Efficient Multiplication in Finite Fields of Characteristic 3 and 5 for Pairing Based Cryptography

Murat CENK, Ferruh ÖZBUDAK

***Abstract*— In [1], it is investigated the eta paring computation on general divisors over hyperelliptic curves $y = x^p - x + d$ where p is a prime satisfying $p \equiv 1 \mod 4$. One of the used finite field in that paper is $\mathbb{F}_{5^n}$. In that paper, it is given a multiplication formula for $\mathbb{F}_{5^n}$ with at most 15 multiplications in $\mathbb{F}_{5^n}$. In our paper, firstly we give a brief survey of efficient multiplication in finite fields by giving an example of multiplication formula for $\mathbb{F}_{3^{6m}}$. Then we will apply the methods used for $\mathbb{F}_{3^{6m}}$ to $\mathbb{F}_{5^{5n}}$ in order to obtain explicit multiplication formula in $\mathbb{F}_{5^{5n}}$. We give a formula for multiplying elements of $\mathbb{F}_{5^{5n}}$ with 11 multiplications in $\mathbb{F}_{5^n}$ which is better than the formula given in [1].**

***Keywords* — Finite field multiplication, pairing-based cryptography**

I. Introduction

FINITE fields of characteristic three are useful for pairing-based cryptography. Therefore, special attention has been given to $\mathbb{F}_{3^m}$, recently [2], [3], [4], [5]. The elements of $\mathbb{F}_{3^m}$ can be represented by at most $(m-1)$ degree polynomials over $\mathbb{F}_3$. To multiply elements of $\mathbb{F}_{3^m}$ one can use Karatsuba method [6], [7] or Montgomery formulae [8], which are among the main algorithms used in every finite fields. On the other hand, for finite fields of fixed characteristics, there are other methods that give more efficient algorithms for polynomial multiplication than Karatsuba and Montgomery in some cases. Some of those methods are Chinese Remainder Theorem (CRT) method [9] and Discrete Fourier Transform (DFT) method. In [3], [4], using DFT method, the multiplication formula in [2] for $\mathbb{F}_{3^{6m}}$ is improved. Moreover, in [5], it is found that using a method based on CRT for polynomial multiplication over $\mathbb{F}_3$ and suitable reductions, it is obtained an efficient multiplication method for finite fields of characteristic 3. For $5 \leq \ell \leq 18$, it is shown the canonical multiplication formulae over $\mathbb{F}_{3^{\ell m}}$ for any $m \geq 1$ with the best multiplicative complexity improving the bounds in [8].

In the recent paper [1], it is investigated the eta paring computation on general divisors over hyperelliptic curves $y^3 = x^p - x + d$ where p is a prime satisfying $p \equiv 1 \mod 4$. One of the used finite field in that paper is $\mathbb{F}_{5^{5n}}$. Moreover, in that paper, it is also given a multiplication formula for $\mathbb{F}_{5^{5n}}$ with at most 15 multiplications in $\mathbb{F}_{5^n}$.

Murat Cenk is with the Department of Mathematics and Computer Science, Çankaya University, Ankara, Turkey, E-mail:mcenk@cankaya.edu.tr

Ferruh Özbudak is with the Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey, E-mail:ozbudak@metu.edu.tr

In this paper, firstly we give a brief survey of efficient multiplication in finite fields by giving an example of multiplication formula for $\mathbb{F}_{3^{6m}}$. Then we will apply the methods used for $\mathbb{F}_{3^{6m}}$ to $\mathbb{F}_{5^{5n}}$ in order to obtain explicit multiplication formula in $\mathbb{F}_{5^{5n}}$. We give a formula for multiplying elements of $\mathbb{F}_{5^{5n}}$ with 11 multiplications in $\mathbb{F}_{5^n}$ which is better than the formula given in [1].

