathscr{P}}, y_{\mathscr{P}})$ of E defined over $\mathbb{F}_{q^n}$ and then, we need to apply to the point $\mathscr{P}$, n-times the Frobenius map φ defined by

$$\begin{array}{rccc} \varphi: & E(\overline{\mathbb{F}}_{q^n}) & \longrightarrow & E(\overline{\mathbb{F}}_{q^n}) \\ & (x,y) & \longmapsto & (x^q, y^q). \end{array}$$

Thus the orbit of $\mathscr{P}$ obtained under the action of φ is a degree n place. In 2006, Shallue and Van De Woestijne [26] gave a deterministic polynomial-time algorithm that computes a nontrivial rational point given a Weierstrass equation for the elliptic curve. More precisely, they performed the computation of a nontrivial rational point on an elliptic curve E defined over $\mathbb{F}_q$ in time polynomial in $\log(q)$. It follows that $\mathscr{P}$ can be constructed in time polynomial in $\log(q^n)$, and thus in time polynomial in n since q is fixed. The action of the Frobenius map φ on the point $\mathscr{P}$ is simply a modular exponentiation that can be done polynomially. Consequently, constructing a degree n place of an elliptic function field can be done in time polynomial in n. ■

Theorem III.8. *Given an elliptic curve E defined over $\mathbb{F}_q$, one can polynomially construct a sequence $\mathscr{A}_{q,n}$ of symmetric elliptic bilinear multiplication algorithms in finite fields $\mathbb{F}_{q^n}$ for the given sequence $n \to +\infty$ such that*

$$\mu_{q,E}^{sym}(\mathscr{A}_{q,n}) \ \in \ O\left(n(2q/K)^{\log_q^*(n)}\right),$$

where $K = 2/3$ if the characteristic of $\mathbb{F}_q$ is 2 or 3, and $K = 5/8$ otherwise.

Proof: Let $F/\mathbb{F}_q$ be the elliptic function field associated to the curve E. According to the proof of Theorem III.5, to construct a symmetric elliptic multiplication algorithm in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, we first have to construct places and divisor of certain degree. Indeed, we need to construct

- a place Q of degree n of $F/\mathbb{F}_q$,
- a divisor D of degree n of $F/\mathbb{F}_q$,
- a sufficient number N of degree d places of $F/\mathbb{F}_q$, such that the degree of the divisor G formed by these N places, is greater or equal to $2n$.

The divisor D and the place Q are equivalent in terms of construction (in practice we can take any place to construct a divisor [3]), so their complexities of construction are similar and from Lemma III.7 this complexity is in time polynomial in n. The point now is to construct sufficiently places of degree d of $F/\mathbb{F}_q$. To achieve this, from lemma III.7 it suffices to construct rational points of the curve E over $\mathbb{F}_{q^d}$. Icart [22] shows that it is possible to construct deterministically, a constant proportion K of the number of rational points of an elliptic curve defined over $\mathbb{F}_q$. More precisely, his method allows us to construct $K = 5/8$ of the number of rational points in time polynomial in $\log^3(q)$. Note that if the characteristic of $\mathbb{F}_q$ is 2 or 3, Farashi et al. [20] proved that $K = 2/3$. This implies that asymptotically, we can construct in time polynomial in $\log^3(q^d)$, a sufficient number of places of degree d of $F/\mathbb{F}_q$ by choosing d such that $q^d \geq 2n/K$. Finally, the complexity of construction of places of degree d is polynomial in $\log^3(n)$, thus polynomial in n. In conclusion, we can polynomially construct symmetric elliptic bilinear multiplication algorithms since for a given divisor D, construct vector spaces $\mathscr{L}(D),\ \mathscr{L}(2D)$, associated basis $\mathscr{B}_D,\ \mathscr{B}_{2D}$ and evaluation maps $Ev_Q,\ Ev_P$ can be done polynomially [28, Section 4, Remarks] (cf. also [30, p. 509, Remark 4.3.33]). ■

Remark III.9. *This complexity can indeed be refined. We plan to study in detail this problem in a forthcoming work.*

IV. Upper bounds and example of construction

Using our strategy, we propose in this section:

- upper bounds of symmetric bilinear complexity for large extension of finite fields $\mathbb{F}_2$ and $\mathbb{F}_3$, and
- an example of a multiplication algorithm construction.

In order to obtain the best bounds of symmetric bilinear complexity, we use our Remark III.2 not with bounds $\mu_{q,\mathcal{C}}^{sym}(\deg P_i, u_i)$ derived from the same elliptic curve $\mathcal{C}$, but with the better known bounds for $\mu_q^{sym}(\deg P_i, u_i)$ as in Proposition III.1. Moreover, for a fixed n, to obtain the best bounds of symmetric bilinear complexity, we need

to find the best curve of genus one and thus we compute, not $\mu_{q,\mathcal{C}}^{sym}(n)$ but $\mu_{q,1}^{sym}(n)$. We note throughout the rest of the paper $\mu_q^{sym}(n)$ instead of $\mu_{q,1}^{sym}(n)$.

