BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 3(61), 2009, Pages 57–63
ISSN 1024–7696

# Vector Form of the Finite Fields $GF(p^m)$ *

N. A. Moldovyan, P. A. Moldovyanu

**Abstract.** Specially defined multiplication operation in the $m$-dimensional vector space (VS) over a ground finite field (FF) imparts properties of the extension FF to the VS. Conditions of the vector FF (VFF) formation are derived theoretically for cases $m = 2$ and $m = 3$. It has been experimentally demonstrated that under the same conditions VFF are formed for cases $m = 4$, $m = 5$, and $m = 7$. Generalization of these results leads to the following hypotheses: for each dimension value $m$ the VS defined over a ground field $GF(p)$, where $p$ is a prime and $m|p-1$, can be transformed into a VFF introducing special type of the vector multiplication operations that are defined using the basis-vector multiplication tables containing structural coefficients. The VFF are formed in the case when the structural coefficients that could not be represented as the $m$th power of some elements of the ground field are used. The VFF can be also formed in VS defined over extension FF represented by polynomials. The VFF present interest for cryptographic application.

**Mathematics subject classification:** 11G20, 11T71.
**Keywords and phrases:** Vector space, ground finite field, extension finite field, cryptography, digital signature.

## 1 Introduction

The finite fields (FF) play a prominent role in the public key cryptography. They are well studied as primitives of the digital signature (DS) algorithms [1–3]. Finding discrete logarithm (DL) in a subgroup of the multiplicative group of some FF is used as the hard computational problem put into the base of DS algorithms. The security of the DS is determined by the difficulty of the DL problem.

Since all FF of the same order are isomorphic, in many cases it is sufficient to consider only the polynomial FF $GF(p^n)$ and extend the results to any possible type of the field $GF(p^n)$. However in the case of computational problems it is reasonable to take into account concrete forms of the FF representation. For example, finding DL has essentially different difficulty in various particular variants of the field $GF(p^n)$ for the same values $p$ and $n$. To reduce the DL problem defined in one representation form to the DL problem defined in some other particular form of the field $GF(p^n)$ one should compute the isomorphism between these FF variants. A prominent example of the analogous situation is presented by elliptic curves (EC) over finite fields [4]. Finite groups of the EC points are isomorphic to some subgroups of the multiplicative group of some ring $Z_p$, where the DL problem can be solved with methods having subexponential complexity, however the best known

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

methods for solving the DL problem on specially selected EC have exponential complexity [5]. At present the DS algorithms based on the difficulty of the DL problem on EC are the most computationally efficient among the DSA providing the same security level. However performing the group operation over the EC points includes the inversion operation in the field over which the EC are defined [5]. The inversion operation significantly restricts the rate of the EC-based DS algorithms.

Search of new representation forms of the FF and their use in the DS algorithms have significant importance for information security practice. In the present paper we introduce a new form of the FF $GF(p^m)$ defined over the $m$-dimensional finite vector spaces (VS), the vector coordinates being the elements of some ground FF $GF(p)$. In such FF, called vector FF (VFF), the multiplication operation is free of the inversion in the underlying field $GF(p)$. Therefore the use of the VFF can provide significant improvement of the DS algorithm performance [6]. In Section 2 we derive the VFF formation conditions for cases $m = 2$ and $m = 3$. In Section 3 we experimentally show that the derived conditions work for the cases $m = 4$, $m = 5$, and $m = 7$. In Section 4 we generalize the VFF formation conditions to arbitrary dimension values. In the concluding Section 5 it is underlined that the VFF can be defined over some extended FF.

In the paper the following specific term is used:

*The kth-power element in some FF* $GF(p^d)$, 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 Two- and three-dimensional vector finite fields

Let us have some $m$-dimensional vector space over a field $GF(p)$. Suppose $\mathbf{e}$, $\mathbf{i}$, $\dots$, $\mathbf{j}$ be some $m$ basis vectors and $a, b, c \in GF(p)$, where $p \geq 3$, are coordinates. So this space is the set of vectors $a\mathbf{e} + b\mathbf{i} + \dots + c\mathbf{j}$. A vector can be also represented as a set of its coordinates $(a, b, \dots, c)$. The terms $\epsilon\mathbf{v}$, where $\epsilon \in GF(p)$ and $\mathbf{v} \in \{\mathbf{e}, \mathbf{i}, \dots, \mathbf{j}\}$, are called components of the vector.