The rest of the paper is organized as follows. In Section II, we give a brief survey of efficient multiplication in finite fields by giving an example of multiplication formula for $\mathbb{F}_{3^{6m}}$. An explicit formula for multiplication in $\mathbb{F}_{5^{5n}}$ which requires 11 multiplications in $\mathbb{F}_{5^n}$ is presented in Section III. Finally, we give the conclusion.

II. Efficient Polynomial Multiplication over $\mathbb{F}_q$

In this section we give a brief review of efficient polynomial multiplication over $\mathbb{F}_q$.

Let $\mathbb{F}_q$ be the field with q elements. Let $n \geq 1$ be an integer. A polynomial $A(x)$ of the form

$$A(x) = a_0 + a_1 x + ... + a_{n-1} x^{n-1}, \ a_{n-1} \neq 0$$

is called an n-term polynomial. $M_q(n)$ denotes the minimum number of multiplications needed in $\mathbb{F}_q$ in order to multiply two arbitrary n-term polynomials. We note that $M_q(n)$ is also called multiplicative complexity of n-term polynomials. Let $n \geq 1$ be an integer, $f(x)$ be an irreducible polynomial and $\ell \geq 1$ be an integer such that

$$\ell \ deg(f(x)) < 2n - 1.$$

Let $A(x)$ and $B(x)$ be arbitrary n-term polynomials, $C(x) = A(x)B(x)$ and $\overline{A}(x), \overline{B}(x), \overline{C}(x)$ be the uniquely determined polynomials of degree strictly less than $\ell \ deg(f(x))$ such that

$$\overline{A}(x) \equiv A(x) \mod f(x)^\ell,$$

$$\overline{B}(x) \equiv B(x) \mod f(x)^\ell,$$

$$\overline{C}(x) \equiv C(x) \mod f(x)^\ell.$$

Notation 2.1: Let $M_{q,f,\ell}(n)$ denote the minimum number of multiplications needed in $\mathbb{F}_q$ in order to obtain $\overline{C}(x)$ from given n-term polynomials $A(x)$ and $B(x)$. Obtaining such $\overline{C}(x)$ from $A(x)$ and $B(x)$ is called multiplication of n-term polynomials modulo $f(x)^\ell$.

Let $1 \leq w \leq 2n-2$ be an integer and $C(x) = c_0 + c_1 x + ... + c_{2n-2} x^{2n-2}$. Obtaining the last w coefficients

$c_{2n-2}, c_{2n-3}, ..., c_{2n-1-w}$ of $C(x)$ is defined as the multiplication of n-term polynomials modulo $(x-\infty)^w$ [9], [10].

Notation 2.2: Let $M_{q,(x-\infty),w}(n)$ denote the minimum number of multiplications needed in $\mathbb{F}_q$ in order to obtain $c_{2n-2}, c_{2n-3}, ..., c_{2n-1-w}$ from given n-term polynomials $A(x)$ and $B(x)$.

CRT method for finite field polynomial multiplication can be summarized as follows. For $1 \leq i \leq t$, let $m_i(x) = f_i(x)^{\ell_i}$ be the ℓ_i-th power ($\ell_i \geq 1$) of an irreducible polynomial $f_i(x)$ such that $deg(m(x)) \geq 2n-1$ where $m(x) = \prod_{i=1}^{t} m_i(x)$. Assume that $f_1(x), ..., f_t(x)$ are distinct. Let $w \geq 1$ be an integer which corresponds to multiplication modulo $(x-\infty)^w$ (see [10] and [9, p. 34]). It follows from CRT algorithm that if

$$w + \sum_{i=1}^{t} \ell_i \ deg(f_i(x)) \geq 2n-1 \qquad \text{(II.1)}$$

then

$$M_q(n) \leq M_{q,(x-\infty),w}(n) + \sum_{i=1}^{t} M_{q,f,\ell}(n). \qquad \text{(II.2)}$$

The value of $M_{q,f,\ell}(n)$ can be bounded from above by $M_q(deg(f^\ell)) \leq M_q(\ell \cdot deg(f))$. For example in [10], $M_{q,f,\ell}(n) \leq M_q(\ell \cdot deg(f))$ is used for binary fields. In [11], we improved the estimate of $M_{q,f,\ell}(n)$ for the binary field $\mathbb{F}_2$. The same techniques also work for any finite field $\mathbb{F}_q$, in particular for fields of small characteristic such as $\mathbb{F}_3$ and $\mathbb{F}_5$. Before giving the improvement, we give the following definition.

