Acceleration of the Elliptic Cryptography with Vector Finite Fields

Nikolay A. Moldovyan
Specialized Center of Program Systems "SPECTR"
Kantemirovskaya, 10, St-Petersburg 197342, Russia (Email: spectrz@mail.ru)

(Received Oct. 16, 2008; revised and accepted Feb. 9, 2009)

Abstract

Special form of finite fields (FFs), called vector FFs (VFFs), is defined in the vector spaces over the ground finite field $GF(p)$ using particular types of the multiplication operation over vectors. Implementation of the cryptographic algorisms based on elliptic curves (ECs) over VFFs provides significantly higher performance than the implementation of the EC-based algorithms, in which the ECs are defined over the ground fields and extension finite fields of polynomials.

Keywords: Digital signature, elliptic curve, finite field, finite vector field

1 Introduction

The most computationally efficient digital signature (DS) algorithms are based on elliptic curves (ECs) over finite fields [6, 9]. The well known DS standards ECDSA [5] and GOST R 34.10-2001 [4] specify EC-based algorithms over the ground fields $GF(p)$. However in many cases of the practical use of DS algorithms there are required the DS schemes providing higher performance in hardware and in software. To meet such requirements there have been proposed different approaches to accelerated the EC-based cryptographic algorithms [7, 8]. These approaches can be categorized into two groups: i) high-level algorithm that manage the ECs selection and ii) low-level algorithm that manage the finite field operation. Especially much attention in these researches is paid to the EC-based algorithms implementation using the finite fields $GF(2^m)$, $GF((2^m)^s)$, and $GF(p^m)$, because of their efficiency in hardware implementation [1, 2, 3].

This paper proposes another approach to acceleration of the EC-based cryptographic algorithms. The new approach consists in implementing the ECs using new form of the extension fields $GF(p^m)$ [10], which provides higher computational efficiency of the multiplication in the finite field and efficacy of the parallelization of the multiplication operation.

In second section, using so called expansion coefficients we introduce special type of the multiplication operation in the finite m-dimension vector space defined over the ground field $GF(p)$. It is shown theoretically that in cases $m = 2$ and $m = 3$ one can select the prime values p and the expansion coefficients such that the fields $GF(p^m)$ are formed. Section 3 extends the conditions of the vector finite fields formation to values $m > 3$ and illustrates with computational experiments that the vector finite fields are formed in the cases $m|p-1$ while the equation $x^m = \tau$, where τ is the expansion coefficient, has no solution in the field $GF(p)$. Section 4 compares computational efficiency of the field multiplication in the polynomial fields $GF(p^m)$ and vector fields $GF(p^m)$. Section 5 concludes the paper.

In the paper the following specific term is used: *The* k*th-power element in some finite field* $GF(p^d)$, where $d \geq 1$, is an element $a \in GF(p^d)$ for which the equation $x^k = a$ has solutions in $GF(p^d)$.

2 Finite Fields in Vector Spaces

2.1 Finite Vector Spaces

Let us consider the set of the m-dimension vectors

$$a\mathbf{e} + b\mathbf{i} + \cdots + c\mathbf{z},$$

where $\mathbf{e}$, $\mathbf{i}$, $\ldots$ $\mathbf{z}$ are some formal basis vectors and $a, b, \ldots c \in GF(p)$, are coordinates. Vector can be also represented as a set of its coordinates $(a, b, \ldots, c)$. The terms $\tau\mathbf{v}$, where $\tau \in GF(p)$ and $\mathbf{v} \in \{\mathbf{e}, \mathbf{i}, \ldots, \mathbf{z}\}$, are called components of the vector. The vectors are also denoted as a sequence of their coordinates:

$$a\mathbf{e} + b\mathbf{i} + \cdots + c\mathbf{z} = (a, b, \ldots, c).$$

The addition of two vectors $(a, b, \ldots, c)$ and $(x, y, \ldots w)$ is defined as addition of the coordinates corresponding to the same basis vector:

