Journal of Computational and Applied Mathematics 236 (2011) 177–183

Contents lists available at ScienceDirect

Journal of Computational and Applied Mathematics

journal homepage: www.elsevier.com/locate/cam

Efficient multiplications in $\mathbb{F}_{5^{5n}}$ and $\mathbb{F}_{7^{7n}}$

Murat Cenk [a], Ferruh Özbudak [b,*]

[a] Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey

[b] Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey

ARTICLE INFO

Keywords:
Finite field multiplication
Algebraic function fields
Pairing based cryptography

ABSTRACT

Efficient multiplications in finite fields of characteristics 5 and 7 are used for computing the Eta pairing over divisor class groups of the hyperelliptic curves Lee et al. (2008) [1]. In this paper, using the recent methods for multiplication in finite fields, the explicit formulas for multiplication in $\mathbb{F}_{5^{5n}}$ and $\mathbb{F}_{7^{7n}}$ are obtained with 10 multiplications in $\mathbb{F}_{5^n}$ for $\mathbb{F}_{5^{5n}}$ and 15 multiplications in $\mathbb{F}_{7^n}$ for $\mathbb{F}_{7^{7n}}$ improving the results in Cenk and Özbudak (2008) [4], Cenk et al. (2009) [5], Lee et al. (2008) [1] and Montgomery (2005) [12]. The timing results of implementations of the Karatsuba type formulas and the proposed formula for multiplication in $\mathbb{F}_{5^{5\cdot 89}}$ are given.

1. Introduction

Finite field multiplication plays an important role in the implementation of elliptic curve cryptography and pairing based cryptography. Recent efficient multiplications in $\mathbb{F}_{5^{5n}}$ and $\mathbb{F}_{7^{7n}}$ are used for computing the Eta paring over divisor class groups of the hyperelliptic curves $y^2 = x^p - x + d$ where p is an odd prime [1] in which the Karatsuba type multiplications [2,3] are used. Let $\mu_q(m)$ denote the minimum number of $\mathbb{F}_q$ multiplications in order to multiply two arbitrary elements of $\mathbb{F}_{q^m}$. The Karatsuba type multiplications imply only $\mu_{5^n}(5) \leq 15$ and $\mu_{7^n}(7) \leq 24$. However, there are more efficient methods for improving the bounds on $\mu_q(m)$. For example, recently it has been shown that one can obtain the explicit formula for multiplication in $\mathbb{F}_{5^{5n}}$ with $\mu_{5^n}(5) \leq 11$ in [4,5]. In this paper, by using the recent methods for multiplication in $\mathbb{F}_{q^m}$ (see, [6–10]) improved the values for the multiplications in $\mathbb{F}_{5^{5n}}$ and $\mathbb{F}_{7^{7n}}$ are obtained. The explicit formulas having $\mu_{5^n}(5) \leq 10$ and $\mu_{7^n}(7) \leq 15$, which also improve the corresponding result in [4,5] are given. In particular, these give more efficient Eta pairing computations than the ones in [1]. We also give timing results of implementations of the Karatsuba type formulas and the proposed formula for comparison.

The rest of the paper is organized as follows: We introduce complexity notions in the next section. The method we used is presented in Section 3. In Section 4, we give the details of obtaining the explicit formulas for multiplication in $\mathbb{F}_{5^{5n}}$ and $\mathbb{F}_{7^{7n}}$. We compare the timing results of implementations of the Karatsuba type formula and the proposed formula for multiplication in $\mathbb{F}_{5^{5\cdot 89}}$ in Section 5. We conclude this paper in Section 6.

2. Preliminaries

Bilinear complexity of multiplication in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is the minimum number of $\mathbb{F}_q$ bilinear multiplications in order to multiply two arbitrary elements of $\mathbb{F}_{q^n}$ and it is denoted by $\mu_q(n)$. There is a related but different complexity notion. Let $M_q(n)$ denote the number of multiplications needed in $\mathbb{F}_q$ in order to multiply two arbitrary n-term polynomials in $\mathbb{F}_q[x]$

* Corresponding author.
E-mail addresses: mcenk@metu.edu.tr (M. Cenk), ozbudak@metu.edu.tr (F. Özbudak).

0377-0427/$ – see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.cam.2011.06.016

(cf. [8,11–13,3,14]). Here a polynomial is called an n-term polynomial in $\mathbb{F}_q[x]$ if it is of the form $a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in \mathbb{F}_q[x]$. As reduction modulo, an irreducible polynomial in $\mathbb{F}_q[x]$ can be performed without multiplications in $\mathbb{F}_q$; we have

$$\mu_q(n) \leq M_q(n). \tag{2.1}$$

However, $\mu_q(n)$ and $M_q(n)$ are not necessarily equal in general. By 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 $M_q(n) \leq \mu_q(2n-1)$. We will use another complexity notion in this paper. For a positive integer ℓ, let $\widehat{M}_q(\ell)$ denote the multiplicative complexity of computing the coefficients of the product of two ℓ-term polynomials modulo x^ℓ over $\mathbb{F}_q$. In other words, $\widehat{M}_q(\ell)$ is the minimum number of multiplications needed in $\mathbb{F}_q$ in order to obtain the first ℓ coefficients of the product of two arbitrary ℓ-term polynomials in $\mathbb{F}_q[x]$. It is not difficult to obtain useful upper bounds on $\widehat{M}_q(\ell)$ for certain values ℓ. For example, we have $\widehat{M}_q(2) \leq 3$, $\widehat{M}_q(3) \leq 5$, $\widehat{M}_q(4) \leq 8$ and $\widehat{M}_q(5) \leq 11$ for any prime power q (cf. [8, Proposition 1], [15]).