The addition of two vectors $(a, b, \dots, c)$ and $(x, y, \dots z)$ is defined as follows:

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

where "+" denotes addition operation in the field $GF(p)$. The first representation of the vectors can be interpreted as the sum of the vector components.

Let the multiplication of the vectors $(a, b, \dots, c)$ and $(x, y, \dots z)$ be defined by the formula

$$(a\mathbf{e} + b\mathbf{i} + \dots + c\mathbf{j}) \cdot (x\mathbf{e} + y\mathbf{i} + \dots + z\mathbf{j}) = a\mathbf{e} \cdot x\mathbf{e} + b\mathbf{i} \cdot x\mathbf{e} + \dots$$

$$\dots + c\mathbf{j} \cdot x\mathbf{e} + a\mathbf{e} \cdot y\mathbf{i} + b\mathbf{i} \cdot y\mathbf{i} + \dots + c\mathbf{j} \cdot y\mathbf{i} + \dots a\mathbf{e} \cdot z\mathbf{j} + b\mathbf{i} \cdot z\mathbf{j} + \dots + c\mathbf{j} \cdot z\mathbf{j} =$$

$$= ax\mathbf{e} \cdot \mathbf{e} + bx\mathbf{i} \cdot \mathbf{e} + \dots + cx\mathbf{j} \cdot \mathbf{e} + ay\mathbf{e} \cdot \mathbf{i} + by\mathbf{i} \cdot \mathbf{i} + \dots + cy\mathbf{j} \cdot \mathbf{i} + \dots az\mathbf{e} \cdot \mathbf{j} + bz\mathbf{i} \cdot \mathbf{j} + \dots + cz\mathbf{j} \cdot \mathbf{j}),$$

where each product of two basis vectors is replaced by a vector component $\epsilon\mathbf{v}$ ($\epsilon \in GF(p)$) in accordance with some given tables called basis-vector multiplication tables (BVMT). To define formation of the VFF the BVMT should be properly designed.

Let us consider two- and three-dimensional VS defined over some ground field $GF(p)$. In the case $m = 2$ the general representation of the BVMT possessing commutativity, associativity, and unit $(1, 0)$ 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 $\epsilon \in GF(p)$ define different variants of the multiplication operation. Each of these variants defines a finite ring of the two-dimensional vectors. Let us consider a nonzero vector $Z = a\mathbf{e}+b\mathbf{i}$. The element $Z^{-1} = x\mathbf{e}+y\mathbf{i}$ is called an inverse of $Z$ if $Z^{-1}Z = \mathbf{e} = (1, 0)$, where 1 and 0 are the identity and zero elements in $GF(p)$. We have

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

For given $(a, b)$ there exists a unique pair $(x, y) \in GF(p) \times GF(p)$ satisfying the last equation if the system of equations

$$\begin{cases} ax + \epsilon by &= 1, \\ bx + ay &= 0 \ . \end{cases}$$

has a unique solution in $GF(p) \times GF(p)$, i.e. if $a^2 - \epsilon b^2 \neq 0$ in $GF(p)$. The last condition holds for all vectors $(a, b)$, except (0,0), if $\epsilon$ 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

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

Thus, in the case $m = 2$ the characteristic equation

$$a^2 - \epsilon b^2 = 0 \tag{1}$$

defines formation of the VFF $GF(p^2)$. If this equation has no solution for each pair $(a, b)$, except $(0, 0)$, then for each nonzero vector of the two-dimensional VS defined over the field $GF(p)$ there exists its unique inverse, i.e. we have the VFF $GF(p^2)$.

In the case $m = 3$ Table 1, where $\mu \in GF(p)$ and $\epsilon \in GF(p)$, represents the BVMT possessing commutativity, associativity, and unit $(1, 0, 0)$ for arbitrary values $\mu$ and $\epsilon$, called structural coefficients. Let us consider a nonzero vector $Z = a\mathbf{e} + b\mathbf{i} + c\mathbf{k}$. There exists its unique inverse $X = x\mathbf{e} + y\mathbf{i} + z\mathbf{k}$ if the vector equation

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

has a unique solution relative to the unknown $X$. From the last equation the following system of equations can be derived