$$(a, b, \ldots, c) + (x, y, \ldots, w) = (a + x, b + y, \ldots, c + w).$$

The multiplication of two vectors $(a, b, \ldots, c)$ and $(x, y, \ldots w)$ is defined as pair-wise multiplication of all components of the vectors in correspondence with the following formula

$$\begin{aligned}
& (a\mathbf{e}+b\mathbf{i}+\cdots+c\mathbf{z})\circ(x\mathbf{e}+y\mathbf{i}+\cdots+w\mathbf{z}) \\
= \;& a\mathbf{e}\circ x\mathbf{e}+b\mathbf{i}\circ x\mathbf{e}+\cdots+c\mathbf{z}\circ x\mathbf{e}+a\mathbf{e}\circ y\mathbf{i} \\
& +b\mathbf{i}\circ y\mathbf{i}+\cdots+c\mathbf{z}\circ y\mathbf{i}+\cdots+a\mathbf{e}\circ w\mathbf{z}+b\mathbf{i}\circ w\mathbf{z} \\
& +\cdots+c\mathbf{z}\circ w\mathbf{z} \\
= \;& ax\mathbf{e}\circ\mathbf{e}+bx\mathbf{i}\circ\mathbf{e}+\cdots+cx\mathbf{z}\circ\mathbf{e}+ay\mathbf{e}\circ\mathbf{i} \\
& +by\mathbf{i}\circ\mathbf{i}+\cdots+cy\mathbf{z}\circ\mathbf{i}+\cdots+aw\mathbf{e}\circ\mathbf{z} \\
& +bw\mathbf{i}\circ\mathbf{z}+\cdots+cw\mathbf{z}\circ\mathbf{z},
\end{aligned}$$

where $\circ$ denotes the vector multiplication operation. In the final expression each product of two basis vectors is to be replaced by some basis vector $\mathbf{v}$ or by a vector $\tau\mathbf{v}$ ($\tau \in GF(p)$) in accordance with some given table called basis-vector multiplication table (BVMT). There exist different variants of the BVMTs that define associative and commutative multiplication of vectors, but in this paper there is used the BVMT of some general type presented by Table 1. For arbitrary values m, $\mu \in GF(p)$, and $\tau \in GF(p)$ Table 1 defines the vector multiplication that is a commutative and associative operation. The coefficients μ and τ in Table 1 are called the expansion coefficients.

2.2 Vector Finite Fields $GF(p^2)$

In the case $m = 2$ the general representation of the BVMT possessing commutativity and associativity can be described as follows

$$\mathbf{e}\circ\mathbf{i}=\mathbf{i}\circ\mathbf{e}=\mathbf{i}, \quad \mathbf{e}\circ\mathbf{e}=\mathbf{e}, \quad \mathbf{i}\circ\mathbf{i}=\tau\mathbf{e},$$

where different values $\tau \in GF(p^d)$ define different variants of the multiplication operation. Each of these variants defines a finite ring of the two-dimension vectors. Let us consider a nonzero element of the vector ring $Z = a\mathbf{e} + b\mathbf{i}$. The element $Z^{-1} = x\mathbf{e} + y\mathbf{i}$ is called inverse of Z, if $Z^{-1}Z = \mathbf{e} = (1, 0)$, where 1 and 0 are the identity and zero elements in $GF(p^d)$. In accordance with the multiplication definition we can write

$$Z^{-1}Z = (ax + \tau by)\mathbf{e} + (bx + ay)\mathbf{i} = 1\mathbf{e} + 0\mathbf{i}.$$

For given (a, b) there exists a pair (x, y) satisfying the last equation, if

$$a^2 - \tau b^2 \neq 0.$$

The last condition holds for all vectors (a, b), except (0,0), if τ is not the second-power element in the field $GF(p)$. In this case the vector space is a field $GF(p^2)$ the multiplicative group of which has the order

$$\Omega = p^2 - 1 = (p - 1)(p + 1).$$

If τ is the second-power element in the field $GF(p)$, then the characteristic equation $a^2 - \tau b^2 = 0$ is satisfied for each value $b \in 1, 2, \ldots, p - 1$ at two different values a. In this case we have a finite group in the vector space, the group order being equal to