Throughout the paper, the algebraic function fields are used. We refer the reader to [16] for details of algebraic function fields.

3. The method

Let $F/\mathbb{F}_q$ be an algebraic function field with full constant field $\mathbb{F}_q$. Let $P_1, \ldots, P_N$ be distinct places of arbitrary degrees. Assume that Q is a place of degree n. Let $\mathcal{O}_Q$ be the valuation ring of the place Q. Note that the residue field $\mathcal{O}_Q/Q$ is isomorphic to $\mathbb{F}_{q^n}$. Let D be a divisor such that $\mathrm{supp}D \cap \{Q, P_1, P_2, \ldots, P_N\} = \emptyset$. Let $\mathcal{L}(D)$ be the Riemann–Roch space of D. Also assume that the evaluation map Ev_Q from $\mathcal{L}(D)$ to the residue field $\mathcal{O}_Q/Q$ is onto. For $1 \leq i \leq N$, let t_i be a local parameter at P_i. For $f \in \mathcal{L}(2D)$, let $f = \alpha_{i,0} + \alpha_{i,1}t_i + \alpha_{i,2}t_i^2 + \cdots$ be the local expansion at P_i with respect to t_i, where $\alpha_{i,0}, \alpha_{i,1}, \ldots \in \mathbb{F}_{q^{\deg(P_i)}}$. Let u_i be a positive integer and consider the $\mathbb{F}_q$-linear map

$$\begin{aligned} \varphi_i : \mathcal{L}(2D) &\to (\mathbb{F}_{q^{\deg(P_i)}})^{u_i} \\ f &\to (\alpha_{i,0}, \alpha_{i,1}, \ldots, \alpha_{i,u_i-1}). \end{aligned}$$

Let φ be the $\mathbb{F}_q$-linear map given by

$$\begin{aligned} \varphi : \quad \mathcal{L}(2D) &\to (\mathbb{F}_{q^{\deg(P_1)}})^{u_1} \times (\mathbb{F}_{q^{\deg(P_2)}})^{u_2} \times \cdots \times (\mathbb{F}_{q^{\deg(P_N)}})^{u_N} \\ f &\to (\varphi_1(f), \varphi_2(f), \ldots, \varphi_N(f)). \end{aligned} \tag{3.1}$$

Finally, we assume that the map φ is injective. Under those assumptions we have the following theorems. The proofs are in [10].

Theorem 3.1. *Under the notation and assumptions as above, we have*

$$\mu_q(n) \leq \sum_{i=1}^{N} \mu_q(\deg(P_i))\widehat{M}_{q^{\deg(P_i)}}(u_i). \tag{3.2}$$

Using Theorem 3.1, we obtain the explicit algorithms for multiplications in $\mathbb{F}_{q^n}$. The conditions of the following theorem guarantee that the assumptions of Theorem 3.1 are satisfied.

Theorem 3.2. *Let $F/\mathbb{F}_q$ be an algebraic function field with full constant field $\mathbb{F}_q$. Let g be the genus of F. Let $P_1, P_2, \ldots, P_N$ be distinct places of arbitrary degrees of F. Let $u_1, u_2, \ldots, u_N$ be arbitrary positive integers. Assume that*

(1) *there exists a non-special divisor of degree $g-1$,*
(2) *there exists a place of degree n,*
(3) $\sum_{i=1}^{N} \deg(P_i)u_i > 2n + 2g - 2$.

Then assumptions in Theorem 3.1 hold and we get (3.2).

4. Explicit formulas for multiplication in $\mathbb{F}_{5^{5n}}$ and $\mathbb{F}_{7^{7n}}$

In this section, we will give the details of obtaining the explicit formulas for multiplication in $\mathbb{F}_{5^{5n}}$ and $\mathbb{F}_{7^{7n}}$ using the method described in Section 3. For obtaining the explicit formula for multiplication in $\mathbb{F}_{7^{7n}}$, we need to use a degree one place with $u = 2$. Since using a degree one place with $u = 2$ is one of the main ideas of the method given in Section 3. We prefer to explain all the details of the calculations for obtaining a formula for multiplication in $\mathbb{F}_{7^{7n}}$ with $\mu_{7^n}(7) \leq 15$. We start with the following remark.