Definition 2.3: Let $R = \mathbb{F}_q[x]$ be the ring of polynomials over $\mathbb{F}_q$ in variable x, $\ell \geq 1$ be an integer and

$$A(Y) = a_0(x) + a_1(x)Y + ... + a_{\ell-1}(x)Y^{\ell-1},$$
$$B(Y) = b_0(x) + b_1(x)Y + ... + b_{\ell-1}(x)Y^{\ell-1}$$

be two ℓ-term polynomials in the polynomial ring $R[Y]$ over R. Let $c_0(x), ..., c_{2\ell-2}(x) \in R$ be given by

$$c_0(x) + c_1(x)Y + ... + c_{2\ell-2}(x)Y^{2\ell-2} = A(Y)B(Y).$$

Let $\lambda_q(\ell)$ denote the minimum number of multiplications needed in R in order to obtain $c_0(x), c_1(x), ..., c_{\ell-1}(x)$.
The following theorem provides further improvements. The proof can be seen in [11] and [5].

Theorem 2.4: Let $f(x)$ be an irreducible polynomial and $\ell \geq 1$ be an integer such that $\ell \ deg(f(x)) < 2n-1$. We have

$$M_{q,f,\ell}(n) \leq \lambda_q(\ell) M_q(deg(f)). \qquad \text{(II.3)}$$

Remark 2.5: Let $1 \leq w \leq 2n-1$ be an integer. Recall that the notation $M_{q,(x-\infty),w}(n)$ is given in Notation 2.2. It is clear that $M_q(1) = 1$. Using similar methods as in Theorem 2.4 we also obtain that

$$M_{q,(x-\infty),w}(n) \leq \lambda_q(w) M_q(1) = \lambda_q(w).$$

Corollary 2.6: $M_{q,x,w}(n)$ corresponds to computing first w coefficients $c_0, c_1, ..., c_w$ of $c(x)$ and $M_{q,x,w}(n) = M_{q,(x-\infty),w}(n) \leq \lambda_q(w)$.
Some effective upper bounds of $\lambda_q(\ell)$ is given in the following proposition which contributes to improvements on $M_{q,f,\ell}(n)$. The proof is in [5].

Proposition 2.7: $\lambda_q(3) \leq 5, \lambda_q(4) \leq 8, \lambda_q(5) \leq 11, \lambda_q(6) \leq 15, \ \lambda_q(7) \leq 19, \ \lambda_q(8) \leq 24, \ \text{and} \ \lambda_q(9) \leq 29.$

Once we obtain a formula for multiplying n-term polynomials over $\mathbb{F}_q$, it is also valid over $\mathbb{F}_{q^m}$ because of the following theorem. The proof can be found in [12].

Theorem 2.8: The formulae for multiplication of two arbitrary n-term polynomials over $\mathbb{F}_q$ are also valid for multiplication of two arbitrary n-term polynomials over $\mathbb{F}_{q^m}$, where m is any positive integer.

