Quasigroups and Related Systems **32** (2024), 299 – 312

https://doi.org/10.56415/qrs.v32.21

Parameterized method for specifying vector finite fields of arbitrary dimensions

Nikolay A. Moldovyan

Abstract. Finite fields defined in the form of finite algebras are of significant interest for constructing multivariate-cryptography algorithms with a relatively small size of public key. This application is associated with specifying vector finite fields of dimension m with large number of their modifications for various fixed values of m. A method for parameterized unified generation of multiplication tables of basis vectors is proposed, with the help of which the commutative and associative multiplication operation is specified. The method is represented by a mathematical formula that includes the dimension m and parameters for specifying the distribution of basis vectors and various independent structural constants.

1. Introduction

The development of practical post-quantum public key cryptosystems represents a pressing challenge for the global cryptographic community [10]. One of the promising areas in the field of post-quantum cryptography is multivariate public-key cryptography [2]. However, multivariate-cryptography algorithms have a significant drawback, which is their extremely large size of public key. Recently, a new paradigm for developing multivariate-cryptography algorithms has been proposed, which consists in specifying nonlinear mappings (with a secret trapdoor) in the form of exponentiation operations in vector finite fields [5].

That paradigm allows for a potential size reduction of 10 times or more for a given level of security. The article [5] presents the implementation of

2010 Mathematics Subject Classification: 94A60, 16Z05, 14G50, 11T71, 16S50

Keywords: finite algebra, vector finite field, structural constant, post-quantum cryptography, multivariate cryptography

This work was financially supported by Russian Science Foundation (project No. 24-41-04006).

nonlinear mappings using heuristically specified vector finite fields of particular dimension values. When heuristically specifying vector finite fields, difficulties arise in finding a sufficiently large number of distributions of structural constants, with the help of which the variety of modifications of such fields is specified for a given value of m, especially in cases of large dimensions.

This article proposes a formalized unified method for specifying vector finite fields for arbitrary dimension values, within the framework of which the construction of basis vector multiplication tables (BVMTs used to specify the multiplication operation) with parameterization of distributions of both the basis vectors and the structural constants is implemented.

2. Preliminaries

In an m-dimensional vector space over the field $GF\left(p^s\right)$, some vector A can be represented in the following two forms: $A=(a_0,a_1,\ldots,a_{m-1})$ or as $A=\sum_{i=0}^{m-1}a_i\mathbf{e}_i$, where $a_0,a_1,\ldots,a_{m-1}\in GF\left(p^s\right)$ are coordinates; $\mathbf{e}_0$, $\mathbf{e}_1$, ... $\mathbf{e}_{m-1}$ are basis vectors. In a finite m-dimensional vector space we have two standard operations: 1) addition of vectors and 2) scalar multiplication. If the vector multiplication operation is additionally (to usual operations of addition and scalar multiplication in the vector space) specified, which is closed and possesses properties of distributivity at the left and at the right relatively the addition operation, then one gets a finite m-dimensional algebra.

Usually, the vector multiplication of two vectors A and B is specified by the following formula

$$AB=\sum_{i=0}^{m-1}\sum_{j=0}^{m-1}a_ib_j(\mathbf{e}_i\mathbf{e}_j), \tag{1}$$

where every of the products $\mathbf{e}_i\mathbf{e}_j$ is to be replaced by a single-component vector $\lambda\mathbf{e}_k$, where $\lambda\in GF\left(p^s\right)$, indicated in the intersection of the ith row and jth column of some BVMT.

The articles [8, 9] present several BVMTs that set the multiplication operation possessing the properties of commutativity and associativity. For some of that BVMTs, parameters for specifying finite algebras can be chosen such that the latter are vector finite fields [9]. For example, when using Table 1 (where $\sigma=\tau^{-1}\epsilon\mu$) to specify a finite m-dimensional ($m\geqslant 2$))

algebra over the field $GF(p^s)$, where m divides the value $p^s - 1$, one can choose many different sets of values of structural constants ϵ, μ, and τ, for which the specified algebra is a finite field $GF\left((p^s)^m\right)$, where p is an even or odd prime [9]. The constants ϵ, μ, and τ are independent and define the constant $\sigma = \epsilon\mu\tau^{-1}$.