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

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

| $\cdot$ | $\overrightarrow{e}$ | $\overrightarrow{\imath}$ | $\overrightarrow{\jmath}$ |
|---|---|---|---|
| $\overrightarrow{e}$ | $\mathbf{e}$ | $\mathbf{i}$ | $\mathbf{j}$ |
| $\overrightarrow{\imath}$ | $\mathbf{i}$ | $\epsilon\mathbf{j}$ | $\mu\epsilon\mathbf{e}$ |
| $\overrightarrow{\jmath}$ | $\mathbf{j}$ | $\mu\epsilon\mathbf{e}$ | $\mu\mathbf{i}$ |

From this system the following characteristic equation can be easily derived

$$a^3 - 3\epsilon\mu bc \cdot a + \epsilon^2\mu b^3 + \epsilon\mu^2 c^3 = 0. \tag{2}$$

If this equation has no solutions relative to the unknown $a$ for each pair $(b, c)$, except $(0, 0)$, and only one solution $a = 0$ for $(b, c) = (0, 0)$, then the three-dimensional VS is an extension FF $GF(p^3)$. Denoting $B = (\epsilon^2\mu b^3 + \epsilon\mu^2 c^3)/2$ and using the well known formulas [7] for cubic equation roots we get the expression for the roots $a$ of equation (2) in the following form

$$a = A' + A'',$$

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 third-power elements in the field $GF(p)$, then the characteristic equation (2) has no solutions relative to the unknown $a$ for all possible pairs $(a, b) \neq (0, 0)$ and only one solution $a = 0$ for $(a, b) = (0, 0)$. It is well known that this situation is possible if $3|p - 1$.

Thus, if $3|p - 1$ and each of the products $\epsilon^2\mu$ and $\epsilon\mu^2$ is not the third-power element in the field $GF(p)$, then for each nonzero vector $Z$ there exists its unique inverse and the VS is the VFF $GF(p^3)$. The multiplicative group of the field $GF(p^3)$ has the order

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

**Example 1.** Suppose $p = 1723$ (i.e. $3|p - 1$). Then for $\mu = 1$ and $\epsilon = 1666$ ($\epsilon$ is not the cubic element in $GF(1723)$) a vector field $GF(p^3)$ is formed in which the vector (2,3,3) is a generator of the multiplicative group of the order $\Omega = p^3 - 1 = 5115120066$.

It is easy to see that characteristic equation (1) has no solutions over FF $GF(p^d)$ for some integer $d \geq 1$, if $b \neq 0$ and $\epsilon$ is not the second-power element in $GF(p^d)$. Analogously, characteristic equation (2) has no solutions over FF $GF(p^d)$ for some integer $d \geq 1$, if $(b, c) \neq (0, 0)$ and both values $\epsilon\mu^2$ and $\epsilon^2\mu$ are not the third-power elements in the field $GF(p^d)$. Thus, the two-dimensional VFF $GF(p^{2d})$ and three-dimensional VFF $GF(p^{3d})$ can be defined over the extension FF $GF(p^d)$.

Table 2. Basis-vector multiplication table for the case $m = 4$

| $\cdot$ | $\overrightarrow{e}$ | $\overrightarrow{\imath}$ | $\overrightarrow{\jmath}$ | $\overrightarrow{k}$ |
|---|---|---|---|---|
| $\overrightarrow{e}$ | $\mathbf{e}$ | $\mathbf{i}$ | $\mathbf{j}$ | $\mathbf{k}$ |
| $\overrightarrow{\imath}$ | $\mathbf{i}$ | $\epsilon\mathbf{j}$ | $\epsilon\mathbf{k}$ | $\mu\epsilon\mathbf{e}$ |
| $\overrightarrow{\jmath}$ | $\mathbf{j}$ | $\epsilon\mathbf{k}$ | $\mu\epsilon\mathbf{e}$ | $\mu\mathbf{i}$ |
| $\overrightarrow{k}$ | $\mathbf{k}$ | $\mu\epsilon\mathbf{e}$ | $\mu\mathbf{i}$ | $\mu\mathbf{j}$ |

## 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 $m|p^d - 1$, provided some of the structural coefficients are not the $m$th-power elements in the field $GF(p^p)$ over which the VS is defined. Validity of this VFF formation condition has been experimentally demonstrated for cases $m = 4$, $m = 5$, and $m = 7$, while using the BVMT presented in Tables 2, 3, and 4, correspondingly. Tables 2 and 3 are designed in line with the BVMT type presented by Table 1 that relates to the case $m = 3$ (note that in the case of Table 3 the vector $(\tau^{-1}, 0, 0, 0, 0)$ is unit). The analogous design is possible for the case $m = 7$, however we used a particular variant for structure of Table 4 to show that in general different types of the BVMT can be applied to define VFF.