A. New Bounds

In elliptic curve cryptography, the NIST (National Institute of Standards and Technology) [24] suggests to use finite fields with $2^{163}, 2^{233}$, $2^{283}, 2^{409}$ and 2^{571} elements. Randriambololona in [25] obtained the following bound

$$\mu_2^{sym}(163) \leq 910.$$

We improve this bound

$$\mu_2^{sym}(163) \leq 906.$$

In order to upgrade $\mu_2^{sym}(163)$, we seek out of the curves given in Remark III.2, the one which provides the lowest bilinear complexity. Using only higher multiplicity with degree one and degree two places, the best curve turns out to be $y^2 + y + x^3 = 0$. This curve has 3 points of degree one, and the lowest bilinear complexity is obtained with the divisor G of degree 326 defined as follows:
we take all 3 points of degree 1 with multiplicity 4, all 3 points of degree 2 with multiplicity 2, and all 2 points of degree 3, all 6 points of degree 5, all 11 points of degree 6 and 25 points of degree 8, all with multiplicity 1. Then the degree of G is

$$\begin{aligned} \deg G &= 3.1.4 + 3.2.2 + 2.3.1 + 6.5.1 + 11.6.1 + 25.8.1 \\ &= 326 = 2.163. \end{aligned}$$

From Remark III.2 used with the best known bounds for $\mu_q^{sym}(\deg P_i, u_i)$ and values of Table I we obtain

$$\begin{aligned} \mu_2^{sym}(163) &\leq 3.\mu_2^{sym}(1,4) + 3.\mu_2^{sym}(2,2) \\ &\quad + 2.\mu_2^{sym}(3,1) + 6.\mu_2^{sym}(5,1) \\ &\quad + 11.\mu_2^{sym}(6,1) + 25.\mu_2^{sym}(8,1) \\ &\leq 3.\widehat{M}_2(4) + 3.\mu_2^{sym}(2)\widehat{M}_2(2) \\ &\quad + 2.\mu_2^{sym}(3) + 6.\mu_2^{sym}(5) \\ &\quad + 11.\mu_2^{sym}(6) + 25.\mu_2^{sym}(8) \\ \mu_2^{sym}(163) &\leq 906. \end{aligned}$$

Table III (respectively Table IV) represents optimal bounds for $\mu_2^{sym}(n)$ (respectively $\mu_3^{sym}(n)$) and the size of extension for $\mathbb{F}_2$ is in accordance with the NIST for elliptic curve cryptography. The column N represents the number of places of arbitrary degrees used to obtain the optimal bound, and column U, the associated order for derivative evaluation. As example, for $n = 233$, we obtain the lower bound 1340 using the elliptic curve (up to isomorphism) defined by $y^2 + xy = x^3 + 1$. This lower bound is achieved with $N = [4, 2, 0, 2, 8, 8, 10, 34]$ and $U = [5, 2, 1, 1, 1, 1, 1, 1]$, meaning that we use 4 degree one places with multiplicity $u_1 = 5$, 2 degree two places with multiplicity $u_2 = 2$ and the remainder with multiplicity $u_3 = \cdots = u_8 = 1$.

TABLE III

OPTIMAL BOUNDS FOR $\mu_2^{sym}(n)$.

n	$\mu_2^{sym}(n)$	Elliptic Curve	N	U
163	906	$y^2+y+x^3=0$	$[3,3,2,0,6,11,0,25]$	$[4,2,1,1,1,1,1,1]$
233	1340	$y^2+xy+x^3+1=0$	$[4,2,0,2,8,8,10,34]$	$[5,2,1,1,1,1,1,1]$
283	1668	$y^2+xy+x^3+1=0$	$[4,2,0,2,8,8,14,34,8]$	$[5,2,1,1,1,1,1,1,1]$
409	2495	$y^2+xy+x^3+1=0$	$[4,2,0,2,8,8,16,34,0,31]$	$[5,2,1,1,1,1,1,1,1,1]$
571	3566	$y^2+xy+x^3+1=0$	$[4,2,0,2,8,8,16,34,2,62]$	$[5,1,1,1,1,1,1,1,1,1]$

TABLE IV

OPTIMAL BOUNDS FOR $\mu_3^{sym}(n)$.

n	$\mu_3^{sym}(n)$	Elliptic Curve	N	U
57	234	$y^2+2x^3+2x^2+1=0$	$[3,6,11,15]$	$[3,1,1,1]$
97	410	$y^2+2x^3+2x^2+1=0$	$[3,6,11,15,16]$	$[3,1,1,1,1]$
150	643	$y^2+2x^3+2x^2+1=0$	$[3,6,11,14,38]$	$[3,1,1,1,1]$
200	878	$y^2+2x^3+x^2+1=0$	$[2,5,12,21,47,5]$	$[3,1,1,1,1,1]$
400	1879	$y^2+2x^3+x^2+1=0$	$[2,5,12,21,47,72]$	$[2,1,1,1,1,1]$

B. Effective multiplication algorithm in $\mathbb{F}_{3^{57}}$

In this section, we choose to present the construction of the multiplication algorithm in $\mathbb{F}_{3^{57}}$ with 234 bilinear multiplications, using elliptic curves, points of higher degree and higher multiplicity.