Table 1

A general form of BVMT for setting the vector fields $GF\left((p^s)^m\right)$ [9].

$\cdot$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\cdots$	$\mathbf{e}_{m-2}$	$\mathbf{e}_{m-1}$
$\mathbf{e}_0$	$\tau\mathbf{e}_0$	$\tau\mathbf{e}_1$	$\tau\mathbf{e}_2$	$\tau\mathbf{e}_3$	$\tau\cdots$	$\tau\mathbf{e}_{m-2}$	$\tau\mathbf{e}_{m-1}$
$\mathbf{e}_1$	$\tau\mathbf{e}_1$	$\epsilon\mathbf{e}_2$	$\epsilon\mathbf{e}_3$	$\epsilon\cdots$	$\epsilon\mathbf{e}_{m-2}$	$\epsilon\mathbf{e}_{m-1}$	$\sigma\mathbf{e}_0$
$\mathbf{e}_2$	$\tau\mathbf{e}_2$	$\epsilon\mathbf{e}_3$	$\epsilon\cdots$	$\epsilon\mathbf{e}_{m-2}$	$\epsilon\mathbf{e}_{m-1}$	$\sigma\mathbf{e}_0$	$\mu\mathbf{e}_1$
$\mathbf{e}_3$	$\tau\mathbf{e}_3$	$\epsilon\cdots$	$\epsilon\mathbf{e}_{m-2}$	$\epsilon\mathbf{e}_{m-1}$	$\sigma\mathbf{e}_0$	$\mu\mathbf{e}_1$	$\mu\mathbf{e}_2$
$\cdots$	$\tau\cdots$	$\epsilon\mathbf{e}_{m-2}$	$\epsilon\mathbf{e}_{m-1}$	$\sigma\mathbf{e}_0$	$\mu\mathbf{e}_1$	$\mu\mathbf{e}_2$	$\mu\ldots$
$\mathbf{e}_{m-2}$	$\tau\mathbf{e}_{m-2}$	$\epsilon\mathbf{e}_{m-1}$	$\sigma\mathbf{e}_0$	$\mu\mathbf{e}_1$	$\mu\mathbf{e}_2$	$\mu\cdots$	$\mu\mathbf{e}_{m-3}$
$\mathbf{e}_{m-1}$	$\tau\mathbf{e}_{m-1}$	$\sigma\mathbf{e}_0$	$\mu\mathbf{e}_1$	$\mu\mathbf{e}_2$	$\mu\cdots$	$\mu\mathbf{e}_{m-3}$	$\mu\mathbf{e}_{m-2}$

In the multivariate cryptography algorithms, the public key is set as a hard to reverse non-linear mapping $\Pi(X)$ (with a secret trapdoor) of n-dimensional vectors X over the field $GF\left(p^s\right)$ of small order into u-dimensional vectors Y over the same finite field [1, 11]. The mapping Π is specified as a set of u power polynomials (usually quadratic) in n variables (that are coordinates of X). The construction of the public key Π is the main point in the development of the multivariate cryptography algorithms and is carried out in the following way.

A set of u secret power polynomials $f_j\left(x_0, x_1, \ldots, x_{n-1}\right)$ over $GF\left(p^s\right)$ ($j = 0, 1 \ldots u-1$ and the values of f_j are respective coordinates of the image vector Y) , which specify a mapping $\Psi(X)$ that is easy to reverse, i.e. to calculate the pre-image vector X for a given image vector Y. Thus, when constructing the said set of polynomials, the presence of an effectively computable inverse mapping $\Psi^{-1}(Y)$ is provided. Then, using one or two secret linear mappings Λ_1: $\left(GF\left(p^s\right)\right)^n \to \left(GF\left(p^s\right)\right)^n$ (performed as computation of n secret linear polynomials f'_j over $GF\left(p^s\right)$) and $\Lambda_2 : \left(GF\left(p^s\right)\right)^u \to \left(GF\left(p^s\right)\right)^u$ (performed as computation of u secret linear polynomials f''_k over $GF\left(p^s\right)$).