The notation $\mu_q(n)$ represents *the bilinear complexity of multiplication in* $\mathbb{F}_{q^n}$ *over* $\mathbb{F}_q$. It corresponds to the minimum number of $\mathbb{F}_q$ multiplications in order to multiply two arbitrary elements of $\mathbb{F}_{q^n}$. As reduction modulo an irreducible polynomial in $\mathbb{F}_q[x]$ can be performed without multiplications in $\mathbb{F}_q$, we have

$$\mu_q(n) \leq M_q(n). \qquad \text{(II.4)}$$

However $\mu_q(n)$ and $M_q(n)$ are not necessarily equal in general. Using a polynomial basis $\{1, \xi, \xi^2, \ldots, \xi^{n-1}, \ldots, \xi^{2n-2}\}$ for $\mathbb{F}_{q^{2n-1}}$ over $\mathbb{F}_q$, it is easy to show that

$$M_q(n) \leq \mu_q(2n-1).$$

Example 2.9: The finite fields of $\mathbb{F}_{3^{6m}}$, where m is prime are used in id-based cryptography for efficient computation of the Tate pairing. In [2], it is given a multiplication algorithm in $\mathbb{F}_{3^{6m}}$ with 18 multiplications in $\mathbb{F}_{3^m}$. In [3], [4], multiplication in $\mathbb{F}_{3^{6m}}$ is decreased to 15 multiplications in $\mathbb{F}_{3^m}$. On the other hand, when we use $(x-\infty)^2$, f_{11}, f_{12}, f_{13}, f_{21}, f_{22} and f_{23} in the method describe in Section II, we obtain $M_3(6) \leq 15$. Then by (II.4), the formula for multiplying two 6-term polynomials over $\mathbb{F}_3$ can be used for the multiplication over $\mathbb{F}_{3^{6m}}$ with 15 multiplications in $\mathbb{F}_{3^m}$. Now we will show that multiplication in $\mathbb{F}_{3^{6\cdot 97}}$ which is investigated in [4] can be done with 15 multiplications in $\mathbb{F}_{3^{97}}$. Let us construct,

$$\mathbb{F}_{3^{97}} \cong \mathbb{F}_3[x]/(x^{97} + x^{16} + 2),$$
$$\mathbb{F}_{3^{6\cdot 97}} \cong \mathbb{F}_{3^{97}}[y]/(y^6 + y - 1).$$

Let $\alpha, \beta, \gamma \in \mathbb{F}_{3^{6\cdot 97}}$ such that $\alpha = \sum_{i=0}^{5} a_i y^i$, $\beta = \sum_{i=0}^{5} b_i y^i$ and $\gamma = \alpha \cdot \beta = \sum_{i=0}^{5} c_i y^i$. Then the coefficients of γ can be found as follows: First compute the coefficients of $\left(\sum_{i=0}^{5} a_i y^i\right)\left(\sum_{i=0}^{5} b_i y^i\right)$ and then reduce it modulo y^6+y-1. Therefore, using the method described in Section II we get

$c_0 = -m_{15} - m_1 + m_{10} - m_6 - m_5 + m_7 - m_8 - m_9 - m_{12} - m_{11}$;
$c_1 = m_{15} + m_2 - m_3 - m_4 + m_5 - m_7 - m_8 + m_{10} - m_{11} + m_{12} + m_{13} + m_{14}$;
$c_2 = -m_3 + m_5 + m_4 - m_6 - m_1 - m_2 - m_8 + m_9 - m_{13}$;
$c_3 = -m_3 - m_5 + m_7 - m_1 - m_8 - m_9 - m_{13} - m_{15}$;
$c_4 = m_6 + m_{13} - m_{12} - m_{11} - m_8 - m_{10} - m_5 - m_7 + m_2 - m_3 - m_4$;
$c_5 = m_{14} - m_8 + m_9 - m_{10} - m_6 + m_{13} - m_1 + m_3 - m_{11} + m_{12}$;
where m_i's are
$m_1 = (a_0 + a_1 + a_2 + a_3 + a_4 + a_5)(b_0 + b_1 + b_2 + b_3 + b_4 + b_5)$;
$m_2 = (a_0 + a_1)(b_0 + b_1)$; $m_3 = a_0 b_0$; $m_4 = a_1 b_1$;

