Quasigroups and Related Systems **17** (2009), 271 – 282

New primitives for digital signature algorithms

Nikolay A. Moldovyan and Peter A. Moldovyanu

Abstract. Particular types of the multiplication operation over elements of the finite vector space over the field $GF(p^d)$, $d \geqslant 1$, are introduced so that there are formed the finite fields $GF\left((p^d)^m\right)$ with fast multiplication operation that also suites well to parallelized implementation. Finite fields implemented in such form are proposed for accelerating the digital signature algorithms.

1. Introduction

The finite fields (FFs) $GF(p)$ and $GF(p^d)$ represented by rings Z_p, where p is a prime, and polynomials, correspondingly, are well studied as primitives for the digital signature (DS) algorithms design [8, 11, 13].

Finding discrete logarithm (DL) in a subgroup of the multiplicative group of the FF is used as the hard computational problem put into the base of the DS algorithms (DSAs).

The upper security boundary of such DSAs is limited by the difficulty of the DL problem in the used FF. There are known the general-purpose methods for solving the DL, which work in arbitrary groups [8]. Such methods have exponential complexity $W = O(\sqrt{q})$, where $O(\cdot)$ is the order notation, and q is the largest prime divisor of the group order. If $q \geqslant 2^{160}$, then the general methods are impracticable, i.e., computationally infeasible. However in the case of the mentioned above FFs some particular methods for solving the DL problem can be applied, which have sub-exponential complexity.

Therefore the DSAs based on computations in the ground FFs $GF(p)$ and in the polynomial FFs fields $GF(p^d)$ satisfy the minimum security requirement (difficulty of the best attack should be equal to $\geqslant 2^{80}$ exponentiation operations in the used FF), if the size of the FF order is greater or equal to 1024 bits [4]. This fact restricts significantly the performance of

2000 Mathematics Subject Classification: 11G20, 11T71
Keywords: Cryptography, digital signature, vector space, finite field.

the known DSAs based on computations in the FFs $GF(p)$ and $GF(p^d)$. Higher performance is provided by the DSA using the computations in the finite groups of the elliptic curve (EC) points, while the EC are defined over FFs the size order of which equals 160 to 320 bits [5, 9].

The complexity of the point addition operation is defined by the complexity of the multiplication operation in the underlying FF. However in many cases of the practical use of DSAs 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 accelerating the EC-based cryptographic algorithms [9, 7].

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 FF operation. Especially much attention in these researches is paid to the EC-based algorithms implementation using the FFs $GF(2^d)$, $GF\left(\left(2^d\right)^s\right)$, and $GF(p^d)$, because of their efficiency in hardware implementation [1, 2, 3].

However in the both approaches few attention is paid to accelerating the EC-based DSAs with parallelization of the multiplication in the underlying FF. Actually, in these approaches there are used the ground or polynomial FFs in which the multiplication operation involves arithmetic division by a prime or by an irreducible polynomial, respectively.

In present paper it is proposed a particular form of the FFs implementation, called vector FFs, providing possibility of efficient parallelization of the multiplication operation.

Besides, in the proposed particular form of the extension FFs $GF(p^{m'})$ the multiplication complexity is lower than in the ground FFs $GF(p')$ and in polynomial FFs $GF(p^d)$ for the same size of the FF order. The vector FFs are proposed to implement ECs providing faster DSAs.

The rest of the paper is organized as follows. In Section 2, the multiplication operation in the finite vector spaces over the FFs $GF(p^d)$ is defined using so called basis vector multiplication tables (BVMTs). This particular method allows one to define only a particular subclass of all possible variants of the associative multiplication. However this subclass includes the multiplication variants for which the vector space represents a field.

Section 3 provides comparison of the computational efficacy of the multiplication operation in FFs implemented in different forms. Section 4 concludes the paper.

In the paper the following specific term is used:

The *k-th power element a of the field* $GF(p^d)$ is an element of the field $GF(p^d)$ for which the equation $x^k = a$ has solutions in the field $GF(p^d)$, $d \geqslant 1$.

2. Extension of finite fields in the vector form

The vector form of the extension FFs implementation represents significant interest for the applied cryptography due to lower complexity of the multiplication and possibility to efficient parallelization. This form of the implementation of the extension FFs is introduced using some subclass of possible associative multiplications in finite vector spaces over the FF $GF(p^d)$, where $d \geqslant 1$. The multiplication operation is introduced with BVMT.

This particular method is sufficiently simple and provides possibility to define vector FFs $GF\left((p^d)^m\right)$ for arbitrary value of m.