**Example 2.** For prime $p = 2609$, the dimension $m = 4$ $(m|p - 1)$, and coefficients $\mu = 1$ and $\epsilon = 2222$ ($\epsilon$ 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 VFF $GF(p^4)$. 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 3.** For prime $p = 151$, the dimension $m = 5$ $(5|p - 1)$, and coefficients $\tau = \mu = 1$ and $\epsilon = 111$ ($\epsilon$ is not the 5th-power element in $GF(151)$) the vector $G_\Omega = 1\mathbf{e} + 3\mathbf{i} + 5\mathbf{j} + 7\mathbf{k} + 11\mathbf{u}$ is a generator of the multiplicative group of the VFF $GF(p^5)$. The vector $G_q = 141\mathbf{e} + 111\mathbf{i} + 50\mathbf{j} + 28\mathbf{k} + 142\mathbf{u}$ is a generator of the subgroup having prime order $q = 104670301$.

**Example 4.** For prime $p = 29$, the dimension $m = 7$ $(7|p - 1)$, and coefficient $\epsilon = 3$ ($\epsilon$ 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 $q = 88009573$.

Theoretic results presented in Section 2 and experiments for the cases $m = 4$ and $m = 5$ give us grounds to put forward the following hypothesis.

*In some finite $m$-dimensional VS defined over a FF $GF(p^d)$ such that $m|p^d - 1$ and $d \geq 1$ it is possible to define vector multiplication with BVMT which imparts to the VS properties of the FF $GF(p^{dm})$.*

Table 3. Basis-vector multiplication table for the case $m = 5$

| $\cdot$ | $\overrightarrow{e}$ | $\overrightarrow{\imath}$ | $\overrightarrow{\jmath}$ | $\overrightarrow{k}$ | $\overrightarrow{u}$ |
|---|---|---|---|---|---|
| $\overrightarrow{e}$ | $\tau\mathbf{e}$ | $\tau\mathbf{i}$ | $\tau\mathbf{j}$ | $\tau\mathbf{k}$ | $\tau\mathbf{u}$ |
| $\overrightarrow{\imath}$ | $\tau\mathbf{i}$ | $\epsilon\mathbf{j}$ | $\epsilon\mathbf{k}$ | $\epsilon\mathbf{u}$ | $\epsilon\mu\tau^{-1}\mathbf{e}$ |
| $\overrightarrow{\jmath}$ | $\tau\mathbf{j}$ | $\epsilon\mathbf{k}$ | $\epsilon\mathbf{u}$ | $\epsilon\mu\tau^{-1}\mathbf{e}$ | $\mu\mathbf{i}$ |
| $\overrightarrow{k}$ | $\tau\mathbf{k}$ | $\epsilon\mathbf{u}$ | $\epsilon\mu\tau^{-1}\mathbf{e}$ | $\mu\mathbf{i}$ | $\mu\mathbf{j}$ |
| $\overrightarrow{u}$ | $\tau\mathbf{u}$ | $\epsilon\mu\tau^{-1}\mathbf{e}$ | $\mu\mathbf{i}$ | $\mu\mathbf{j}$ | $\mu\mathbf{k}$ |