$m_5 = (a_1 - a_3 - a_5 + a_2)(b_1 - b_3 - b_5 + b_2)$;
$m_6 = (a_0 - a_2 - a_4 + a_1 - a_5)(b_0 - b_2 - b_4 + b_1 - b_5)$;
$m_7 = (a_0 - a_2 + a_4 + a_1 - a_3 + a_5)(b_0 - b_2 + b_4 + b_1 - b_3 + b_5)$;
$m_8 = (a_0 - a_2 + a_4)(b_0 - b_2 + b_4)$; $m_9 = (a_1 - a_3 + a_5)(b_1 - b_3 + b_5)$;
$m_{10} = (a_0 - a_1 + a_2 - a_3 + a_4 - a_5)(b_0 - b_1 + b_2 - b_3 + b_4 - b_5)$;
$m_{11} = (a_0 + a_2 - a_4 - a_3)(b_0 + b_2 - b_4 - b_3)$;
$m_{12} = (a_0 - a_4 + a_3 + a_1 - a_5)(b_0 - b_4 + b_3 + b_1 - b_5)$;
$m_{13} = (a_0 + a_2 - a_4 + a_3)(b_0 + b_2 - b_4 + b_3)$;
$m_{14} = (a_1 - a_3 - a_5 - a_2)(b_1 - b_3 - b_5 - b_2)$; $m_{15} = a_5 b_5$;

On the other hand $\mathbb{F}_{3^{6\cdot 97}}$ is constructed in [3], [4] using tower field representation, i.e.

$$\begin{aligned} \mathbb{F}_{3^{97}} &\cong \mathbb{F}_3[x]/(x^{97} + x^{16} + 2), \\ \mathbb{F}_{3^{2\cdot 97}} &\cong \mathbb{F}_{3^{97}}[y]/(y^2 + 1), \\ \mathbb{F}_{3^{6\cdot 97}} &\cong \mathbb{F}_{3^{2\cdot 97}}[z]/(z^3 - z - 1). \end{aligned}$$

Therefore, the formula in [3], [4] contains multiplication by $\mp s, \mp(s+1)$ and $\mp(s-1)$, where $s \in \mathbb{F}_{3^{2\cdot 97}}$ is a root of $y^2 + 1$. For both our proposed formula and the formula in [4], the number of multiplications is 15. The number of additions for our proposed formula is 137. Note that there are multiplications of form $(s \mp 1)m_i$ in the formula in [4]. Here $s \notin \mathbb{F}_3$. If we disregard the multiplication by s in the formula [4] and if we consider the cost of multiplication of the form $(s \mp 1)m_i$ for the formula in [4] as 1 addition only then the number of additions for the formula in [4] is still 138. Moreover, in our formula the only nonzero coefficients are ∓ 1 and we don't need to introduce intermediate field extension like $\mathbb{F}_{3^{2\cdot 97}}$ containing $s \notin \mathbb{F}_3$. Therefore it seems that our construction would be preferable to the construction in [3], [4].

III. Efficient Multiplication for $\mathbb{F}_{5^{5n}}$

The finite field $\mathbb{F}_{5^{5n}}$ is used in [1]. Multiplication in $\mathbb{F}_{5^{5n}}$ in [1] is performed by using Karatsuba-Ofman algorithm with 15 multiplications in $\mathbb{F}_{5^n}$ as follows. Let $A = \sum_{i=0}^{4} a_i \rho^i$, $B = \sum_{i=0}^{4} a_i \rho^i \in \mathbb{F}_{5^{5n}}$ where $\{1, \rho, \rho^2, \rho^3, \rho^4\}$ is a basis for $\mathbb{F}_{5^{5n}}$ over $\mathbb{F}_{5^n}$ Then

$$AB = (A_2\rho^3 + A_1)(B_1\rho^3 + B_2) = A_2B_2\rho^6 + ((A_2 + A_1)(B_2 + B_1) - A_2B_1 - A_1B_1)\rho^3 + A_1B_1,$$