*1) **Method**:* Let α and β be two elements of $\mathbb{F}_{3^{57}}$. Since there exists a point Q of degree 57, the residue class field $\mathcal{O}_Q/Q$ is isomorphic to $\mathbb{F}_{3^{57}}$ and we can consider that both elements are in $\mathcal{O}_Q/Q$. Furthermore, there exists a divisor D such that the evaluation map

$$\begin{aligned} Ev_Q : \mathscr{L}(D) &\longrightarrow \frac{\mathcal{O}_Q}{Q} \\ f \quad &\longmapsto f(Q) \end{aligned}$$

is onto. Hence there exist two functions $F_\alpha,\ F_\beta \in \mathscr{L}(D)$ such that $Ev_Q(F_\alpha)=\alpha$, and $Ev_Q(F_\beta)=\beta$. Finally, to obtain the product $\alpha.\beta$, we compute $Ev_Q(F_\alpha.F_\beta)=\alpha.\beta$. At this step, we have to construct the only $F_\gamma \in \mathscr{L}(2D)$ such that $F_\alpha.F_\beta = F_\gamma$. The uniqueness of F_γ comes from the injectivity of the second evaluation map $Ev_{\mathcal{P}}$. Consider $F_\alpha=\sum_{i=1}^{57} a_i f_i$, $F_\beta=\sum_{i=1}^{57} b_i f_i$ and let F_γ be the product of F_α and F_β given by the relation

$$\underbrace{(F_\alpha).(F_\beta)}_{M} = \underbrace{F_\gamma}_{C}, \tag{5}$$

where M and C are the matrix representation of the relation (5).

*2) **Choice of the degree of places**:* For a fixed q and n, we do not know how to find an order of magnitude of the degree of places to use for the interpolation. This task depends on two factors that is the number of places and the derivative evaluation. We reason now similarly as for the proof of Theorem III.5: in the worst case we suppose that we do not use derivative evaluation, and that we only use places of a fixed degree d. Recall that from [29, Corollary 5.2.10] applied to elliptic curves, the number B_d of places of degree d verifies

$$\frac{q^d}{d} - 9\frac{q^{d/2}}{d} < B_d < \frac{q^d}{d} + 9\frac{q^{d/2}}{d}.$$

In practice, we reason in asymptotic way. Asymptotically $B_d \backsimeq q^d/d$ so it suffices to find the smallest d such that $d(q^d/d) > 2n$. Since this process only gives us an estimation for the maximal degree of places to use, it is possible that for a given d, $B_d = 0$. In this case we shall take $d+1$ and so on. Consequently, to choose the right elliptic curve for the multiplication in $\mathbb{F}_{3^{57}}$ we increase the degree of places until d equals to five.

*3) **Choice of the order for derivative evaluation**:* We know that using derived evaluation with places of high degree does not improve the bilinear complexity so for $\mathbb{F}_{3^{57}}$, we choose to use derived evaluation only for places of degree one and two. Moreover, we choose to use derivative evaluation until order $u_1 = 5$ for degree one places and until order $u_2 = 3$ for degree two places.

*4) **Choice of the Curve**:* Let P_j denotes the set of places of degree j and $P_j[\ k\ ]$ be the k^{th} places of degree j. In order to find the suitable curve, one just have to execute the procedure below for each curve of Remark III.2:

1) construct the associated elliptic function field,
2) determine all places of degree $1, 2, 3$, 4 and 5,
3) find all combinations of the divisor

$$G = u_1 P_1 + \cdots + u_N P_N,$$

with the appropriate degree,

4) for each combination, compute $\sum_{i=1}^{N} \mu_q^{sym}(\deg P_i, u_i)$ and store the lowest bilinear complexity.

Note that super singular curves can be used with no danger since we only use points for interpolation. Results of the previous procedure are collected in Table V.

TABLE V
CHOICE OF THE CURVE FOR $\mu_3^{sym}(57)$.