The vector FFs can be defined with BVMT not for all possible triples m, p, and d, though. However the proposed method suites well for defining the vector FFs oriented to application in the applied cryptography.

2.1. Addition and multiplication operations in finite vector spaces

Let us consider the set of the m-dimension vectors

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

where $\mathbf{e}, \mathbf{i}, \ldots \mathbf{j}$ are some formal basis vectors and $a, b, \ldots c \in GF(p^d)$, $d \geqslant 1$, are coordinates. Vector can be also represented as a set of its coordinates $(a, b, \ldots, c)$.

The terms $\epsilon\mathbf{v}$, where $\epsilon \in GF(p^d)$ and $\mathbf{v} \in \{\mathbf{e}, \mathbf{i}, \ldots, \mathbf{j}\}$, are called components of the vector.

The addition of two vectors $(a, b, \ldots, c)$ and $(x, y, \ldots, z)$ is defined in the usual way as follows

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

where "+" denotes addition operation in the field $GF(p^d)$. It is easy to see that the first representation of the vectors can be interpreted as sum of the vector components.

The multiplication of the vectors $(a, b, \ldots, c)$ and $(x, y, \ldots, z)$ is defined analogously to multiplication of polynomials, i.e., it is defined with the formula

$$\begin{gathered}(a\mathbf{e} + b\mathbf{i} + \cdots + c\mathbf{j}) \cdot (x\mathbf{e} + y\mathbf{i} + \cdots + z\mathbf{j}) = \\ = ax\mathbf{e}\cdot\mathbf{e} + bx\mathbf{i}\cdot\mathbf{e} + \cdots + cx\mathbf{j}\cdot\mathbf{e} + ay\mathbf{e}\cdot\mathbf{i} + by\mathbf{i}\cdot\mathbf{i} + \cdots + cy\mathbf{j}\cdot\mathbf{i} + \ldots \\ \cdots + az\mathbf{e}\cdot\mathbf{j} + bz\mathbf{i}\cdot\mathbf{j} + \cdots + cz\mathbf{j}\cdot\mathbf{j},\end{gathered}$$

where gh denotes multiplication of the elements $g \in GF(p^d)$ and $h \in GF(p^d)$. See [12] for more details.

In the final expression each product of two basis vectors is replaced by a vector component $\epsilon\mathbf{v}$ ($\epsilon \in GF(p^d)$) in accordance with some given tables called basis-vector multiplication tables (BVMT).

For example, if the used BVMT defines $\mathbf{i}\cdot\mathbf{j} = \epsilon\mathbf{e}$, then $bz\mathbf{i}\cdot\mathbf{j} = \epsilon bz\mathbf{e}$. The coordinate ϵ is called the expansion coefficient. The BVMT defines the concrete variant of the multiplication in the finite vector space.

It is easy to see, if the BVMT defines commutative and associative multiplication of the basis vectors, then the multiplication in the finite vector space is also commutative and associative. In this case the finite vector space is a commutative ring. In some particular cases the finite vector rings are FFs $GF\left((p^d)^m\right)$, called vector FFs.

Below there are shown constructions of the vector FFs for diffrent values m. For the case $m = 2$ the construction of the vector FF $GF\left((p^d)^2\right)$ is sufficiently close to construction with attaching the root of the irreducible (in $GF(p^d)$) polynomial $x^2 - \epsilon$ to $GF(p^d)$.

Principally for all values m the FFs $GF\left((p^d)^m\right)$ can be constructed with the well known method using irreducible polynomials in $GF(p^d)$, however this method constructs the extension FFs $GF\left((p^d)^m\right)$ as polynomial FFs in which the multiplication operation is more complex and suites less to parallelized implementation than multiplication in the FFs constructed with BVMTs.

Indeed, in the polynomial FFs the multiplication is performed as arithmetic multiplication of two polynomials and arithmetic division of the result by the irreducible polynomial, while the multiplication in the vector FFs is free of such division operation.

Actually, the BVMT-based construction method is less general, however it provides efficient and immediate practical way to construct vector FFs with fast multiplication for arbitrary values m.

2.2. Vector finite fields $GF\left((p^d)^2\right)$

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

$$\mathbf{e} \cdot \mathbf{i} = \mathbf{i} \cdot \mathbf{e} = \mathbf{i}, \quad \mathbf{e} \cdot \mathbf{e} = \mathbf{e}, \quad \mathbf{i} \cdot \mathbf{i} = \epsilon \mathbf{e},$$

where different values $\epsilon \in GF(p^d)$ define different variants of the multiplication operation. Each of these variants defines a finite ring of the two-dimension vectors. See, also, [12].