By sets of secret polynomials $\{f_0, f_1, \ldots f_{u-1}\}$, $\left\{f'_0, f'_1, \ldots f'_{n-1}\right\}$, and $\left\{f''_0, f''_1, \ldots f''_{u-1}\right\}$, the set of polynomials $\{\pi_0, \pi_1, \ldots \pi_{u-1}\}$ is calculated the

latter being the public key Π:

$$\Pi(X) = \Lambda_2(\Psi(\Lambda_1(X))). \tag{2}$$

The secret trapdoor related to the public key Π represent the triple of mappigs Λ_2^{-1}, Ψ^{-1}, Λ_1^{-1}, computation of the latter from the set of polynomials Π being computationally impossible. Public encryption is performed representing the source message as an n-dimensional vector $T = (t_0, t_1, \ldots, t_{n-1})$ and computing the ciphertext as the u-dimensional vector $C = \Pi(T)$. The owner of the public key Π can easily decrypt the ciphertext C:

$$T = \Pi^{-1}(C) = \Lambda_1^{-1}\left(\Psi^{-1}\left(\Lambda_2^{-1}(C)\right)\right). \tag{3}$$

A direct attack on algorithms of such type consists in reversing the mapping Π by the way of solving a system of u power equations with n unknowns $\{t_0, t_1, \ldots, t_{n-1}\}$. The best known methods for solving such systems are based on using so called algorithms F4 [3] and F5 [4]. To ensure security level (to direct attacks) 2^{80} to 2^{256} the public key should include 26 to 110 power polynomials (see Table 1 in [1]).

The implementation of the mapping Π as a superposition of a readily reversible nonlinear mapping and masking linear mappings leads to the fact that the size of the public key is excessively large compared to other types of post-quantum algorithms. The paper [5] proposed a method for significantly reducing the size of the public key (by a factor of 10 or more). That method consists of implementing the mapping Ψ as a set of power polynomials, which is determined by one or several exponentiation operations to the degrees 2 and 3 in the vector finite fields of odd characteristic, or to significantly higher degrees in vector finite fields of characteristic two [5].

This technique allows us to avoid the use of masking linear mappings, which significantly increase the size of the public key. This method makes it possible to free ourselves from the need to provide for the possibility of implementing the inverse mapping Ψ^{-1}, since it arises naturally due to the computationally efficient ability to perform the operation of extracting roots of various degrees in finite fields. A detailed example of constructing a mapping Ψ for vectors of dimension 85 using exponentiation operations in 5-dimensional and 17-dimensional vector finite fields is presented in [5]. In that design the linear mapping (permutation of the coordinates of the transformed vectors) is also used, which, however, do not increase the size of the public key.

The sufficiency of using linear mappings free from increasing the size of the public key is due to the fact that there is no need to provide masking of the mapping Ψ^{-1}, since masking of root extraction operations is ensured by the fact that from the coefficients in the public key polynomials it is computationally difficult to restore the set of secret structural constants used in the BVMTs used to specify the multiplication operation in vector finite fields. Recovering the modifications of the vector fields used to define the nonlinear mapping Ψ becomes more difficult as the number of different structure constants in the BVMTs increases, since the coefficients of the public key polynomials are determined by large number of structural constants. In the paradigm by [5] it is assumed to use exponential operations in vector finite fields of dimensions from 5 to 110, depending on the required level of security and the nonlinear-mapping topology used.