$$\Omega = p^2 - 2(p - 1) - 1 = (p - 1)^2.$$

Example 1. *For $p = 1003001$, $\mu = 1$, and $\tau = 3$ (3 is not the second-power element in $GF(1003001)$) the vector $1\mathbf{e} + 2\mathbf{i}$ has the order $\omega = 1006011006000$ and is a primitive element of the multiplicative group of the field $GF(1003001^2)$. For $p = 1003001$, $\mu = 1$, and $\tau = 4$ there is formed the the non-cyclic finite vector group having the order $\Omega = 1006009000000$, in which the vector $1\mathbf{e}+2\mathbf{i}$ has the order $\omega = 1003000$. The last value is the maximum possible order of the elements in this vector group (this fact has been established with computation experiments).*

2.3 Vector Finite Fields $GF(p^3)$

In the case $m = 3$ the general representation of the BVMT possessing commutativity and associativity is shown in Table 2, where $\mu \in GF(p)$ and $\tau \in GF(p)$ are the expansion coefficients. In accordance with the multiplication operation defined by Table 2 for vectors $Z = a\mathbf{e} + b\mathbf{i} + c\mathbf{j}$ and $X = x\mathbf{e} + y\mathbf{i} + w\mathbf{j}$ we can write

$$Z \circ X = (ax + \tau\mu cy + \tau\mu bw)\mathbf{e} + (bx + ay + \mu cw)\mathbf{i}+$$

$$+(cx + \tau by + aw)\mathbf{j} = 1\mathbf{e} + 0\mathbf{i} + 0\mathbf{j}.$$

If the last equation has solution relatively unknown X for all nonzero vectors Z, then the vector space will be a vector finite field $GF(p^{3d})$. From the last equation the following system of equations can be derived

$$\left\{\begin{array}{rcl} ax + \tau\mu cy + \tau\mu bw & = & 1 \\ bx + ay + \mu cw & = & 0 \\ cx + \tau by + aw & = & 0. \end{array}\right.$$

From this system the following characteristic equation can be get

$$a^3 - 3\tau\mu bc \cdot a + \tau^2\mu b^3 + \tau\mu^2 c^3 = 0 \qquad (1)$$

Let us consider Equation (1) relatively the unknown value a. Denoting $B = (\tau^2\mu b^3 + \tau\mu^2 c^3)/2$ and using the well known formulas [11] for cubic equation roots we get the expression for the Equation (1) roots in the following form

$$a = A' + A'', \quad \text{where,}$$

$$A' = \sqrt[3]{B + \sqrt{B^2 - (\tau\mu bc)^3}} = \sqrt[3]{-\tau\mu^2 c^3},$$

$$A'' = \sqrt[3]{B - \sqrt{B^2 - (\tau\mu bc)^3}} = \sqrt[3]{-\tau^2\mu b^3}.$$

Thus, if both of the values $\tau\mu^2$ and $\tau^2\mu$ are not the third-power elements in the field $GF(p)$, then the characteristic Equation (1) has no solutions relatively unknown a for all possible pairs (b, c), except $(b, c) = (0, 0)$. In this case the vector space is a field $GF(p^3)$. In general the analysis of the characteristic Equation (1) leads to the following cases.