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

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

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

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

The last condition holds for all vectors (a, b), except (0,0), if ϵ is a quadratic non-residue in the field $GF(p^d)$. In this case the vector space is a field $GF\left((p^d)^m\right)$.

If the vector space is defined over a ground field $GF(p)$, then we have the vector finite field $GF(p^2)$ the multiplicative group of which has the order $\Omega = p^2 - 1 = (p - 1)(p + 1)$.

If ϵ is a quadratic residue in the field $GF(p^d)$, where $d = 1$, then the characteristic equation $a^2 - \epsilon b^2 = 0$ 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 is equal to

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

Example 1. For $p = 101$ and $\epsilon = 32$ (quadratic non-residue mod 101) the vector $93\mathbf{e} + 24\mathbf{i}$ has the order $\omega = 10200$ and is a primitive element of the multiplicative group of the field $GF(101^2)$. For $p = 101$ and $\epsilon = 31$ (quadratic residue mod 101) the vector $2\mathbf{e} + 3\mathbf{i}$ has the order $\omega = 100$, the last value being the maximum possible element order in the non-cyclic finite vector group having the order $\Omega = 10000$.

2.3. Vector finite fields $GF\left((p^d)^3\right)$

In the case $m = 3$ the general representation of the BVMT possessing commutativity and associativity is shown in Table 1, where $\mu \in GF(p^d)$ and $\epsilon \in GF(p^d)$ are the expansion coefficients. In accordance with the multiplication operation defined by Table 1 for vectors $Z = a\mathbf{e} + b\mathbf{i} + c\mathbf{k}$ and $X = x\mathbf{e} + y\mathbf{i} + z\mathbf{k}$ we can write

$$ZX = (ax+\epsilon\mu cy+\epsilon\mu bz)\mathbf{e}+(bx+ay+\mu cz)\mathbf{i}+(cx+\epsilon by+az)\mathbf{j} = 1\mathbf{e}+0\mathbf{i}+0\mathbf{j}.$$

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

$$\begin{cases} ax + \epsilon\mu cy + \epsilon\mu bz &= 1 \\ bx + ay + \mu cz &= 0 \\ cx + \epsilon by + az &= 0. \end{cases}$$

From this system the following characteristic equation can be get

$$a^3 - (3\epsilon\mu bc)\, a + \left(\epsilon^2\mu b^3 + \epsilon\mu^2 c^3\right) = 0 \qquad (1)$$

Denoting $B = (\epsilon^2\mu b^3 + \epsilon\mu^2 c^3)/2$ and using the well known formulas [6] for cubic equation roots we get the expression for the equation (1) roots a in the following form

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

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

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

Thus, if both of the values $\epsilon\mu^2$ and $\epsilon^2\mu$ are not the 3rd-power elements in the field $GF(p^d)$, then the characteristic equation (1) has no solutions relatively unknown a for all possible pairs (a, b), except $(a, b) = (0, 0)$. In this case the vector space is a field $GF\left((p^d)^3\right)$.

$\cdot$	$\overrightarrow{e}$	$\overrightarrow{i}$	$\overrightarrow{j}$
$\overrightarrow{e}$	$\mathbf{e}$	$\mathbf{i}$	$\mathbf{j}$
$\overrightarrow{i}$	$\mathbf{i}$	$\epsilon\mathbf{j}$	$\mu\epsilon\mathbf{e}$
$\overrightarrow{j}$	$\mathbf{j}$	$\mu\epsilon\mathbf{e}$	$\mu\mathbf{i}$

Table 1. The BVMT in the general case for $m = 3$.

In the case of the vector space defined over a ground field $GF(p)$ the analysis of the characteristic equation leads to the following cases.

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 3rd-power element 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 $\omega = (p-1)(p+1)$. 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 $\epsilon^2\mu$ and $\epsilon\mu^2$ is not a 3rd-power element 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 $\Omega = p^3 - 1$. 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 significantly larger that the size of the $GF(p)$ field order. Such cases are very interesting for designing fast DSAs.

Case 2b. Each of the products $\epsilon^2\mu$ and $\epsilon\mu^2$ is a 3rd-power element in $GF(p)$. 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 $\Omega = (p-1)$ (experimental result).

Case 3. For $\epsilon = 0$ and $\mu \neq 0$ or for $\epsilon \neq 0$ and $\mu = 0$, or for $\epsilon = 0$ 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 $\Omega = p(p-1)$ (experiment).