Remark 4.1. We consider $\mathbb{F}_{7^{7n}}$ as the extension field of $\mathbb{F}_{7^n}$ with extension degree 7. In other words, we can consider $\mathbb{F}_{7^{7n}} \cong \mathbb{F}_{7^n}[x]/\langle f(x)\rangle$ where $\mathbb{F}_{7^n}[x]$ is the ring of polynomials over $\mathbb{F}_{7^n}$ and $f(x) \in \mathbb{F}_{7^n}[x]$ is an irreducible polynomial. The elements of $\mathbb{F}_{7^n}$ are called scalars. Note that for $n > 1$, one can find a formula for multiplying the elements of $\mathbb{F}_{7^{7n}}$ with 13 multiplications in $\mathbb{F}_{7^n}$ using the interpolation method [14]. This formula contains scalars from $\mathbb{F}_{7^n}$ and depending on n, i.e. when we change the value of n, we must construct a new formula. However, we find a multiplication formula for $\mathbb{F}_{7^{7n}}$ with 15 multiplications containing scalars from only $\mathbb{F}_7$ and it will be valid for all n satisfying $gcd(n, 7) = 1$ where $gcd(a, b)$ for integers a and b is the greatest common divisor of a and b. Moreover, note that the multiplicative cost of multiplication in $\mathbb{F}_{7^n}$ for $n > 1$ is more expensive than the multiplicative cost of multiplication in $\mathbb{F}_7$.

In order to obtain a multiplicative formula for $\mathbb{F}_{7^{7n}}$ which contains scalars only from $\mathbb{F}_7$, we will find a formula for multiplication in $\mathbb{F}_{7^7}$. If $gcd(n, 7) = 1$, then multiplication formula in $\mathbb{F}_{7^7}$ is valid for $\mathbb{F}_{7^{7n}}$. The reason can be explained as follows: let $f(x) \in \mathbb{F}_7[x]$ be the reduction polynomial of $\mathbb{F}_{7^7}$, i.e. $\mathbb{F}_{7^7} \cong \mathbb{F}_7[x]/\langle f(x)\rangle$ and $gcd(n, 7) = 1$. Then $f(x)$ is also irreducible over $\mathbb{F}_{7^n}$. Therefore, we can write $\mathbb{F}_{7^{7n}} \cong \mathbb{F}_{7^n}[x]/\langle f(x)\rangle$. Note that a degree one place of an algebraic function field over $\mathbb{F}_7$ is also a degree one place of the same algebraic function field over $\mathbb{F}_{7^n}$. When we use the method given in Section 3 for multiplication in $\mathbb{F}_{7^7}$ and $\mathbb{F}_{7^{7n}}$, using the same degree one places, we obtain the same formulas. Therefore, if $gcd(n, 7) = 1$, the multiplication formula for $\mathbb{F}_{7^7}$ will be the same with the multiplication formula for $\mathbb{F}_{7^{7n}}$

The following remark is related to the condition $gcd(n, 7) = 1$ from the cryptographical point of view.

Remark 4.2. In pairing based cryptography, the extension degree n is generally selected as a prime number for security. For example, in [1] $n = 29$ for $\mathbb{F}_{7^{7n}}$ and $n = 89$ for $\mathbb{F}_{5^{5n}}$ are selected. So, in general, the conditions $gcd(n, 7) = 1$ for $\mathbb{F}_{7^{7n}}$ and $gcd(n, 5) = 1$ for $\mathbb{F}_{5^{5n}}$ are satisfied.

Now we will give the details of obtaining an explicit formula for multiplication in $\mathbb{F}_{7^7}$ with 15 multiplications in $\mathbb{F}_7$. Consider the elliptic curve $E/\mathbb{F}_7 : y^2 = x^3 + 3$. This curve contains 13 degree one places. Let $\{P_1, \ldots, P_{13}\}$ be the set of degree one places of E. Those places are

$$P_1 = \infty, \quad P_2 = (x + 4, y + 3), \quad P_3 = (x + 4, y + 4), P_4 = (x + 5, y + 2),$$
$$P_5 = (x + 5, y + 5), \quad P_6 = (x + 1, y + 3), \quad P_7 = (x + 1, y + 4),$$
$$P_8 = (x + 3, y + 2), \quad P_9 = (x + 3, y + 5), \quad P_{10} = (x + 2, y + 3),$$
$$P_{11} = (x + 2, y + 4), \quad P_{12} = (x + 6, y + 2), \quad P_{13} = (x + 6, y + 5).$$

Note that throughout the paper we use the notation of Magma [17] for presenting the places and divisor of algebraic function fields. When we use P_1 with $u = 2$ and $P_2, \ldots, P_{13}$ with $u = 1$, the map φ defined in Section 3 becomes injective. In order to obtain an explicit formula, we need to find a local parameter of P_1. A local parameter of P_1 is $t = xy/(x^3 + 3)$. Let us choose $D = (x^7 + 6x^5 + 6x^3 + 5x + 1, 6x^6 + x^5 + 3x^3 + 6x^2 + 4x + y + 2)$. Let $\{f_1, \ldots, f_{14}\}$ be a basis of $\mathcal{L}(2D)$ where $\{f_1, \ldots, f_7\}$ is the basis of $\mathcal{L}(D)$. A basis of $\mathcal{L}(2D)$ containing a basis of $\mathcal{L}(D)$ is given in Appendix A.