Table 1: The basis-vector multiplication table of the general type

$\circ$	$\overrightarrow{e}$	$\overrightarrow{\imath}$	$\overrightarrow{\jmath}$	$\overrightarrow{k}$	$\overrightarrow{u}$	$\dots$	$\overrightarrow{z}$
$\overrightarrow{e}$	$\mathbf{e}$	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$	$\mathbf{u}$	$\dots$	$\mathbf{z}$
$\overrightarrow{\imath}$	$\mathbf{i}$	$\tau\mathbf{j}$	$\tau\mathbf{k}$	$\tau\mathbf{u}$	$\tau\dots$	$\tau\mathbf{z}$	$\tau\mu\mathbf{e}$
$\overrightarrow{\jmath}$	$\mathbf{j}$	$\tau\mathbf{k}$	$\tau\mathbf{u}$	$\tau\dots$	$\tau\mathbf{z}$	$\tau\mu\mathbf{e}$	$\mu\mathbf{i}$
$\overrightarrow{k}$	$\mathbf{k}$	$\tau\mathbf{u}$	$\tau\dots$	$\tau\mathbf{z}$	$\tau\mu\mathbf{e}$	$\mu\mathbf{i}$	$\mu\mathbf{j}$
$\overrightarrow{u}$	$\mathbf{u}$	$\tau\dots$	$\tau\mathbf{z}$	$\tau\mu\mathbf{e}$	$\mu\mathbf{i}$	$\mu\mathbf{j}$	$\mu\mathbf{k}$
$\dots$	$\dots$	$\tau\mathbf{z}$	$\tau\mu\mathbf{e}$	$\mu\mathbf{i}$	$\mu\mathbf{j}$	$\mu\mathbf{k}$	$\mu\mathbf{u}$
$\overrightarrow{z}$	$\mathbf{z}$	$\tau\mu\mathbf{e}$	$\mu\mathbf{i}$	$\mu\mathbf{j}$	$\mu\mathbf{k}$	$\mu\mathbf{u}$	$\mu\dots$

Table 2: The BVMT in the general case for $m = 3$

$\circ$	$\overrightarrow{e}$	$\overrightarrow{\imath}$	$\overrightarrow{\jmath}$
$\overrightarrow{e}$	$\mathbf{e}$	$\mathbf{i}$	$\mathbf{j}$
$\overrightarrow{\imath}$	$\mathbf{i}$	$\tau\mathbf{j}$	$\mu\tau\mathbf{e}$
$\overrightarrow{\jmath}$	$\mathbf{j}$	$\mu\tau\mathbf{e}$	$\mu\mathbf{i}$

Case 1. The value p is such that 3 does not divide $p-1$. Then each nonzero element of the field $GF(p)$ is the cubic residue and only for $\Omega = (p-1)^2(p+1)$ different vectors there exist inverses and we have non-cyclic finite vector group having order Ω. Experiment has shown the maximum vector order is $\omega_{max} = (p-1)(p+1)$ (the fact due to computational experiments). In this case the finite vector spaces are not fields.

Case 2. The value p is such that $3|p-1$. This case is divided into the following two cases.

Case 2a. Each of the products $\tau^2\mu$ and $\tau\mu^2$ is a cubic non-residue in the field $GF(p)$. Then for each nonzero vector Z there exists its inverses and the vector space is a field $GF(p^3)$ multiplicative group of which has the order

$$\Omega = p^3 - 1 = (p-1)(p^2+p+1).$$

Selecting properly the prime value p one can get prime $q|\Omega$ such that $q = \frac{1}{3}(p^2+p+1)$. Thus, in the case of the field formation in the finite vector spaces it is possible to get vector subgroups of the prime order that has the size that is significantly larger that the size of the $GF(p)$ field order. Such cases are very interesting for designing fast DS algorithms based on using the finite groups in vector spaces.

Case 2b. Each of the products $\tau^2\mu$ and $\tau\mu^2$ is a cubic residue in the field $GF(p)$. In this case only for $\Omega = (p-1)^3$ different vectors there exist inverses and we have non-cyclic finite vector group having order Ω. The maximum vector order is $\omega_{max} = p-1$ (the experimental fact).

Case 3. For $\tau = 0$ and $\mu \neq 0$ or for $\tau \neq 0$ and $\mu = 0$, or for $\tau = 0$ and $\mu = 0$ we have degenerative case, when the characteristic equation has the form $a^3 \equiv 0 \bmod p$ and unique solution $a = 0$ for all pair of the values (b, c). In this case the vector space contains a vector group of the order $\Omega = p^2(p-1)$. This group is non-cyclic and the maximum vector order is $\omega_{max} = p(p-1) = \Omega/p$ (the experimental fact).