For a given value of dimension and a given distribution of basis vectors in the BVMT, it is important to find sufficiently large number of different distributions of structural constants that preserve the commutativity and associativity properties of the vector multiplication operation. Ensuring a sufficiently complete solution to such a problem using a computational heuristic method is problematic. This determines the interest in developing formalized unified methods for specifying BVMTs with large number of independent structural constants and finding the distributions of the latter. The following Section 3 proposes a unified method for specifying BVMTs with parameterized distribution of the bases vectors, which are suitable for defining vector finite fields. Section 4 introduces a technique for specifying a parameterized distribution of structural constants, which preserves the commutative and associative properties of the multiplication operation and allows one to construct BVMTs suitable for developing hard to reverse nonlinear mappings with a secret trapdoor. Section 5 presents some results of the experimental verification of the proposed method.

3. A unified method for setting commutative associative finite algebras

It can be easily shown that a given BVMT defines associative multiplication if the following equality holds for all possible triples of basis vectors $\mathbf{e}_i$, $\mathbf{e}_j$, and $\mathbf{e}_k$:

$$(\mathbf{e}_i\mathbf{e}_j)\,\mathbf{e}_k = \mathbf{e}_i\,(\mathbf{e}_j\mathbf{e}_k)\,. \tag{4}$$

By analogy with the unified method [6] and with specifying non-commutative associative algebras of arbitrary even dimensions $m \geqslant 6$ [7], one can propose a mathematical formula for generating BVMTs defining commutative algebras of arbitrary dimensions $m \geqslant 2$, which has the following form:

$$\mathbf{e}_i \mathbf{e}_j = \mathbf{e}_{(i+j+d) \bmod m}, \tag{5}$$

where parameter $d = 0, 1, \ldots m-1$ specifies m different distributions of the basis vectors. The following Proposition 3.1 is evident:

Proposition 3.1. *The BVMTs generated by formula* (5) *specify commutative multiplication operation.*

Proposition 3.2. *The BVMT generated by formula* (5) *for the fixed values of m and d sets the finite algebra with the global two-sided unit $U = (0, \ldots, 1, \ldots 0)$ with $m-1$ zero coordinates and one coordinate equal to $1 \in GF(p^s)$, namely, $u_{(m-d) \bmod m} = 1$.*

Proof. Using formula (1) one can write

$$UA = AU = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} a_i u_j (\mathbf{e}_i \mathbf{e}_j) = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} a_i u_j \mathbf{e}_{(i+j+d) \bmod m} =$$
$$= \sum_{i=0}^{m-1} a_i u_{(m-d) \bmod m} \mathbf{e}_{(i+m-d+d) \bmod m} = \sum_{i=0}^{m-1} a_i \mathbf{e}_i = A.$$

Thus, the vector U is the global two-sided unit. □

Proposition 3.3. *The BVMTs generated by formula* (5) *specify associative multiplication operation.*

Proof. For an arbitrary triple $(\mathbf{e}_i, \mathbf{e}_j, \mathbf{e}_k)$, for the right and left parts of equation (4) we have correspondingly:

$$(\mathbf{e}_i \mathbf{e}_j)\, \mathbf{e}_k = \mathbf{e}_{(i+j+d) \bmod m} \mathbf{e}_k = \mathbf{e}_{(i+j+d+k+d) \bmod m} = \mathbf{e}_{(i+j+k+2d) \bmod m};$$
$$\mathbf{e}_i\, (\mathbf{e}_j \mathbf{e}_k) = \mathbf{e}_i \mathbf{e}_{(j+k+d) \bmod m} = \mathbf{e}_{(i+j+k+d+d) \bmod m} = \mathbf{e}_{(i+j+k+2d) \bmod m}.$$

Thus, equality (4) holds true for all possible triples of basis vectors, i.e. the multiplication operation is associative. □

4. A unified method for setting the vector finite fields for multivariate cryptography

To ensure the possibility of a unified generation of BVMTs including structural constants, the following version of formula (5) is proposed:

$$\mathbf{e}_i\mathbf{e}_j = \begin{cases} \mathbf{e}_{(i+j+d) \bmod m}, & \text{if } t(i+d) \bmod m + t(j+d) \bmod m < m; \\ \lambda_t \mathbf{e}_{(i+j+d) \bmod m}, & \text{if } t(i+d) \bmod m + t(j+d) \bmod m \geqslant m, \end{cases} \tag{6}$$

where $t = 1, 2, \ldots m-1$ is a parameter specifying distributions of $m-1$ independent structural constants for every of the fixed values of the parameter d. It is easy to see that the algebra set by the BVMT generated by formula (6) is commutative and contains the global two-sided unit U that has the single non-zero coordinate $u_{(m-d) \bmod m}$, i.e. Propositions 3.1 and 3.2 hold true also in the latter case.