where

$$A_2 = (a_4\rho + a_3),\ A_1 = (a_2\rho^2 + a_1\rho + a_1)$$

$$B_2 = (b_4\rho + b_3),\ B_1 = (b_2\rho^2 + b_1\rho + b_1).$$

Since the polynomials A_2 and B_2 have 2 terms, A_2B_2 needs 3 multiplications in $\mathbb{F}_{5^n}$ due to Karatsuba method. Since A_1B_1 and $(A_2+A_1)(B_2+B_1)$ are 3-term polynomials over $\mathbb{F}_{5^n}$, they need 6 multiplications in $\mathbb{F}_{5^n}$ by Karatsuba method. Therefore, $\mu_{5^n}(5) \leq 15$.

In fact, the multiplication can be further improved. For example, we can improve this bound to 14 multiplications in $\mathbb{F}_{5^n}$ by observing a common multiplication a_2b_2 in both A_1B_1 and $(A_2 + A_1)(B_2 + B_1)$.

Moreover, we can decrease this bound to 13 as follows. Since A_1B_1 and $(A_2 + A_1)(B_2 + B_1)$ are three term polynomials over $\mathbb{F}_{5^n}$, we can multiply them with 5 multiplications by using the interpolation algorithm. For example, we can multiply 3-term polynomials over $\mathbb{F}_{5^n}$ as follows:
$(a_0 + a_1x + a_2x^2)(b_0 + b_1x + b_2x^2) = m_1 + (4m_2 + 2m_3 + 3m_4 + m_5)x + (4m_2 + m_3 + m_4 + 4m_5)x^2 + (4m_2 + 3m_3 + 2m_4 + m_5)x^3 + (4m_1 + 4m_2 + 4m_3 + 4m_4 + 4m_5)x^4$
where
$m_1 = a_0b_0$,
$m_2 = (a_0 + a_1 + a_2)(b_0 + b_1 + b_2)$,
$m_3 = (a_0 + 2a_1 + 4a_2)(b_0 + 2b_1 + 4b_2)$,
$m_4 = (a_0 + 3a_1 + 4a_2)(b_0 + 3b_1 + 4b_2)$,
$m_5 = (a_0 + 4a_1 + a_2)(b_0 + 4b_1 + b_2)$.
Therefore, we can write $\mu_{5^n}(5) \leq 13$.

Now, we will show that this bound can be further improved by using the method presented in Section II by obtaining $M_5(5) \leq 11$. Let $a(x) = \sum_{i=0}^{4} a_i x^i$ and $b(x) = \sum_{i=0}^{4} b_i x^i$ be two 5-term polynomials over $\mathbb{F}_5$. Let

$$c(x) = \left(\sum_{i=0}^{4} a_i x^i\right)\left(\sum_{i=0}^{4} b_i x^i\right) = \sum_{i=0}^{8} c_i x^i \qquad \text{(III.1)}$$

be product the polynomial. When we use the modulus polynomials $x^2, (x-1), (x-2), (x-3), (x-4)$ and $x^2 + 3$ as evaluation points in (III.1), we obtain the following system of linear, equations:

$$\begin{array}{lll} x^2 & \Rightarrow & \begin{cases} m_1 = c_0, \\ m_2 - m_1 - m_3 = c_1, \end{cases} \\ x-1 & \Rightarrow & m_4 = (c_0 + \cdots + c_8), \\ x-2 & \Rightarrow & m_5 = (c_0 + 2c_1 + ... + 2^8c_8), \\ x-3 & \Rightarrow & m_6 = (c_0 + 3c_1 + ... + 3^8c_8), \\ x-4 & \Rightarrow & m_7 = (c_0 + 4c_1 + ... + 4^8c_8), \\ x-\infty & \Rightarrow & m_8 = c_8, \\ x^2+3 & \Rightarrow & \begin{cases} m_9 + 2m_{10} = c_0 + 2c_2 + 4c_4 + 3c_6 + c_8, \\ m_{11} - m_9 - m_{10} = c_1 + 2c_3 + 4c_5 + 3c_7, \end{cases} \end{array}$$