Example 2. *Suppose* $p = 103$ *(i.e.* $3|p-1$*). Then for* $\mu = 1$*, and* $\tau = 0$ *there is formed a vector group of the order* $\Omega = p^2(p-1) = 1082118$*, in which the maximum vector order is* $\omega = p(p-1) = 10506$*. For* $\mu = 1$ *and* $\tau = 2$ *(2 is not the third-power element in* $GF(103)$*) the vector field* $GF(103^3)$ *is formed, in which there exist vectors having order* $\omega = p^3 - 1 = 1092726$ *(for example vector* $1\mathbf{e} + 2\mathbf{i} + 3\mathbf{j}$*). For* $\mu = 1$ *and* $\tau = 23$ *(23 is the third-power element in* $GF(103)$*) there is formed the vector group of the order* $\Omega = (p-1)^3 = 1061208$*, in which the maximum vector order is* $\omega_{max} = p - 1 = 102$*.*

Example 3. *Suppose* $p = 636333488554432197$ *(i.e. 3 does not divide* $p-1$*). Then for* $\mu = 1$ *and* $\tau = 3$ *there is formed the vector finite group having the order value* $\Omega = (p-1)^2(p+1)$*. All vectors of this group have order* $\omega \leq \omega_{max} = (p-1)(p+1) = 4049203086557134095975355664246808$*.*

Example 4. *Suppose* $p = 10032608122899198367$*, where* $3|p-1$*. Then for* $\mu = 1$ *and* $\tau = 3$ *(3 is not the third-power element in the field* $GF(p)$*) there is formed a vector field* $GF(p^3)$*, containing vectors (for example,* $3\mathbf{e} + 5\mathbf{i} + 7\mathbf{j}$*) of the order* $\omega = 1009814370232010317429445111885983558910602162469891696862$*. Such vectors are primitive elements of the vector field* $GF(p^3)$*. Such elements generates the multiplicative group of* $GF(p^3)$*, which has the order* $\Omega = p^3 - 1$*.*

3 Formation of the Vector Finite Fields in the Case $m \geq 4$

Analysis of the cases $m = 2$ and $m = 3$ shows that vector fields are formed in the case $m|p-1$, provided some of the expansion coefficients are not the the mth degree elements in $GF(p)$. We have experimentally established that under such conditions the vector fields are formed for $m = 4, 5, \dots 55$, while defining the vector multiplication operation with the corresponding BVMTs derived as respective particular variants of Table 1 for the each of the indicated values m. The computational experiments has shown that for arbitrary m there exists vector finite fields defined over the field $GF(p)$ such that $m|p-1$. For defining formation of the finite fields of the m-dimension vectors the necessary condition is the use of the expansion coefficients in BVMT, which are not the mth-power elements in $GF(p)$. Let us consider some examples.

Example 5. *For prime* $p = 2609$, *dimension* $m = 4$ $(m|p-1)$, *and coefficients* $\mu = 1$ *and* $\tau = 2222$ *(*τ *is not the 4th-power element in* $GF(2731)$*) the vector* $G_\Omega = 1\mathbf{e}+3\mathbf{i}+3\mathbf{j}+5\mathbf{k}$ *is a generator of the multiplicative group of the vector field* $GF(p^4)$*. The vector* $G_q = 392\mathbf{e} + 2173\mathbf{i} + 2545\mathbf{j} + 443\mathbf{k}$ *is a generator of the cyclic subgroup having prime order* $q = 3403441$.

Example 6. *For prime* $p = 268675256028581$ *and coefficients* $\mu = 1$ *and* $\tau = 3048145277787$ *(*τ *is not the 5th-power element in* $GF(p)$*) the vector* $G_\Omega = 2\mathbf{e} + 5\mathbf{i} + 7\mathbf{j} + 11\mathbf{k} + 13\mathbf{u}$ *is a generator of the multiplicative group of the vector field* $GF(p^5)$*. The vector* $G_\Omega = 88815218764680\mathbf{e} + 238886012231841\mathbf{i} + 157317400153847\mathbf{j} + 215935132\ 18048\mathbf{k} + 204824491909450\mathbf{u}$ *is a generator of the qth order cyclic subgroup, where* $q = 104217507270343426\ 574520347813472921450310523418174019396\,1$ *is a prime.*

Example 7. *For prime* $p = 29$, *dimension* $m = 7$ $(7|p-1)$, *and coefficient* $\epsilon = 3$ *(*ϵ *is not the 7th-power element in* $GF(29)$*) the vector* $G_\Omega = (1, 3, 7, 5, 3, 1, 4)$ *is a generator of the multiplicative group of the VFF* $GF(p^7)$*. The vector* $G_q = (7, 10, 0, 3, 15, 14, 22)$ *is a generator of the subgroup having prime order* $q = 88009573$.