Equation $\mathcal{C}$	N	U	$\mu_{3,\mathcal{C}}^{sym}(57)$
$y^2 + 2x^3 + 2x^2 + 2 = 0$	[6, 3, 4, 21, 0]	[2, 1, 1, 1, 1]	240
$y^2 + 2x^3 + x^2 + 1 = 0$	[2, 5, 12, 15, 1]	[2, 1, 1, 1, 1]	240
$y^2 + 2x^3 + x^2 + 2 = 0$	[5, 5, 5, 15, 3]	[3, 1, 1, 1, 1]	241
$y^2 + 2x^3 + 2x^2 + 1 = 0$	[3, 6, 11, 15, 0]	[3, 1, 1, 1, 1]	**234**
$y^2 + 2x^3 + 2x = 0$	[4, 6, 8, 9, 6]	[3, 1, 1, 1, 1]	239
$y^2 + 2x^3 + x + 2 = 0$	[7, 0, 7, 18, 0]	[3, 1, 1, 1, 1]	239
$y^2 + 2x^3 + x + 1 = 0$	[1, 3, 9, 19, 1]]	[3, 1, 1, 1, 1]	251

From Table V, the suitable curve, up to isomorphism, is

$$E : y^2 + 2x^3 + 2x^2 + 1 = 0,$$

and the divisor G is constructed as follows: we take all 3 points of degree 1 with multiplicity 3, and then we take all 6 points of degree 2, all 11 points of degree 3, and all 15 points of degree 4, all with multiplicity 1. It must be verified that G has degree

$$\deg G = 3.1.3 + 6.2.1 + 11.3.1 + 15.4.1 = 114 = 2 \cdot 57.$$

Using values of Table I we obtain

$$\begin{aligned}\mu_3^{sym}(57) &\leq 3.\mu_3^{sym}(1,3) + 6.\mu_3^{sym}(2,1)\\ &+11.\mu_3^{sym}(3,1) + 15.\mu_3^{sym}(4,1)\\ &\leq 3.\widehat{M_3}(3) + 6.\mu_3^{sym}(2)\\ &+11.\mu_3^{sym}(3) + 15.\mu_3^{sym}(4)\\ &\leq 234.\end{aligned}$$

*5) **Place $\mathscr{Q}$ and Divisor D**:* In the following, we use the notation of magma [13] for the representation of places and divisors. In order to construct $\mathbb{F}_{3^{57}}$ we choose the place $\mathscr{Q}$ defined by

$$\mathscr{Q} := (x^{57} + x^{56} + 2x^{54} + 2x^{53} + 2x^{51} + 2x^{50} + 2x^{49} + x^{48} + x^{46} + x^{43} + 2x^{42} + 2x^{41} + 2x^{39} + 2x^{38} + 2x^{37} + 2x^{36} + x^{35} + 2x^{32} + 2x^{29} + x^{28} + x^{27} + 2x^{26} + x^{25} + x^{24} + 2x^{23} + 2x^{21} + 2x^{20} + x^{19} + x^{18} + 2x^{15} + x^{14} + 2x^{13} + x^{10} + 2x^8 + x^7 + x^6 + 2x^5 + x^4 + x^3 + 2x^2 + x + 2, z + 2x^{56} + x^{55} + x^{54} + x^{53} + x^{52} + 2x^{50} + 2x^{49} + x^{48} + 2x^{47} + 2x^{45} + 2x^{43} + 2x^{42} + 2x^{41} + 2x^{38} + 2x^{37} + 2x^{36} + 2x^{35} + x^{34} + x^{33} + x^{32} + 2x^{31} + 2x^{29} + x^{28} + 2x^{25} + 2x^{24} + x^{23} + 2x^{22} + 2x^{20} + x^{19} + 2x^{18} + x^{17} + x^{15} + 2x^{13} + 2x^{12} + x^{11} + x^{10} + x^8 + x^6 + 2x^5 + x^2 + 2x + 1),$$

and we choose the following divisor $\mathscr{D}$ such that

$$\mathscr{D} = (x^{57} + x^{55} + x^{53} + x^{48} + x^{46} + 2x^{45} + 2x^{43} + 2x^{42} + x^{40} + 2x^{36} + x^{35} + x^{34} + x^{33} + x^{32} + x^{29} + 2x^{27} + x^{26} + 2x^{24} + 2x^{23} + 2x^{21} + 2x^{18} + 2x^{17} + x^{16} + 2x^{13} + x^{12} + 2x^{10} + 2x^9 + x^8 + 2x^7 + 2x^6 + 2x^3 + 2x^2 + x + 2, z + x^{56} + 2x^{55} + x^{54} + x^{53} + 2x^{52} + x^{51} + x^{50} + 2x^{49} + x^{48} + 2x^{47} + 2x^{46} + 2x^{45} + x^{43} + 2x^{42} + 2x^{41} + 2x^{39} + x^{38} + x^{37} + x^{36} + 2x^{35} + 2x^{34} + x^{32} + 2x^{30} + 2x^{29} + 2x^{28} + x^{27} + x^{26} + x^{25} + x^{24} + x^{21} + x^{20} + 2x^{17} + x^{16} + x^{13} + 2x^{12} + x^{10} + x^9 + x^8 + 2x^7 + 2x^6 + 2x^5 + x^4 + 2x^2),$$

to construct $\mathscr{B} = \{f_1, \ldots, f_{114}\}$ the basis of $\mathscr{L}(2\mathscr{D})$ containing a basis of $\mathscr{L}(\mathscr{D})$. Note that to construct the degree 57 divisor $\mathscr{D}$ it is sufficient to take a degree 57 place Q' different from $\mathscr{Q}$ since the support of $\mathscr{D}$ must not contain $\mathscr{Q}$.