Table 4. Basis-vector multiplication table for the case $m = 7$

| $\cdot$ | $\overrightarrow{e}$ | $\overrightarrow{\imath}$ | $\overrightarrow{\jmath}$ | $\overrightarrow{k}$ | $\overrightarrow{u}$ | $\overrightarrow{v}$ | $\overrightarrow{w}$ |
|---|---|---|---|---|---|---|---|
| $\overrightarrow{e}$ | $\mathbf{e}$ | $\mathbf{i}$ | $\mathbf{j}$ | $\mathbf{k}$ | $\mathbf{u}$ | $\mathbf{v}$ | $\mathbf{w}$ |
| $\overrightarrow{\imath}$ | $\mathbf{i}$ | $\epsilon\mathbf{k}$ | $\epsilon\mathbf{v}$ | $\epsilon\mathbf{j}$ | $\epsilon\mathbf{e}$ | $\epsilon\mathbf{w}$ | $\epsilon\mathbf{u}$ |
| $\overrightarrow{\jmath}$ | $\mathbf{j}$ | $\epsilon\mathbf{v}$ | $\epsilon\mathbf{u}$ | $\epsilon\mathbf{w}$ | $\mathbf{k}$ | $\epsilon\mathbf{e}$ | $\mathbf{i}$ |
| $\overrightarrow{k}$ | $\mathbf{k}$ | $\epsilon\mathbf{j}$ | $\epsilon\mathbf{w}$ | $\epsilon\mathbf{v}$ | $\mathbf{i}$ | $\epsilon\mathbf{u}$ | $\epsilon\mathbf{e}$ |
| $\overrightarrow{u}$ | $\mathbf{u}$ | $\epsilon\mathbf{e}$ | $\mathbf{k}$ | $\mathbf{i}$ | $\mathbf{w}$ | $\mathbf{j}$ | $\mathbf{v}$ |
| $\overrightarrow{v}$ | $\mathbf{v}$ | $\epsilon\mathbf{w}$ | $\epsilon\mathbf{e}$ | $\epsilon\mathbf{u}$ | $\mathbf{j}$ | $\mathbf{i}$ | $\mathbf{k}$ |
| $\overrightarrow{w}$ | $\mathbf{w}$ | $\epsilon\mathbf{u}$ | $\mathbf{i}$ | $\epsilon\mathbf{e}$ | $\mathbf{v}$ | $\mathbf{k}$ | $\mathbf{j}$ |

The required BVMT can be constructed analogously to Tables 2 and 3 and using the unit element of $GF(p)$ as the coefficient $\mu$ and a value $\epsilon$ that is not the $m$th-power element in $GF(p)$. Since $m|p^d - 1$ such values $\epsilon$ exist and can be easily found.

## 4 Conclusion

Defining the vector multiplication operation with BVMT that contain the structural coefficients having large size and using sufficiently large values $m$ one can define more difficult DL problem in the VFF. Therefore in such cases VFF with smaller order size can be used to design the DS algorithms. Besides, the vector multiplication operation can be implemented as parallel performing the multiplications in the FF over which the VFF is defined. These two facts provide possibility to get sufficiently high performance of the DS algorithms based on VFF.

The following problems are important for further consideration of the VFF as cryptographic primitive.

1. Proof of the hypothesis presented in the end of Section 3.

2. Proof of the generalization of the experimental results (if there exist $m$-dimensional VFF over $GF(p^d)$ for some values $d$ and $p$ such that $m|p-1$, then there exist VFF for the same value $d$ and arbitrary values $p$ such that $m|p-1$).

3. Development of the BVMT providing minimization of the vector multiplication complexity.

4. Detailed investigation of the DL problem difficulty in VFF and its connection with the dimension value and the size of the structural coefficients in BVMT.

Using special type of BVMT it is possible to define non-commutative rings over finite VS, which also present interest as cryptographic primitive and is a subject of independent research.

## References

[1] Menezes A. J., Van Oorschot P. C., Vanstone S. A. *Handbook of Applied Cryptography.* CRC Press, Boca Raton, FL, 1997.

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

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

[4] Koblitz N. *A Course in Number Theory and Cryptography.* Springer-Verlag, Berlin, 2003.

[5] Menezes A. J., Vanstone S. A. *Elliptic Curve Cryptosystems and Their Implementation.* J. Cryptology, 1993. **6**, No. 4, 209–224.

[6] Moldovyan D. N., Moldovyan N. A. *A Method for Generating and Verifying Electronic Digital Signature Certifying an Electronic Document.* Russian patent # 2369974.

[7] Kurosh A. G. *Kurs vysshey algebry.* Moskva. Nauka, 1971 (in Russian)

*Received January 10, 2009*

N. A. Moldovyan
St. Petersburg Institute for Informatics
and Automation of Russian Academy of Sciences
14 Liniya, 39, St. Petersburg 199178
Russia
E-mail: *nmold@mail.ru*

P. A. Moldovyanu
Specialized Center of Program Systems "SPECTR"
Kantemirovskaya, 10, St.Petersburg 197342
Russia
E-mail: *p1960@mail.ru*