Table 3 presents some other cases of the vector field formation.

Table 3: Parameters m, p, μ, and τ defining formation of the vector fields $GF(p^m)$

m	p	μ	τ
8	2436749489	1	3
11	8419049	1	2
16	8021873	1	2
29	59509	1	2
32	65537	3	1
41	83	2	1
53	107	2	1

4 Vector Finite Fields over Fields $GF(p^s)$

Let us consider the case of the finite vector space defined over the finite fields $GF(p^s)$, where $s \geq 2$. For example the fields $GF(p^s)$ can be represented by the finite polynomial fields. In the cases of two-dimension and three-dimension vector spaces it is easy to derive theoretically (like it is performed in Section 2) that vector fields $GF\left((p^s)^m\right)$ are formed, if $m|p^s-1$ and one of the expansion coefficients in Table 1 is not the mth-power element in the field $GF(p^s)$. Theoretic consideration of the cases $m \geq 4$ is not so evident (as it is in the cases $m = 2$ and $m = 3$), therefore we have experimentally investigated such cases. Like in the case of vectors defined over the ground field $GF(p)$, we have established that in the case $m|p^s - 1$ the vector finite fields $GF\left((p^s)^m\right)$ are formed for the dimension values $m = 4, 5, \ldots 55$, while respective expansion coefficients are used. Let us consider some examples, where the finite polynomial fields $GF(p^s)$ are defined with the irreducible polynomials $P(x)$ of the degree s and the vector multiplication operation is defined with Table 1 in which the expansion coefficients are polynomials $\mu = M(x) = 1$ and $\tau = T(x)$, where $T(x)$ is not the mth-power element in $GF(p^s)$.

Example 8. *For* $m = 2$, $p = 13$, $P(x) = x^2 + 9x + 2$ $(m|p^s - 1)$, *and* $T(x) = 7x + 11$ *there is formed the vector field* $GF\left((13^2)^2\right)$*. The vector* $G = (3x + 7)\mathbf{e} + (x + 5)\mathbf{i}$ *having the order* $\omega = 28560$ *is generator of the multiplicative group of the field.*

Example 9. *For* $m = 3$, $p = 7$, $P(x) = x^2 + 6x + 3$ $(m|p^s - 1)$, *and* $T(x) = 5x + 2$ *there is formed the vector field* $GF\left((7^2)^3\right)$*. The vector* $G = (3x + 2)\mathbf{e} + (x + 5)\mathbf{i}$ *having the order* $\omega = 117648$ *is generator of the multiplicative group of the field.*

Example 10. *For* $m = 5$, $p = 2$, $P(x) = 101111011 = x^8+x^6+x^5+x^4+x^3+x+1$ $(m|p^s-1)$, *and* $T(x) = x^3+1$ *there is formed the vector field* $GF\left((2^8)^5\right)$*. The vector* $G = (x^4 + 1)\mathbf{e} + (x^4 + x^2 + 1)\mathbf{i} + (x^6 + x^5 + x^2 + x + 1)\mathbf{j} + (x^5+1)\mathbf{k}+(x^4+1)\mathbf{u}$ *having the order* $\omega = 1099511627775$ *is generator of the multiplicative group of the field.*

Example 11. *For* $m = 5$, $p = 2$, $P(x) = x^{32}+x^{31}+\cdots+1 = 111101010100001110001100111010111$ $(m|p^s - 1)$, *and* $T(x) = x + 1$ *there is formed the vector field* $GF\left((2^{32})^5\right)$*. The vector* $G = (x^4 + 1)\mathbf{e} + (x^4 + x^3 + x + 1)\mathbf{i} + (x^6 + x^5 + x^2 + 1)\mathbf{j} + (x^5 + 1)\mathbf{k} + (x^4 + 1)\mathbf{u}$ *having the order* $\omega = 1461501637330902918203684832716283019655932542975$ *is a generator of the multiplicative group of the field.*