*6) **Interpolation Phase**:* In order to construct the function F_γ of $\mathscr{L}(2\mathscr{D})$, it suffices to use the relation (5) to interpolate at all points chosen to obtain the bound 234. We classify the interpolation phase starting with places used with derivative evaluation $u > 1$, and we finish by the ones used with no derivative evaluation.

- **Derivative Evaluation**

  Remember that the higher multiplicity $u = 3$, occurs only with places of degree 1. This means that we use

the local expansion at order 3 for all points of degree 1, hence for any function f_i of the basis $\mathscr{B}$ we have

$$f_i(P_1[k]) = \alpha_{i,0} + \alpha_{i,1} t_k + \alpha_{i,2} {t_k}^2, \tag{6}$$

where $\alpha_{i,j}$ is an element of $\mathbb{F}_3$, and t_k is the local parameter for $P_1[k]$. Using the relation (5) to interpolate at points of degree 1 leads to

$$\begin{array}{c} \left(\sum_{i=1}^{57} a_i f_i(P_1[\ k\ ])\right) . \left(\sum_{i=1}^{57} b_i f_i(P_1[\ k\ ])\right) \\ = \sum_{i=1}^{114} c_i f_i(P_1[\ k\ ]), \end{array} \tag{7}$$

where $k \in [1, \ldots, 3]$, $a_i,\ b_i,$ and $c_i \in \mathbb{F}_3$. Substituting expression (6) in equation (7) allows us to write

$$\begin{array}{c} \left(A_0 + A_1 t_k + A_2 {t_k}^2\right) . \left(B_0 + B_1 t_k + B_2 {t_k}^2\right) \\ = C_0 + C_1 t_k + C_2 {t_k}^2, \end{array} \tag{8}$$

where

$$A_\ell = \sum_{i=1}^{57} a_i \alpha_{i,\ell},\ B_\ell = \sum_{i=1}^{57} b_i \alpha_{i,\ell} \ \text{ and } \ C_\ell = \sum_{i=1}^{114} c_i \alpha_{i,\ell}.$$

The quantity (8) is exactly the complexity of 3-multiplication of two 3-$term$ polynomials of $\mathbb{F}_{3^{\deg P_1}}[t_k]$. We have $\widehat{M_3}(3) = 5$, meaning that to obtain the three first coefficients of the product, we need the 5 bilinear multiplications in $\mathbb{F}_{3^{\deg P_1}}$

$$\begin{aligned} m_1 &= A_0.B_0, \\ m_2 &= A_1.B_1, \\ m_3 &= A_2.B_2, \\ m_4 &= (A_0 + A_1).(B_0 + B_1), \\ m_5 &= (A_0 + A_2).(B_0 + B_2). \end{aligned}$$

Remember, if we use derivative evaluation with places of degree more than one, we should have 5 bilinear multiplications in $\mathbb{F}_{3^{\deg P}}$, and finally we should add $\mu_3^{sym}(\deg P)$ the bilinear complexity of multiplication in $\mathbb{F}_{3^{\deg P}}$. This being said, for our example we use all 3 points of degree 1 with multiplicity 3, so we obtain 15 bilinear multiplications, the matrix representation of which is

$$\begin{pmatrix} m_1 \\ m_4 - m_1 - m_2 \\ m_5 - m_3 - m_1 + m_2 \\ m_6 \\ m_9 - m_6 - m_7 \\ m_{10} - m_8 - m_6 + m_7 \\ m_{11} \\ m_{14} - m_{11} - m_{12} \\ m_{15} - m_{13} - m_{11} + m_{12} \end{pmatrix} = \begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \\ C_4 \\ C_5 \\ C_6 \\ C_7 \\ C_8 \end{pmatrix}.$$

For places of higher degree, we use all of them with multiplicity 1, thus with no derivative evaluation.