where

$m_1 = a_0b_0,\ m_2 = (a_0 + a_1)(b_0 + b_1),\ m_3 = a_1b_1,$
$m_4 = (a_0 + a_1 + a_2 + a_3 + a_4)(b_0 + b_1 + b_2 + b_3 + b_4),$
$m_5 = (a_0 + 2a_1 + 4a_2 + 3a_3 + a_4)(b_0 + 2b_1 + 4b_2 + 3b_3 + b_4),$
$m_6 = (a_0 + 3a_1 + 4a_2 + 2a_3 + a_4)(b_0 + 3b_1 + 4b_2 + 2b_3 + b_4),$
$m_7 = (a_0 + 4a_1 + a_2 + 4a_3 + a_4)(b_0 + 4b_1 + b_2 + 4b_3 + b_4),$
$m_8 = a_4b_4,\ m_9 = (a_0 + 2a_2 + 4a_4)(b_0 + 2b_2 + 4b_4)$
$m_{10} = (a_1 + 2a_3)(b_1 + 2b_3),$
$m_{11} = (a_1 + 2a_3 + a_0 + 2a_2 + 4a_4)(b_1 + 2b_3 + b_0 + 2b_2 + 4b_4).$

So we obtain the following system of linear equations

$$M = G \cdot C, \qquad \text{(III.2)}$$

where

$$M = \begin{bmatrix} m_1 \\ m_2 - m_1 - m_3 \\ m_4 \\ m_5 \\ m_6 \\ m_7 \\ m_8 \\ m_9 + 2m_{10} \\ m_{11} - m_9 - m_{10} \end{bmatrix},\ C = \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \\ c_8 \end{bmatrix},$$

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 3 & 1 & 2 & 4 & 3 & 1 \\ 1 & 3 & 4 & 2 & 1 & 3 & 4 & 2 & 1 \\ 1 & 4 & 1 & 4 & 1 & 4 & 1 & 4 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 2 & 0 & 4 & 0 & 3 & 0 & 1 \\ 0 & 1 & 0 & 2 & 0 & 4 & 0 & 3 & 0 \end{bmatrix}.$$

The resulting coefficients c_i's for $0 \leq i \leq 8$ are obtained by solving equation (III.2). Since matrix G is invertible we have $C = M \cdot G^{-1}$ where

$$G^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 3 & 4 & 4 & 3 & 2 & 4 & 0 \\ 0 & 2 & 3 & 2 & 3 & 2 & 0 & 0 & 4 \\ 4 & 0 & 4 & 4 & 4 & 4 & 4 & 0 & 0 \\ 0 & 4 & 4 & 2 & 3 & 1 & 0 & 0 & 0 \\ 3 & 0 & 1 & 2 & 2 & 1 & 3 & 1 & 0 \\ 0 & 3 & 1 & 1 & 4 & 4 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

By using $C = M \cdot G^{-1}$, we get the following explicit formula.

$$\begin{aligned} c_0 &= m_1, \\ c_1 &= m_2 - m_1 - m_3, \\ c_2 &= 2m_1 + 3m_4 + 4m_5 + 4m_6 + 3m_7 + 2m_8 + 4m_9 + 8m_{10}, \\ c_3 &= 2m_2 - 2m_1 - 2m_3 + 3m_4 + 2m_5 + 3m_6 + 2m_7 + 4m_{11} - \\ &\quad 4m_9 - 4m_{10}, \\ c_4 &= 4m_1 + 4m_4 + 4m_5 + 4m_6 + 4m_7 + 4m_8, \\ c_5 &= 4m_2 - 4m_1 - 4m_3 + 4m_4 + 2m_5 + 3m_6 + m_7, \\ c_6 &= 3m_1 + m_4 + 2m_5 + 2m_6 + m_7 + 3m_8 + m_9 + 2m_{10}, \\ c_7 &= 3m_2 - 3m_1 - 3m_3 + m_4 + m_5 + 4m_6 + 4m_7 + m_{11} - \\ &\quad m_9 - m_{10}, \\ c_8 &= m_8. \end{aligned}$$