Now consider the elements $a = \sum_{i=1}^{7} a_i f_i \in \mathcal{L}(\mathcal{D})$ and $b = \sum_{i=1}^{7} b_i f_i \in \mathcal{L}(\mathcal{D})$. Let $c = \sum_{i=1}^{14} c_i f_i$ be the product of a and b given by

$$\left(\sum_{i=1}^{7} a_i f_i\right) \cdot \left(\sum_{i=1}^{7} b_i f_i\right) = \sum_{i=1}^{14} c_i f_i. \tag{4.1}$$

Then we get the following system of linear equations

$$\underbrace{\begin{bmatrix} m_1 \\ m_2 + m_3 \\ m_4 \\ m_5 \\ m_6 \\ m_7 \\ m_8 \\ m_9 \\ m_{10} \\ m_{11} \\ m_{12} \\ m_{13} \\ m_{14} \\ m_{15} \end{bmatrix}}_{M} = \underbrace{\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 6 & 3 & 2 & 1 & 0 & 5 & 1 & 2 & 3 & 6 & 1 & 2 & 2 & 4 \\ 1 & 6 & 3 & 6 & 4 & 4 & 1 & 4 & 6 & 5 & 2 & 4 & 4 & 1 \\ 0 & 5 & 4 & 6 & 6 & 0 & 1 & 6 & 3 & 6 & 0 & 5 & 3 & 1 \\ 2 & 6 & 1 & 1 & 0 & 4 & 1 & 5 & 6 & 5 & 0 & 3 & 6 & 2 \\ 1 & 3 & 1 & 5 & 3 & 3 & 1 & 3 & 4 & 1 & 5 & 6 & 0 & 1 \\ 3 & 1 & 3 & 3 & 5 & 1 & 1 & 3 & 4 & 1 & 5 & 6 & 0 & 1 \\ 6 & 4 & 0 & 2 & 2 & 6 & 1 & 0 & 0 & 4 & 3 & 5 & 5 & 1 \\ 0 & 6 & 4 & 3 & 4 & 3 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 6 & 6 & 6 & 0 & 4 & 1 & 1 & 6 & 4 & 1 & 1 & 4 & 3 & 4 \\ 3 & 4 & 0 & 3 & 6 & 0 & 1 & 5 & 1 & 2 & 2 & 1 & 6 & 1 \\ 5 & 1 & 4 & 5 & 4 & 5 & 1 & 1 & 1 & 2 & 6 & 4 & 1 & 4 \\ 3 & 6 & 2 & 3 & 2 & 3 & 1 & 1 & 1 & 2 & 6 & 4 & 1 & 4 \end{bmatrix}}_{G} \underbrace{\begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \\ c_8 \\ c_9 \\ c_{10} \\ c_{11} \\ c_{12} \\ c_{13} \\ c_{14} \end{bmatrix}}_{C}$$

where multiplications m_i for $1 \le i \le 15$ are given in Appendix A. Since G is invertible, we have $C = G^{-1} \cdot M$. Then we can find a multiplication in $\mathbb{F}_{7^7}$ by using $Ev_Q(f)$ where $Ev_Q(f)$ is the evaluation map from $\mathcal{L}(D)$ to $\mathbb{F}_{7^7}$ and we choose

Table 1
Timings (s) for multiplication in $\mathbb{F}_{5^{89\cdot5}}$.

The proposed formula	The Montgomery formula	The Karatsuba method
0.01167	0.01514	0.01725

$Q = (x^7 + 6x + 4, 3x^6 + 4x^4 + 5x^3 + 2x^2 + 2x + y + 1)$. Note that we represent $\mathbb{F}_{7^7}$ as the field $\mathbb{F}_7(w) = \mathbb{F}_7[x]/(f(x))$, where w is the root of the irreducible polynomial $f(x) = x^7 + 6x + 4$. Let $\{\xi_1, \xi_2, \ldots, \xi_7\}$ be a basis of $\mathbb{F}_{7^7}$ over $\mathbb{F}_7$ such that

$$\xi_1 = 4w^6 + 6w^5 + 4w^4 + 4w^3 + w^2 + 3w + 1,$$
$$\xi_2 = 6w^6 + 4w^5 + 6w^4 + 4w^3 + 4w^2 + w + 4,$$
$$\xi_3 = 6w^5 + 4w^4 + 6w^3 + 4w^2 + 4w + 1, \qquad \xi_4 = 3w^6 + 6w^4 + 4w^3 + 6w^2 + 4w + 1,$$
$$\xi_5 = 3w^5 + 6w^3 + 4w^2 + 6w + 4, \qquad \xi_6 = 4w^6 + 3w^4 + 6w^2 + 4w + 2, \qquad \xi_7 = 1,$$

where $Ev_Q(f_i) = \xi_i$. The formula that we obtain is valid for the above basis. A well known basis of a finite field is the polynomial basis. Since the polynomial basis is easy to use, we convert the formula obtained above to polynomial basis. The explicit formula using the polynomial basis is given in Appendix C.

Now we will explain how to obtain an explicit formula for multiplication in $\mathbb{F}_{5^{5n}}$ with 10 multiplications. We use the elliptic curve $y^2 + xy + 2y - x^3 + x = 0$. It has 10 degree one places. We select the reduction polynomial as $x^5 - x^4 + 1$. Note that this polynomial is irreducible over $\mathbb{F}_{5^n}$ for all positive integer n satisfying. When we apply the method given in Section 3, we get a multiplication formula for $\mathbb{F}_{5^{5n}}$ with 10 multiplications. The explicit formula in the polynomial basis is given in Appendix B.