Example 2. Suppose $p = 67$ (i.e., $3|p-1$). Then for $\mu = 1$, and $\epsilon = 0$ there is formed a vector group of the order $\Omega = p^2(p-1) = 296274$, in which the maximum vector order is $\omega = p(p-1) = 4422$. For $\mu = 1$ and $\epsilon = 60$ (this value is not the 3rd-power element) the vector field is formed, in which there exist vectors having order $\omega = p^3 - 1 = 300762$. For $\mu = 1$ and $\epsilon = 1$ (this value is the 3rd-power element) there is formed the vector group of the order $\Omega = (p-1)^3 = 287496$, in which the maximum vector order is $\omega = p - 1 = 66$.

Example 3. Suppose $p = 63633348855432197$ (i.e., 3 does not divide $p-1$). Then for $\mu = 1$ and $\epsilon = 3$ there is formed the vector group having

the order $\Omega = (p-1)^2(p+1)$. The maximum vector order is $\omega = (p-1)(p+1) = 40492030865571340959753556642468 08$. For $\mu = 1$ and $\epsilon = 0$ there is formed a vector group having the order $\Omega = p^2(p-1)$, the maximum vector order being $\omega = p(p-1)$.

Example 4. Suppose $p = 16406161737685927$ (i.e., $3|p-1$). Then for $\mu = 1$ and $\epsilon = 3$ (this value is the 3rd-power element) there is formed a vector field $GF(p^3)$, containing vectors of the order equal to $\Omega = p^3 - 1 = 44159176511149200026845377235834409855798616929 82$. Such vectors are primitive elements of the vector field $GF(p^3)$.

2.4. Formation of the vector finite fields in the case $m \geqslant 4$

Analysis of the cases $m = 2$ and $m = 3$ shows that vector fields are formed in the case $m|p^d - 1$, provided some of the expansion coefficients are not the mth-power elements in $GF(p^d)$. In this research it has been experimentally established that under such conditions, while using the BVMTs shown as Table 2 the vector fields are formed for $m = 4, 5, \ldots, 55$, if $m|p^d - 1$ and the equation $x^\tau = \epsilon$ has no solutions in $GF(p^d)$ for each divisor $\tau|m$, $\tau > 1$. It appears that for arbitrary m there exists vector FFs defined over the field $GF(p^d)$ such that $m|p^d - 1$.

Our experiments have been stopped since we have estimated that the investigated cases cover the demands of the practical cryptography. To define formation of the m-dimension vector FF the BVMT should be properly designed and for given m there exist a variety of different BVMTs, but in this paper the simplest variants of BVMTs have been used.

$\cdot$	$\overrightarrow{e}$	$\overrightarrow{i}$	$\overrightarrow{j}$	$\overrightarrow{k}$	$\overrightarrow{u}$	$\ldots$	$\overrightarrow{w}$
$\overrightarrow{e}$	**e**	**i**	**j**	**k**	**u**	$\ldots$	**w**
$\overrightarrow{i}$	**i**	ϵ**j**	ϵ**k**	ϵ**u**	$\epsilon\ldots$	ϵ**w**	ϵ**e**
$\overrightarrow{j}$	**j**	ϵ**k**	ϵ**u**	$\epsilon\ldots$	ϵ**w**	ϵ**e**	**i**
$\overrightarrow{k}$	**k**	ϵ**u**	$\epsilon\ldots$	ϵ**w**	ϵ**e**	**i**	**j**
$\overrightarrow{u}$	**u**	$\epsilon\ldots$	ϵ**w**	ϵ**e**	**i**	**j**	**k**
$\ldots$	$\ldots$	ϵ**w**	ϵ**e**	**i**	**j**	**k**	**u**
$\overrightarrow{w}$	**w**	ϵ**e**	**i**	**j**	**k**	**u**	$\ldots$

Table 2. The used variant of the BVMTs for the cases $m = 4, 5, \ldots, 55$.

Let us consider some examples, where the finite polynomial fields $GF(p^d)$ are defined with the irreducible polynomials $P(x)$ of the degree d and the

vector multiplication operation is defined with Table 2 in which the expansion coefficients are polynomials $\epsilon = \epsilon(x)$, where $\epsilon(x)$ is not the mth-power element in $GF(p^m)$.

Example 5. For prime $p = 268675256028581$ and coefficients $\mu = 1$ and $\epsilon = 3048145277787$ (ϵ is not the 5th-power element) 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 $G_\Omega = 88815218764680\mathbf{e} + 238886012231841\mathbf{i} + 157317400153847\mathbf{j} + 21593513218048\mathbf{k} + 204824491909450\mathbf{u}$ is a generator of the q-th order cyclic subgroup, where
q=1042175072703434265745203478134729214503105234181740193961
is a prime.