- **No Derivative Evaluation**

Using the relation (5) to interpolate at points of degree $\deg P_j$ leads to

$$\left(\sum_{i=1}^{57} a_i f_i(P_j[\ k\ ])\right).\left(\sum_{i=1}^{57} b_i f_i(P_j[\ k\ ])\right) = \sum_{i=1}^{114} c_i f_i(P_j[\ k\ ]). \tag{9}$$

For any function f_i of the basis $\mathscr{B}$, $f_i(P_j[\ k\ ])$ is an element of the finite field $\mathbb{F}_{3^{\deg P_j}}$ in which a representation is

$$\mathbb{F}_{3^{\deg P_j}} = \mathbb{F}_3(w_k) = \frac{\mathbb{F}_3[X]}{< P_j[\ k\ ] >}.$$

If the set $\{1, w_k, \ldots, {w_k}^{j-1}\}$ denotes a basis of $\mathbb{F}_{3^{\deg P_j}}$, then there exist j elements, $s_{i,0}, s_{i,1}, \ldots, s_{i,j-1}$ of $\mathbb{F}_3$ such that

$$f_i(P_j[\ k\ ]) = s_{i,0} w_k^0 + s_{i,1} w_k^1 + \cdots + s_{i,j-1} {w_k}^{j-1}. \tag{10}$$

Equation (10) allows us to rewrite relation (9) as

$$\left(\sum_{\ell=0}^{j-1} A_\ell {w_k}^\ell\right).\left(\sum_{\ell=0}^{j-1} B_\ell {w_k}^\ell\right) = \left(\sum_{\ell=0}^{j-1} C_\ell {w_k}^\ell\right), \tag{11}$$

where

$$A_\ell = \sum_{i=1}^{57} a_i s_{i,\ell}, \quad B_\ell = \sum_{i=1}^{57} b_i s_{i,\ell}, \text{ and } C_\ell = \sum_{i=1}^{114} c_i s_{i,\ell}.$$

One can easily identify expression (11) as the multiplication of two elements of $\mathbb{F}_{3^{\deg P_j}}$ over $\mathbb{F}_3$. The bilinear complexity of multiplication is, in the case of interpolation at places with no derivative evaluation, $\mu_3^{sym}(\deg P)$.

- When $\deg P = 2$ equation (11) becomes

$$\left(\sum_{\ell=0}^{1} A_\ell {w_k}^\ell\right).\left(\sum_{\ell=0}^{1} B_\ell {w_k}^\ell\right) = \left(\sum_{\ell=0}^{1} C_\ell {w_k}^\ell\right),$$

and this expression is the multiplication of two elements of $\mathbb{F}_{3^2}$ over $\mathbb{F}_3$ which bilinear complexity $\mu_3^{sym}(2)$ equals 3. It means that to obtain coefficients C_0, C_1, one needs three bilinear multiplications, obtained with Karatsuba algorithm and defined by

$m_1 = A_0.B_0,$

$m_2 = A_1.B_1,$

$m_3 = (A_0 + A_1).(B_0 + B_1).$

– For degrees 3 places, we have $\mu_3^{sym}(3) = 6$ where the 6 multiplications needed are

$$m_1 = A_0.B_0,$$
$$m_2 = A_1.B_1,$$
$$m_3 = A_2.B_2,$$
$$m_4 = (A_0 + A_1).(B_0 + B_1),$$
$$m_5 = (A_0 + A_2).(B_0 + B_2),$$
$$m_6 = (A_1 + A_2).(B_1 + B_2).$$

– Finally for degrees 4 places where $\mu_3^{sym}(4) = 9$, with

$$m_1 = A_0.B_0,$$
$$m_2 = A_1.B_1,$$
$$m_3 = A_2.B_2,$$
$$m_4 = A_3.B_3,$$
$$m_5 = (A_0 + A_1).(B_0 + B_1),$$
$$m_6 = (A_0 + A_2).(B_0 + B_2),$$
$$m_7 = (A_2 + A_3).(B_2 + B_3),$$
$$m_8 = (A_1 + A_3).(B_1 + B_3),$$
$$m_9 = (A_0 + A_1 + A_2 + A_3).(B_0 + B_1 + B_2 + B_3).$$

*7) **Evaluation at Place** $\mathscr{Q}$:* In order to complete the multiplication algorithm, we have to reconstruct F_γ and then evaluate it at the chosen place $\mathscr{Q}$. The final matrix representation of the interpolation phase can be rewrite as

$$\underbrace{\begin{pmatrix} m_1 \\ m_4 - m_1 - m_2 \\ m_5 - m_3 - m_1 + m_2 \\ m_6 \\ m_9 - m_6 - m_7 \\ m_{10} - m_8 - m_6 + m_7 \\ m_{11} \\ m_{14} - m_{11} - m_{12} \\ m_{15} - m_{13} - m_{11} + m_{12} \\ \vdots \\ m_1 + \cdots + 2m_{230} - m_{231} + m_{234} \end{pmatrix}}_{M} = \underbrace{\begin{pmatrix} 11101101 \ldots 01020010 \\ 01001110 \ldots 10200110 \\ 21201101 \ldots 01020022 \\ 21201101 \ldots 10221122 \\ 11201011 \ldots 02021010 \\ 11201110 \ldots 11020011 \\ 01201101 \ldots 01020112 \\ 11201001 \ldots 01020211 \\ \vdots \\ 21201110 \ldots 01020011 \\ 01201111 \ldots 01020011 \end{pmatrix}}_{G} \underbrace{\begin{pmatrix} c_1 \\ \vdots \\ c_{114} \end{pmatrix}}_{c}.$$