5. Timing results

The proposed formulas use less number of multiplications than the known methods. However, since the proposed formulas are obtained using the interpolation method on algebraic function fields, the number of additions may increase. The main question is the effect of those additions in practice. Now, we will give the timing results for multiplication in $\mathbb{F}_{5^{89\cdot5}}$. Here we choose $n = 89$, because $\mathbb{F}_{5^{89\cdot5}}$ is used in [1]. We compare the Karatsuba, Montgomery and proposed formulas. We consider $\mathbb{F}_{5^{89\cdot5}}$ as the extension field of $\mathbb{F}_{5^{89}}$ with extension degree 5. The elements of $\mathbb{F}_{5^{89\cdot5}}$ are multiplied by using the Karatsuba and Montgomery 5-term polynomial multiplication formulas together with (2.1) with 15 and 13 multiplications in $\mathbb{F}_{5^{89}}$ respectively. On the other hand, the proposed formula uses only 10 multiplications in $\mathbb{F}_{5^{89}}$. The implementation of the formula in the platform of a single processor 1.7 Ghz Intel Celeron gives that the proposed formula is faster than both the Karatsuba and Montgomery formulas. We use Magma [17] for the multiplication in $\mathbb{F}_{5^{89}}$ (Table 1).

Note that since the multiplication in $\mathbb{F}_{5^{89}}$ takes much more time than the addition in $\mathbb{F}_{5^{89}}$, the proposed formula which uses less multiplication than the Karatsuba and Montgomery formulas yields faster multiplication.

6. Conclusions

Using the recent methods for multiplication in $\mathbb{F}_{q^m}$, we obtain improved values for the explicit formulas for multiplication in $\mathbb{F}_{5^{5n}}$ and $\mathbb{F}_{7^{7n}}$. We get the explicit formulas giving $\mu_{5^n}(5) \leq 10$ and $\mu_{7^n}(7) \leq 15$. In particular, these give more efficient Eta pairing computations than the ones in [1]. We also give timing results of implementations of the Karatsuba type formulas and the proposed formula for comparison. The implementation of the multiplication formula in $\mathbb{F}_{5^{89\cdot5}}$ gives that the proposed formula is faster than both the Karatsuba and Montgomery formulas.

Acknowledgments

Murat Cenk performed this work while he was with the Institute of Applied Mathematics, Middle East Technical University. The authors were partially supported by TÜBİTAK under Grant No. TBAG-107T826 and TBAG-109T672.

Appendix A

A basis $\{f_1, f_2, \ldots, f_{14}\}$ used in Section 4 of $\mathcal{L}(2\mathcal{D})$ is given where $\{f_1, f_2, \ldots, f_7\}$ is a basis of $\mathcal{L}(\mathcal{D})$ and $f = x^7 + 6x^5 + 6x^3 + 5x + 1$.

$$f_1 = \frac{5x^6 + x^5y + 4x^5 + 6x^3 + 5x^2 + 3x + 4}{f}, \qquad f_2 = \frac{3x^6 + 5x^5 + x^4y + x^4 + 3x^2 + 5x + 4}{f}$$
$$f_3 = \frac{3x^6 + 3x^5 + 2x^4 + x^3y + x^3 + 4x^2 + 3x + 6}{f}, \qquad f_4 = \frac{x^6 + 3x^5 + 2x^4 + 2x^3 + x^2y + 4x + 1}{f}$$

$$f_5 = \frac{6x^6 + x^5 + 4x^4 + 2x^3 + 3x^2 + xy + 6}{f}, \qquad f_6 = \frac{x^6 + 6x^5 + 4x^3 + x^2 + 3x + y + 5}{f}, \qquad f_7 = 1,$$

$$f_8 = \frac{2x^{14} + x^{13} + 2x^{12} + x^{11}y + 3x^{11} + x^{10} + 4x^9y + 5x^9 + 4x^8y + 5x^8 + 3x^7y}{f^2} + \frac{3x^7 + 3x^6y + 2x^6 + 4x^5y + 4x^5 + x^4y + 2x^4 + 4x^3y + 6x^2y + 5x^2 + 5xy + 4x}{f^2},$$

$$f_9 = \frac{2x^{13} + x^{12} + 2x^{11} + x^{10}y + 3x^{10} + x^9 + 4x^8y + 5x^8 + 4x^7y + 5x^7}{f^2} + \frac{3x^6y + 3x^6 + 3x^5y + 2x^5 + 4x^4y + 4x^4 + x^3y + 2x^3 + 4x^2y + 6xy + 5x + 5y + 4}{f^2},$$

$$f_{10} = \frac{2x^{12} + x^{11} + 2x^{10} + x^9y + 3x^9 + x^8 + 4x^7y + 2x^7 + 4x^6y + 3x^6 + 3x^5y + 6x^5}{f^2} + \frac{5x^4y + x^4 + 2x^3y + x^3 + 6x^2y + x^2 + 4xy + 4x + 6y + 2}{f^2},$$

$$f_{11} = \frac{2x^{11} + x^{10} + 2x^9 + x^8y + 3x^8 + 3x^7 + 4x^6y + x^6 + 4x^5y + x^5 + 4x^4y + 2x^4}{f^2} + \frac{4x^3y + 3x^3 + x^2y + 4x^2 + 6xy + 3x + 4y + 6}{f^2},$$

$$f_{12} = \frac{2x^{10} + x^9 + 2x^8 + x^7y + 2x^7 + 4x^5y + 2x^5 + 3x^4 + x^3y + x^3 + x^2y}{f^2} + \frac{5x^2 + xy + 3x + 6y + 2}{f^2},$$

$$f_{13} = \frac{2x^9 + x^8 + 4x^7 + x^6y + x^6 + 5x^5 + 5x^4y + 5x^4 + 6x^3y + 5x^34x^2 + xy + y + 5}{f^2},$$

$$f_{14} = \frac{2x^8 + 6x^7 + 5x^6 + x^5y + 3x^5 + 6x^4y + 2x^4 + 6x^3y + 3x^3 + 2x^2 + 2x + y + 5}{f^2}.$$