Example 12. *For* $m = 8$, $p = 233$, $P(x) = x^3 + 179x^2 + 13x + 81 = (m|p^s - 1)$, *and* $T(x) = x + 1$ *there is formed the vector field* $GF\left((233^3)^8\right)$*. The vector* $G = (3x^2 + 7x + 1,\ 3x + 3,\ x + 2,\ x^2 + 2x + 1,\ x+5,\ 71x+1,\ 17x+1,\ 11x^2+7x+1)$ *having the order* $\omega = 655453828661462718740867094804609871011228021078182589120$ *is generator of the multiplicative group of the field* $(\omega = \Omega = p^{ms} - 1)$.

5 Comparison of the Computational Efficacy of the Multiplication in Different Finite Fields

Performance of the DS algorithms based on computations on ECs is inversely proportional to the difficulty of the point addition operation that is defined mainly by several field multiplications and one inversion operation in the finite field over which the ECs are defined. The inversion is the most contributing to the difficulty of the point addition operation. Even though there are some special techniques for computing inverses in the finite field, inversion is still far more expensive than the field multiplication. The inverse operation needed when adding two points can be eliminated by resorting to projective coordinates [8]. In this way adding two points is performed with about ten field multiplications. Thus, the difficulty of the multiplication in the underlying field defines difficulty of the point addition operation.

The vector finite fields $GF(p^m)$ defined over the ground field $GF(p)$ can be applied to design the EC-based cryptographic algorithms providing significantly higher performance. Indeed, in known EC-based algorithms one can replace the underlying field by the respective vector finite field. For different values $m \in \{2, 3, 4 \dots\}$ it is easy to generate ECs the order of which contains large prime factor q such that $|q| \approx m|p|$, where $|q|$ is the bit size of q. While comparing the computational efficiency of the multiplication operation in different fields one should consider the case of the approximately equal values of the field order. Let us compare the difficulty of the multiplication operation in the ground field $GF(p)$ and in the vector extension fields $GF(p_v^m)$ for different values m in the case $|p| = m|p_v|$.

Multiplication in $GF(p)$ is performed with arithmetic multiplication of two $|p|$-bit values and arithmetic division of some $2|p|$-bit value by some $|p|$-bit value. Multiplication in the vector field $GF(p_v^m)$ is performed with m^2 arithmetic multiplications of two $|p_v|$-bit values and m arithmetic divisions of some $2|p_v|$-bit values by some $|p_v|$-bit values (because of sufficiently low difficulty we do not take into account the arithmetic additions and $m^2/2$ multiplications with expansion coefficients having usually the size of two bits). Taking into account that difficulty of the both arithmetic multiplication and arithmetic division is proportional to the squared size of operands one can easily derive the following formula

$$\rho = \frac{W_{GF(p)}}{W_{GF(p_v^m)}} = \frac{m(1+c)}{m+c},$$

where $W_{GF(p)} \quad \left(W_{GF(p_v^m)}\right)$ is the computational difficulty of the multiplication in $GF(p) \quad (GF(p_v^m))$ and c is the ratio of the arithmetic division difficulty to the arithmetic multiplication difficulty. The value c depends on the hardware used to perform computations. For many types of micro-controllers and microprocessors we have $c > 5$. For example, in this case for $m = 5$ and $c = 6$ $(c = 12)$ we have $\rho \approx 3.2 \;\; (\rho \approx 3.8)$.

Analogous consideration of the computational efficacy of the multiplication in polynomial and vector fields gives the ratio $\rho \geq 2$. The lower multiplication efficacy in the polynomial fields is connected with the division operation of the $2s$-power polynomials by the s-power irreducible polynomial, which is additionally required to multiplications and additions in the ground field $GF(p)$ over which the polynomial field is defined.