Since G is invertible, we have $G^{-1}.M = (c_1, \ldots, c_{114})$ and then the only function F_γ of $\mathscr{L}(2\mathscr{D})$ such that $F_\alpha.F_\beta = F_\gamma$ is

$$F_\gamma = c_1 f_1 + \cdots + c_{114} f_{114}.$$

Recall that to obtain the product $\alpha.\beta$ we just have to evaluate F_γ at the place $\mathscr{Q}$ so

$$\alpha.\beta = F_\gamma(\mathscr{Q}) = c_1 f_1(\mathscr{Q}) + \cdots + c_{114} f_{114}(\mathscr{Q}).$$

8) ***Final product*** $\alpha\beta$*:* To complete the algorithm, we must find coefficients $\widehat{c}_i$ for i $[1..57]$ such that

$$\left(\sum_{i=1}^{57} a_i f_i\right) . \left(\sum_{i=1}^{57} b_i f_i\right) = \sum_{i=1}^{57} \widehat{c}_i f_i.$$

Let

$$(e_1, \ldots, e_{114}) = (f_1(\mathscr{Q}), \ldots, f_{114}(\mathscr{Q}))$$

With these notations we have

$$F_\gamma(\mathscr{Q}) = c_1 e_1 + \cdots + c_{57} e_{57} + c_{58} e_{58} + \cdots + c_{114} e_{114}.$$

Vectors $(e_1, \ldots, e_{57})$ form a basis of $\mathbb{F}_{3^{57}}$ as $(f_1, \ldots, f_{57})$ is a basis of $\mathscr{L}(\mathscr{D})$, then to find coefficients $\widehat{c}_i$ for $i \in [1..57]$, it is sufficient to express vectors $(e_{58}, \ldots, e_{114})$ according to $(e_1, \ldots, e_{57})$. This leads to

$$\begin{aligned} e_{58} &= e_1 + 2e_2 + \cdots + e_{57}, \\ \vdots & \qquad \vdots \\ e_{114} &= 2e_1 + e_2 + \cdots + 2_{57}, \end{aligned}$$

and bringing together terms in $(e_1, \ldots, e_{57})$, we finally get

$$\alpha\beta = \underbrace{(c_1 + c_{58} + \cdots + c_{114})}_{\widehat{c}_1} e_1 + \cdots + \underbrace{(c_{57} + \cdots + 2c_{114})}_{\widehat{c}_{57}} e_{57}.$$

Remark IV.1. *Explicit formulas for the multiplication in $\mathbb{F}_{3^{57}}$ and the verification program to execute with Magma can be found in [31].*

REFERENCES

[1] N. Arnaud. Évaluation Dérivées, Multiplication dans les Corps Finis et Codes Correcteurs. *PhD Thesis*, 2006. Université de la Méditerranée, Institut de Mathématiques de Luminy.

[2] S. Ballet. Curves with many points and multiplication complexity in any extension of $\mathbb{F}_q$. *Finite Fields and their Applications*, 5(4), 364-377, 1999.

[3] S. Ballet. Quasi-optimal algorithms for multiplication in the extensions of $\mathbb{F}_{16}$ of degree $13, 14$ and 15. *Journal of Pure and Applied Algebra*, 171(2-3), 149-164, 2002.

[4] S. Ballet. An improvement of the construction of the D.V. and G.V. Chudnovsky algorithm for multiplication in finite fields. *Theoretical Computer Science*, 352(1-3), 293-305, 2006.

[5] S. Ballet. On the tensor rank of the multiplication in the finite fields. *Journal of Number Theory 128*, 6, 1795-1806, 2008.

[6] S. Ballet and D. Le Brigand. On the existence of non special divisor of degree g and $g-1$ in algebraic function fields over $\mathbb{F}_q$. *Journal of Number Theory*, 116, 293-310, 2006.

[7] S. Ballet and J. Chaumine. On the bounds of the bilinear complexity of multiplication in some finite fields. *Applicable Algebra in Engineering, Communication and Computing*, 15(3-4), 205-211, 2004.

[8] S. Ballet and J. Pieltant. On the tensor rank of multiplication in any extension of $\mathbb{F}_2$. *Journal of Complexity*, 27, 230-245, 2011.

[9] S. Ballet and R. Rolland. Multiplication algorithm in a finite field and tensor rank of the multiplication. *Journal of Algebra*, 272/1, 173-185, 2004.

[10] S. Ballet and R. Rolland. On the bilinear complexity of the multiplication in finite fields. In *Proceedings of the Conference Arithmetic, Geometry and Coding Theory (AGCT 2003), Société Mathématique de France, sér. Séminaires et Congrès 11, 179-188*, 2005.