The multiplications used in Section 4 are

$$m_1 = a_7b_7,\ m_2 = a_1b_7,\ m_3 = a_7b_1,$$
$$m_4 = (6a_1 + 3a_2 + 2a_3 + a_4 + 5a_6 + a_7)(6b_1 + 3b_2 + 2b_3 + b_4 + 5b_6 + b_7),$$
$$m_5 = (a_1 + 6a_2 + 3a_3 + 6a_4 + 4a_5 + 4a_6 + a_7)(b_1 + 6b_2 + 3b_3 + 6b_4 + 4b_5 + 4b_6 + b_7),$$
$$m_6 = (5a_2 + 4a_3 + 6a_4 + 6a_5 + a_7)(5b_2 + 4b_3 + 6b_4 + 6b_5 + b_7)$$
$$m_7 = (2a_1 + 6a_2 + a_3 + a_4 + 4a_6 + a_7)(2b_1 + 6b_2 + b_3 + b_4 + 4b_6 + b_7),$$
$$m_8 = (a_1 + 3a_2 + 1a_3 + 5a_4 + 3a_5 + 3a_6 + a_7)(b_1 + 3b_2 + 1b_3 + 5b_4 + 3b_5 + 3b_6 + b_7),$$
$$m_9 = (3a_1 + a_2 + 3a_3 + 3a_4 + 5a_5 + a_6 + a_7)(3b_1 + b_2 + 3b_3 + 3b_4 + 5b_5 + b_6 + b_7),$$
$$m_{10} = (6a_1 + 4a_2 + 2a_4 + 2a_5 + 6a_6 + a_7)(6b_1 + 4b_2 + 2b_4 + 2b_5 + 6b_6 + b_7),$$
$$m_{11} = (6a_2 + 4a_3 + 3a_4 + 4a_5 + 3a_6 + a_7)(6b_2 + 4b_3 + 3b_4 + 4b_5 + 3b_6 + b_7),$$
$$m_{12} = (6a_1 + 6a_2 + 6a_3 + 4a_5 + 1a_6 + a_7)(6b_1 + 6b_2 + 6b_3 + 4b_5 + 1b_6 + b_7),$$
$$m_{13} = (3a_1 + 4a_2 + 3a_4 + 6a_5 + a_7)(3b_1 + 4b_2 + 3b_4 + 6b_5 + b_7),$$
$$m_{14} = (5a_1 + a_2 + 4a_3 + 5a_4 + 4a_5 + 5a_6 + a_7)(5b_1 + b_2 + 4b_3 + 5b_4 + 4b_5 + 5b_6 + b_7),$$
$$m_{15} = (3a_1 + 6a_2 + 2a_3 + 3a_4 + 2a_5 + 3a_6 + a_7)(3b_1 + 6b_2 + 2b_3 + 3b_4 + 2b_5 + 3b_6 + b_7).$$

Appendix B

We give an explicit formula for multiplication in $\mathbb{F}_{5^{5n}}$ where $gcd(5, n) = 1$. Let the reduction polynomial be $f(x) = x^5 + 4x^4 + 1 \in \mathbb{F}_5[x]$. Note that this polynomial is also irreducible in $\mathbb{F}_{5^n}$ for $gcd(n, 5) = 1$. Then we can construct $\mathbb{F}_{5^{5n}} \cong \mathbb{F}_{5^n}[x]/f(x)$. Let $\alpha = \sum_{i=0}^{4} a_i x^i$, $\beta = \sum_{i=0}^{4} b_i x^i$, and $\gamma = \sum_{i=0}^{4} c_i x^i$ with $(\sum_{i=0}^{4} a_i x^i)\cdot(\sum_{i=0}^{4} b_i x^i) \bmod (x^5+4x^4+1) = \sum_{i=0}^{4} c_i x^i$, with $a_i, b_i, c_i \in \mathbb{F}_{5^n}$. Then, we have

$$c_0 = 4m_1 + m_2 + 4m_3 + 2m_4 + 4m_5 + 2m_6 + 2m_7 + 3m_8 + 4m_9,$$
$$c_1 = 4m_1 + m_{10} + 2m_2 + 4m_3 + 3m_6 + m_7 + 4m_8 + m_9,$$
$$c_2 = 2m_1 + m_{10} + 3m_2 + 3m_3 + 3m_4 + 2m_6 + m_7,$$
$$c_3 = 4m_1 + m_2 + 2m_3 + 4m_4 + 4m_5 + m_7 + 4m_9,$$