IV. Conclusion

We explain an efficient method for polynomial multiplication over $\mathbb{F}_q$. We give an explicit formula for multiplication in $\mathbb{F}_{5^{5n}}$ which requires 11 multiplications in $\mathbb{F}_{5^n}$. To the best of our knowledge, given formula which is better than the formula given in [1] is the best known formula.

Acknowledgments

This work was supported by TÜBİTAK under Grant No. TBAG-107T826.

References

[1] E. Lee, H. Lee and Y. Lee , Eta pairing computation on general divisors over hyperelliptic curves $y = x^p - x + d$, Journal of Symbolic Computation, 43(6-7),pp. 452-474.

[2] T. Kerins, W. P. Marnane, E. M. Popovici, and P. S. L. M. Barreto, "Efficient hardware for the tate pairing calculation in characteristic three", in *Cryptographic Hardware and Embedded Systems, CHES2005, ser. Lecture Notes in Computer Science*, J. R. Rao and B. Sunar, Eds., vol. 3659. Springer- Verlag, 2005, pp. 412 - 426.

[3] E. Gorla, C. Puttmann and J. Shokrollahi, "Explicit formulas for efficient multiplication in $\mathbb{F}_{6m}$", in *Selected Areas in Cryptography (SAC 2007)* (Also avaliable at http://www.arxiv.org/PS_cache/arxiv/pdf/0708/0708.3014v1.pdf).

[4] J. Shokrollahi, E. Gorla and C. Puttmann, "Efficient FPGA-Based Multipliers for $\mathbb{F}_{97}$ and $\mathbb{F}_{6\cdot 97}$", in *Field Programmable Logic and Applications (FPL 2007)* (Also avaliable at http://www.arxiv.org/PS_cache/arxiv/pdf/0708/0708.3022v1.pdf).

[5] M. Cenk, F. Özbudak, "Efficient multiplication in $\mathbb{F}_{\ell m}$, $m \geq 1$ and $5 \leq \ell \leq 18$", *Africacrypt 2008 volume 5023 of Lecture Notes in Computer Science*, 406-414 Springer - Verlag.

[6] A. Karatsuba and Y. Ofman, "Multiplication of multidigit numbers by automata", *Soviet Physics-Doklady*, (7):595-596, 1963.

[7] A. Weimerskirch, C. Paar, "Generalizations of the Karatsuba Algorithm for Polynomial Multiplication", avaliable: *http://eprint.iacr.org/2006/224*.

[8] P. L. Montgomery, "Five, six, and seven-term Karatsuba-like formulae", *IEEE Transactions on Computers*, 54(3):362-369, March 2005.

[9] S. Winograd, *Arithmetic Complexity of Computations,* SIAM, 1980.

[10] H. Fan and M. Anwar Hasan, Comments on "Five, Six, and Seven-Term Karatsuba-Like Formulae", *IEEE Transactions on Computers*, vol. 56, no. 5, pp. 716-717, 2007.

[11] M. Cenk and F. Özbudak, "Improved Polynomial Multiplication Formulae over $\mathbb{F}$ Using Chinese Remainder Theorem", to appear in *IEEE Transactions on Computers*, accepted for publication on 7 October 2008.

[12] M. D. Wagh and S. D. Morgera, "A new structured design method for convolutions over finite fields, Part I", *IEEE Transactions on Information Theory*, 29(4):583-594, 1983.