[11] U. Baum and M. A. Shokrollahi. An optimal algorithm for multiplication in $\mathbb{F}_{256}/\mathbb{F}_4$. *Applicable Algebra in Engineering, Communication and Computing*, 2:15–20, 1991.

[12] R. Barbulescu, J. Detrey, N. Estibals and P. Zimmermann. Finding Optimal Formulae for Bilinear Maps. Lecture Notes in Computer Science, Vol 7369, pages 168-186. Springer. Arithmetic of Finite Fields - 4th International Workshop, WAIFI 2012, Bochum, Germany, July 16-19, 2012. Proceedings.

[13] W. Bosma, J. Cannon and C. Playoust. The Magma Algebra System I. The user language. *Journal of Symbolic Computation 24*, 3-4, 235-265, 1957.

[14] I. Cascudo, R. Cramer, C. Xing and A. Yang: Asymptotic Bound for Multiplication Complexity in the Extensions of Small Finite Fields. *IEEE Transactions on Information Theory*, 58, 7, 4930-4935, 2012.

[15] M. Cenk and F. Özbudak. Improved Polynomial Multiplication Formulas over $\mathbb{F}_2$ Using Chinese Remainder Theorem. *IEEE Transactions on Computers*, 58(4), 572-576, 2009.

[16] M. Cenk and F. Özbudak. On multiplication in finite fields. *Journal of Complexity*, 26, 172-186, 2010.

[17] J. Chaumine. Multiplication in small finite fields using elliptic curves. *Algebraic geometry and its applications*, 343-350, Ser. Number Theory Appl., 5, World Sci. Publ., Hackensack, NJ, 2005.

[18] J-M. Couveignes and R. Lercier. Elliptic periods for finite fields. *Finite Fields and Their Applications*, Vol 15, pages 1-22, 2009.

[19] D. V. and G. V. Chudnovsky. Algebraic complexities and algebraic curves over finite fields. *Journal of Complexity*, 4, 285-316, 1988.

[20] R. R. Farashi, I. Shparlinski, J. F. Voloch. On Hasing into Elliptic Curves. Journal of Mathematical Cryptology, 3, 4, 353-360, 2009.

[21] H. F. de Groote. *Lectures on the Complexity of Bilinear Problems*, Vol 245 of *Lecture Notes in Computer Science*. Springer, 1987.

[22] T. Icart. How to hash into Elliptic Curves. Lectures Notes in Computer Science, Vol 5677, Springer-Verlag, pages 303–316. Proceedings Crypto' 2009.

[23] P. L. Montgomery. Five, Six, and Seven-Term Karatsuba-Like Formulae. *IEEE Transactions on Computers*, 54, 3, 362-369, 2005.

[24] National Institute of Standards and Technology. Digital Signature Standard. *FIPS Publication*, 186-2, 2000.

[25] H. Randriambololona. Bilinear complexity of algebras and the Chudnovsky-Chudnovsky interpolation method. *Journal of Complexity*, 28, 489-517, 2012.

[26] A. Shallue and C. E. Van De Woestijne. Construction of Rationals points on elliptic curves ove finite fields. *Algorithmic Number Theory, 7th International Symposium, Proceedings*. ANTS, Springer, Lecture Notes in Computer Science, Vol 4076, 2006, 3-540-36075-1.

[27] M. A. Shokrollahi. Optimal algorithms for multiplication in certain finite fields using elliptic curves. *SIAM Journal on Computing*, 21(1193-1198), 1992.

[28] I. Shparlinski, M. Tsfasman, and S. Vladut. Curves with many points and multiplication in finite fields. In H. Stichtenoth and M.A. Tsfasman, editors, *Coding Theory and Algebraic Geometry*, number 1518 in Lectures Notes in Mathematics, pages 145–169, Berlin, 1992. Springer-Verlag. Proceedings of AGCT-3 conference, June 17-21, 1991, Luminy.

[29] H. Stichtenoth. *Algebraic Function Fields and Codes*. Berlin. Springer, 1993.

[30] M. Tsfasman, and S Vladut. Algebraic-Geometry Codes (Translated from the russian by the authors). Mathematics and its applications (Soviet Series), 58, Kluwer Academic. Publisher Group, Dordrecht, xxiv+667 pp. ISBN: 0-7923-0727-5, 1991.

[31] M. Tukumuli. PhD dissertation (Annexes). http://goo.gl/Z957M and http://goo.gl/U7Z8l. 2013.

[32] W.C. Waterhouse. Abelian varieties over finite fields. *Ann. Scient. Ec. Norm. Sup., 4ème série*, t.2, 521–560, 1969.

[33] S. Winograd. On Multiplication in Algebraic Extension Fields. *Theoretical Computer Science*, 8:359–377, 1979.