$$
\begin{aligned}
c_4 &= 2m_{10} + m_2 + 3m_3 + 2m_4 + 2m_5 + 2m_6 + m_8 + 2m_9,\\
m_1 &= (a_1 + 2a_2 + 4a_4 + a_0)(b_1 + 2b_2 + 4b_4 + b_0),\\
m_2 &= (2a_2 + 4a_3 + a_0)(2b_2 + 4b_3 + b_0),\\
m_3 &= (a_2 + a_3 + 3a_4 + a_0 + 4a_1)(b_2 + b_3 + 3b_4 + b_0 + 4b_1),\\
m_4 &= (a_2 + 2a_3 + 2a_4 + 4a_1 + a_0)(b_2 + 2b_3 + 2b_4 + 4b_1 + b_0),\\
m_5 &= (4a_2 + 4a_3 + a_4 + a_1 + a_0)(4b_2 + 4b_3 + b_4 + b_1 + b_0),\\
m_6 &= (a_2 + 4a_3 + 4a_4 + 4a_1 + a_0)(b_2 + 4b_3 + 4b_4 + 4b_1 + b_0),\\
m_7 &= (4a_2 + 4a_3 + 4a_4 + a_0)(4b_2 + 4b_3 + 4b_4 + b_0),\\
m_8 &= (a_0 + 4a_1 + 3a_2 + 3a_3 + 2a_4)(b_0 + 4b_1 + 3b_2 + 3b_3 + 2b_4),\\
m_9 &= (a_2 + 3a_3 + 3a_4 + 2a_1 + a_0)(b_2 + 3b_3 + 3b_4 + 2b_1 + b_0),\\
m_{10} &= (4a_2 + 2a_3 + a_1 + a_0)(4b_2 + 2b_3 + b_1 + b_0).
\end{aligned}
$$

Appendix C

We give an explicit formula for multiplication in $\mathbb{F}_{7^{7n}}$ where $gcd(7, n) = 1$. Let the reduction polynomial be $f(x) = x^7 + 6x + 4 \in \mathbb{F}_7[x]$. Note that this polynomial is also irreducible in $\mathbb{F}_{7^n}$ for $gcd(n, 7) = 1$. Then we can construct $\mathbb{F}_{7^{7n}} \cong \mathbb{F}_{7^n}[x]/f(x)$. Let $\alpha = \sum_{i=0}^{6} a_i x^i$, $\beta = \sum_{i=0}^{6} x^i$, and $\gamma = \sum_{i=0}^{6} c_i x^i$ with $(\sum_{i=0}^{6} a_i x^i)\cdot(\sum_{i=0}^{6} b_i x^i) \bmod (x^7+6x+4) = \sum_{i=0}^{6} c_i x^i$, with $a_i, b_i, c_i \in \mathbb{F}_{7^n}$.

$$
\begin{aligned}
c_0 &= 3m_1 + 4m_2 + 4m_3 + 2m_4 + m_5 + 2m_6 + 5m_7 + 6m_8 + 2m_9 + 3m_{10} + 3m_{11},\\
c_1 &= 3m_1 + 6m_2 + m_5 + 2m_6 + 5m_{12} + 5m_8 + 4m_9 + 3m_{13} + 3m_{10} + 3m_{11} + 6m_{14},\\
c_2 &= 5m_1 + 2m_2 + 2m_3 + 5m_5 + m_6 + 5m_{12} + 3m_7 + 4m_9 + m_{15} + 6m_{13} + m_{10} + m_{11} + m_{14},\\
c_3 &= 3m_2 + 6m_3 + 3m_5 + 3m_6 + m_{12} + 3m_7 + m_8 + 6m_9 + 3m_{13} + 6m_{10} + 6m_{11} + 6m_{14},\\
c_4 &= m_1 + 5m_3 + 4m_4 + 3m_5 + m_6 + 5m_{12} + 4m_7 + 5m_9 + 4m_{15} + 5m_{13} + 2m_{10} + 2m_{11} + 5m_{14},\\
c_5 &= 5m_1 + 2m_2 + 3m_3 + m_4 + 2m_5 + 3m_6 + 5m_{12} + 3m_7 + 2m_8 + 2m_9 + 6m_{13} + m_{14},\\
c_6 &= 5m_1 + 3m_2 + 2m_3 + 4m_4 + 3m_5 + 3m_6 + 5m_7 + 4m_8 + 4m_9 + 2m_{15} + 5m_{13} + 2m_{10} + 2m_{11} + 2m_{14},\\
m_1 &= (6a_1 + 5a_2 + a_0 + 5a_3 + 4a_4 + 5a_5)(6b_1 + 5b_2 + b_0 + 5b_3 + 4b_4 + 5b_5),\\
m_2 &= (4a_1 + 3a_2 + a_0 + a_3 + 6a_4 + 5a_6)(4b_1 + 3b_2 + b_0 + b_3 + 6b_4 + 5b_6),\\
m_3 &= (4a_2 + a_0 + 3a_3 + 3a_4 + a_5)(4b_2 + b_0 + 3b_3 + 3b_4 + b_5),\\
m_4 &= (a_1 + 4a_2 + a_0 + 2a_3 + 4a_4 + 6a_5 + a_6)(b_1 + 4b_2 + b_0 + 2b_3 + 4b_4 + 6b_5 + b_6),\\
m_5 &= (5a_1 + 4a_2 + a_0 + 4a_3 + 3a_4 + 2a_5 + a_6)(5b_1 + 4b_2 + b_0 + 4b_3 + 3b_4 + 2b_5 + b_6),\\
m_6 &= (3a_1 + 3a_2 + a_0 + 2a_4 + 2a_5 + 3a_6)(3b_1 + 3b_2 + b_0 + 2b_4 + 2b_5 + 3b_6),\\
m_7 &= (a_1 + 3a_2 + a_0 + a_3 + 2a_4 + 6a_5 + 2a_6)(b_1 + 3b_2 + b_0 + b_3 + 2b_4 + 6b_5 + 2b_6),\\
m_8 &= (4a_1 + a_2 + a_0 + 6a_3 + 2a_5 + 3a_6)(4b_1 + b_2 + b_0 + 6b_3 + 2b_5 + 3b_6),\\
m_9 &= (4a_1 + a_2 + a_0 + 6a_3 + a_4 + 5a_5 + 2a_6)(4b_1 + b_2 + b_0 + 6b_3 + b_4 + 5b_5 + 2b_6),\\
m_{10} &= (2a_3 + 3a_4 + 3a_5 + 3a_6)(b_0 + 5b_1 + 6b_2 + 6b_3 + 4b_4 + 6b_5),\\
m_{11} &= (a_0 + 5a_1 + 6a_2 + 6a_3 + 4a_4 + 6a_5)(2b_3 + 3b_4 + 3b_5 + 3b_6),\\
m_{12} &= (a_2 + a_0 + a_3 + 5a_4 + 3a_5 + a_6)(b_2 + b_0 + b_3 + 5b_4 + 3b_5 + b_6),\\
m_{13} &= (5a_1 + 4a_2 + a_0 + 3a_4 + 5a_5 + a_6)(5b_1 + 4b_2 + b_0 + 3b_4 + 5b_5 + b_6),\\
m_{14} &= (a_0 + 5a_1 + 6a_2 + 6a_3 + 4a_4 + 6a_5)(b_0 + 5b_1 + 6b_2 + 6b_3 + 4b_4 + 6b_5),\\
m_{15} &= (6a_1 + 3a_2 + a_0 + 5a_3 + 4a_4 + 2a_5 + 3a_6)(6b_1 + 3b_2 + b_0 + 5b_3 + 4b_4 + 2b_5 + 3b_6).
\end{aligned}
$$