Thus, using elliptic curves over vector finite fields one can design the DS algorithms possessing significantly higher performance. Besides, the multiplication in the vector field $GF(p_v^m)$ suites well to cheap parallelization while being implemented in hardware. This is also a significant resource for additional acceleration of the EC-based cryptography.

6 Conclusion

A new form of the finite extension fields have been proposed to accelerate the EC-based cryptographic algorithms. The proposed vector finite fields $GF(p^m)$ are formed in the m-dimension vector space over the ground field $GF(p)$, while special types of the vector multiplication operation is defined. A general type of the BVMT tables that provides the required types of the vector multiplication is proposed. However for any given value m there are possible some other particular types of the BVMTs with which the vector finite fields can be defined. For even values m one can propose the BVMTs with significantly reduced number of the expansion coefficients. For example, such BVMTs are interesting for software implementation of the vector multiplication operations. For hardware implementation it is preferable to select the small size expansion coefficients with which the vector fields are defined.

It has been also shown that the vector fields can be defined in the m-dimension vector spaces over the finite extension fields $GF(p^s)$ represented, for example, by polynomials. Such cases are also interesting for EC-based cryptography.

It should be noted that, besides using the vector fields to define ECs, the finite groups formed in the m-dimension vector spaces over the ground field $GF(p)$ or over the extension fields $GF(p^s)$ represent independent interest, however this is a topic of individual research.

Acknowledgments

The work supported by Russian Foundation for Basic Research grant # 08-07-00096-a.

References

[1] G. B. Agnew, T. Beth, R. C. Mullin, and S. A. Vanstone, “Arithmetic operations in $GF(2^m)$”, *Journal of Cryptology*, vol. 6, pp. 3-13, 1993.

[2] G. B. Agnew, R. C. Mullin, I. M. Onyszchuk, and S. A. Vanstone, “An implementation for a fast public key cryptosystem, *Journal of Cryptology*, vol. 3, pp. 63-79, 1991.

[3] G. B. Agnew, R. C. Mullin, and S. A. Vanstone, “An implementation of elliptic curve cryptosystems over $\mathbb{F}_{2^{155}}$, *IEEE Journal on Selected Areas in Communications*, vol. 11, no. 5, pp. 804-813, 1993.

[4] GOST R 34.10-2001, *Russian Federation Standard*, Information Technology. Cryptographic data Security. Produce and check procedures of Electronic Digital Signature, Government Committee of the Russia for Standards, 2001 (in Russian).

[5] International Standard ISO/IEC 14888-3:2006(E), *Information Technology – Security Techniques – Digital Signatures with Appendix – Part 3: Discrete Logarithm Based Mechanisms*, 2006.

[6] N. Koblitz, “Elliptic curve cryptosystems”, *Mathematics of Computation Advances*, vol. 48, pp. 203-209, 1987.

[7] J. Lee, H. Kim, Y. Lee, S.-M. Hong, H. Yoon. “Parallelized scalar multiplication on elliptic curves defined over optimal extension field”, *Iinternational Journal of Network Security*, vol. 4, no. 1, pp. 99-106, 2007.

[8] A. J. Menezes and S. A. Vanstone, “Elliptic curve cryptosystems and their implementation”, *Journal of Cryptology*, vol. 6, no. 4, pp. 209-224, 1993.

[9] V. Miller. “Use of elliptic curves in cryptography”, *Advances in Cryptology: Proceedings of Crypto’85*, LNCS 218, Springer-Verlag, pp. 417-426, 1986.

[10] N.A. Moldovyan, *Method for Generating and Verifying the Digital Signature*, Russian patent application # 2008140403, Oct. 14, 2008.

[11] B. L. van der Waerden, *Algebra*, Springer, Berlin, 1971.

Nikolay A. Moldovyan is an honored inventor of Russian Federation (2002), a chief researcher with the Specialized Center of Program Systems ”SPECTR”, and a Professor with the Saint Petersburg Electrical Engineering University. His research interests include computer security and cryptography. He has authored or co-authored more than 50 inventions and 210 scientific articles, books, and reports. He received his Ph.D. from the Academy of Sciences of Moldova (1981). Contact him at: spectrz@mail.ru.