Proposition 4.1. *The BVMTs with one structural constant λ_t distribution of which is specified by formula* (6) *set associative multiplication operation.*

Proof. Consider formula (4). Due to Proposition 3.3 the left part of (4) is equal to $\lambda' \mathbf{e}_{(i+j+k+2d) \bmod m}$; the right part is equal to $\lambda'' \mathbf{e}_{(i+j+k+2d) \bmod m}$. One can show that $\lambda' = \lambda''$. Indeed, defining variables $i' = t(i+d) \bmod m$, $j' = t(j+d) \bmod m$, and $k' = t(k+d) \bmod m$ $(0 \leqslant i', j', k' \leqslant m-1)$, one can represent formula (6) in the following form:

$$\mathbf{e}_i\mathbf{e}_j = \begin{cases} \mathbf{e}_{(i+j+d) \bmod m}, & \text{if } i' + j' < m; \\ \lambda_t \mathbf{e}_{(i+j+d) \bmod m}, & \text{if } i' + j' \geqslant m. \end{cases}$$

Using variables i', j', and k' it is easy to show: i) multiplication of the product $\mathbf{e}_i\mathbf{e}_j$ by $\mathbf{e}_k$ contributes the structural constant λ_t as a scalar multiplier, if $(i'+j') \bmod m + k' \geqslant m$; ii) multiplication of $\mathbf{e}_i$ by the product $\mathbf{e}_j\mathbf{e}_k$ contributes a scalar multiplier λ_t, if $i' + (j'+k') \bmod m \geqslant m$. We have the following four cases:

1. Suppose the triple (i, j, k) defines the triple (i', j', k') such that $i' + j' + k' < m$. Then $i' + j' < m$ and $j' + k' < m$, therefore, from formula (6) we have $\lambda' = 1$ and $\lambda'' = 1$.

2. If the triple (i, j, k) defines the triple (i', j', k') such that $i' + j' < m$ and $(i'+j') \bmod m + k' = i' + j' + k' \geqslant m$, then $\lambda' = \lambda_t$. To calculate λ'' one should take into account the following two subcases.

2.1. If $j' + k' < m$ (the product $\mathbf{e}_j\mathbf{e}_k$ does not include structural constant λ_t), then $i' + (j' + k') \bmod m \geqslant m$. Therefore, the product $\mathbf{e}_i\,(\mathbf{e}_j\mathbf{e}_k)$ includes structural constant λ_t and $\lambda'' = \lambda_t = \lambda'$.

2.2. If $j' + k' \geqslant m$ (the product $\mathbf{e}_j\mathbf{e}_k$ includes structural constant λ_t as a factor), then $i' + (j' + k') \bmod m = i' + j' + k' - m < m$. Therefore, $i' + (j' + k') \bmod m < m$ and the multiplication of $\mathbf{e}_i$ by $(\mathbf{e}_j\mathbf{e}_k)$ does not give additional structural constant λ_t and $\lambda'' = \lambda_t = \lambda'$.

3. Suppose the triple (i, j, k) sets the triple (i', j', k') such that $i'+j' \geqslant m$ and $(i' + j') \bmod m + k' < m$. Then we have $\lambda' = \lambda$. To calculate λ'' one should take into account the following two subcases.

3.1. If $j'+k' < m$ (the product $\mathbf{e}_j\mathbf{e}_k$ does not include structural constant λ_t), then $i' + (j' + k') \bmod m = i' + j' + k' \geqslant m$. The product $\mathbf{e}_i\,(\mathbf{e}_j\mathbf{e}_k)$ includes structural constant λ_t, therefore, $\lambda'' = \lambda_t = \lambda'$.