Example 6. 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 $\epsilon(x) = x^3 + 1$ 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 7. For $m = 5$, $p = 2$,

$$P(x) = x^{32} + x^{31} + \cdots + 1 = 11110101010000111000110011101011 1$$

($m|p^s - 1$,) and $\epsilon(x) = x + 1$ 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

$$\omega = 14615016373309029182036848327162830196559325429 75$$

is a generator of the multiplicative group of the field.

Example 8. For $m = 8$, $p = 233$, $P(x) = x^3+179x^2+13x+81 = (m|p^s-1)$, and $\epsilon(x) = x + 1$ there is formed the vector field $GF\left((2^{32})^5\right)$. 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 $\omega = 655453828661462718740867094804609871011228021078$ 182589120 is generator of the multiplicative group of the field ($\omega_G = \Omega = p^{ms} - 1$).

3. Comparison of the multiplication complexity in FFs implemented in different forms

Performance of the DSAs 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 [9]. 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 FF in usually used forms by the respective vector FF [10]. For different values $m \in \{2, 3, 4, 5 \dots\}$ 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 FFs one should consider the case of the approximately equal values of the FF 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 $W_{GF(p)}$ $\left(W_{GF(p_v^m)}\right)$ is the computational difficulty of the multiplication in $GF(p)$ $(GF(p_v^m))$ 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 microcontrollers 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 $\rho \geqslant 2$. The lower multiplication efficacy in the polynomial fields is connected with the division operation of the $(2s-2)$-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 FFs 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.

4. Conclusions

A new form of the extension FFs have been proposed to accelerate the EC-based cryptographic algorithms. The proposed vector FFs $GF\left((p^d)^m\right)$, $d \geqslant 1$, are formed in the m-dimension vector space over the ground FF $GF(p)$ or over the polynomial FF $GF(p^d)$, while special types of the vector multiplication operation is defined. It is proposed the BVMT possessing simple structure and providing the associative vector multiplication.

It has been shown that the complexity of the multiplication in vector FFs is lower than in the ground and polynomial FFs, while the size of the field order is the same. This advantage and suitability of the efficient parallelization of the multiplication operation provides possibility to significant acceleration of the EC-based DSAs with application of the vector FFs as underlying fields.

Acknowledgement. The work supported by Russian Foundation for Basic Research grant # 08-07-90100-Mol_a.

References

[1] **G. B. Agnew, R. C. Mullin, I. M. Onyszchuk, and S. A. Vanstone**, *An implementation for a fast public key cryptosystem*, J. Cryptology **3** (1991),

63 – 79.

[2] **G. B. Agnew, R. C. Mullin, and S. A. Vanstone**, *An implementation of elliptic curve cryptosystems over* $\mathbf{F}_{2^{155}}$, IEEE Journal on Selected Areas in Communications **11** (1993), 804 – 813.

[3] **G. B. Agnew, T. Beth, R. C. Mullin, and S.A. Vanstone**, *Arithmetic operations in* $GF(2^m)$, J. Cryptology **6** (1993), 3 – 13.

[4] **International Standard ISO/IEC 14888-3:2006(E).**, *Information technology – Security techniques – Digital Signatures with appendix – Part 3: Discrete logarithm based mechanisms.*

[5] **N. Koblitz**, *A course in number theory and cryptography*, Springer-Verlag, Berlin, 2003.

[6] **A.G. Kurosh**, *Course of higher algebra*, (Russian), Moskva, Nauka 1971.

[7] **J. Lee, H. Kim, Y. Lee, S.-M. Hong, H. Yoon**, *Parallelized scalar multiplication on elliptic curves defined over optimal extension field*, Internat. J. Network Security **4** (2007), 99 – 106.

[8] **A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone**, *Handbook of applied cryptography*, CRC Press, Boca Raton, FL, 1997.

[9] **A. J. Menezes and S. A. Vanstone**, *Elliptic curve cryptosystems and their implementation*, J. Cryptology **6** (1993), 209 – 224.

[10] **N. A. Moldovyan**, *A method for generating and verifying electronic digital signature certifying an electronic document*, Russian patent application # 2008140403, October 14, 2008.

[11] **J. Pieprzyk, Th. Hardjono, and J. Seberry**, *Fundamentals of computer security*, Springer-Verlag. Berlin, 2003.

[12] **R. Pierce**, *Associative algebras*, (Russian), Moscow, Mir, 1986.

[13] **N. Smart**, *Cryptography: an introduction*, McGraw-Hill Publication, London, 2003.

Received December 18, 2008

St. Petersburg Institute for Informatics and Automation, Russian Academy of Sciences,
St. Petersburg, Russia
E-mail: nmold@cobra.ru