References

[1] E. Lee, H. Lee, Y. Lee, Eta pairing computation on general divisors over hyperelliptic curves $y^2 = x^p - x + d$, Journal of Symbolic Computation (43) (2008) 452–474.
[2] A. Karatsuba, Y. Ofman, Multiplication of multidigit numbers by automata, Soviet Physics-Doklady (7) (1963) 595–596.
[3] A. Weimerskirch, C. Paar, Generalizations of the Karatsuba algorithm for polynomial multiplication. http://eprint.iacr.org/2006/224.
[4] M. Cenk, F. Özbudak, Efficient multiplication in finite fields of characteristic 3 and 5 for pairing based cryptography, in: 3rd Information Security and Cryptology Conference, Ankara, 2008, pp. 111–114.
[5] M. Cenk, Ç.K. Koç, F. Özbudak, Polynomial multiplication over finite fields using field extensions and interpolation, in: Proceedings, 19th IEEE Symposium on Computer Arithmetic, Portland, Oregon, June 8–10, 2009.
[6] N. Arnaud, Evaluation Dérivée, Multiplication dans les Corps finis et codes correcteurs, Ph.D. Dissertation, Université de la Méditerranée, France, 2006.

[7] S. Ballet, On the tensor rank of the multiplication in the finite fields, Journal of Number Theory 128 (2008) 1795–1806.
[8] M. Cenk, F. Özbudak, Efficient multiplication in $\mathbb{F}_{3^{\ell m}}$, $m \geq 1$ and $5 \leq \ell \leq 18$, in: Africacrypt, in: Lecture Notes in Computer Science, vol. 5023, Springer-Verlag, 2008, pp. 406–414.
[9] M. Cenk, F. Özbudak, Improved polynomial multiplication formulae over $\mathbb{F}_2$ using Chinese remainder theorem, IEEE Transactions on Computers 58 (4) (2009) 572–576.
[10] M. Cenk, F. Özbudak, On multiplication in finite fields, Journal of Complexity 26 (2) (2010) 172–186.
[11] H. Fan, M.A. Hasan, Comments on five, six, and seven-term Karatsuba-formulae, IEEE Transactions on Computers 56 (5) (2007) 716–717.
[12] P.L. Montgomery, Five, six, and seven-term Karatsuba-like formulae, IEEE Transactions on Computers 54 (3) (2005) 362–369.
[13] B. Sunar, A generalized method for constructing subquadratic complexity $GF(2^k)$ multipliers, IEEE Transactions on Computers 53 (9) (2004) 1097–1105.
[14] S. Winograd, Arithmetic Complexity of Computations, SIAM, 1980.
[15] M. Cenk, F. Özbudak, Multiplication of polynomials modulo x^n, Theoretical Computer Science 412 (29) (2011) 3451–3462.
[16] H. Stichtenoth, Algebraic Function Fields and Codes, Springer, Berlin, 1993.
[17] W. Bosma, J. Cannon, C. CPlayoust, The Magma algebra system I. The user language, Journal of Symbolic Computation 24 (3–4) (1997) 235–265.