3.2. If $j' + k' \geqslant m$ (the product $\mathbf{e}_j\mathbf{e}_k$ includes structural constant λ_t), then $i' + (j' + k') \bmod m = i' + j' + k' - m = i' + j' - m + k' = (i' + j') \bmod m + k' < m$. Therefore, $i' + (j' + k') \bmod m < m$. Hence, the multiplication of $\mathbf{e}_i$ by $(\mathbf{e}_j\mathbf{e}_k)$ does not give additional structural constant λ_t and $\lambda'' = \lambda_t = \lambda'$.

4. The triple (i, j, k) defines the triple (i', j', k') such that $i'+j' \geqslant m$ and $(i' + j') \bmod m+k' \geqslant m$. One can easily show that $\lambda' = \lambda_t^2$ and $j'+k' \geqslant m$. The latter condition means that the product $(\mathbf{e}_j\mathbf{e}_k)$ includes the constant λ_t as a scalar factor. From the initial conditions of the fourth case we have $i' + (j' + k') \bmod m \geqslant m$. Hence, the multiplication of $\mathbf{e}_i$ by $(\mathbf{e}_j\mathbf{e}_k)$ gives the second time the scalar factor λ_t and we have $\lambda'' = \lambda_t^2 = \lambda'$.

Thus, for all cases and subcases equality $\lambda'' = \lambda'$ holds true. Therefore, for all possible triples (i, j, k) equality (4) also holds true, i.e. the multiplication operation specified by formula (6) is associative. □

Due to the following statement, formula (6) allows you to set a table with h ($h = 1, 2, \ldots, m - 1$) different distributions of structural constants for each fixed value of the parameter d.

Proposition 4.2. *Suppose $t_1, t_2, \ldots, t_h$ are h ($h = 2, 3, \ldots m - 1$) different values of parameter t, for which formula* (6) *at some fixed value of parameter d sets h different BVMTs $\mathbf{T}^{(1)}_{t_1}$, $\mathbf{T}^{(1)}_{t_2}$, $\ldots$ $\mathbf{T}^{(1)}_{t_h}$ with the fixed distribution of the basis vectors, every of which contains a unique distribution of one structural constant λ_{t_g} ($g = 1, 2, \ldots h$). Then the BVMT $\mathbf{T}^{(h)}_{t_1,t_2,\ldots t_h}$ with*

the same distribution of the basis vectors and with the said h distributions of structural constants presenting in the cells of $\mathbf{T}^{(h)}_{t_1,t_2,\dots t_h}$ *as multipliers specifies the associative multiplication operation.*

Proof. Let $\mathbf{T}^{(1)}_{t_g}$ be the BVMT generated by formula (6) with the parameter $t = t_g$. Executing the multiplication operation specified by $\mathbf{T}^{(1)}_{t_g}$, for arbitrary triple of the basis vectors $\mathbf{e}_i$, $\mathbf{e}_j$, and $\mathbf{e}_k$ we have:

$$\begin{aligned}(\mathbf{e}_i\mathbf{e}_j)\,\mathbf{e}_k &= \lambda_{t_g}^{f(i,j|t_g)}\mathbf{e}_{x_{(i,j)}}\mathbf{e}_k = \lambda_{t_g}^{f(i,j|t_g)}\lambda_{t_g}^{f(x_{(i,j)},k|t_g)}\mathbf{e}_{z_{(i,j,k)}};\\ \mathbf{e}_i\,(\mathbf{e}_j\mathbf{e}_k) &= \mathbf{e}_i\left(\lambda_{t_g}^{f(j,k|t_g)}\mathbf{e}_{y_{(j,k)}}\right) = \lambda_{t_g}^{f(j,k|t_g)}\left(\mathbf{e}_i\mathbf{e}_{y_{(j,k)}}\right) =\\ &= \lambda_{t_g}^{f(j,k|t_g)}\lambda_{t_g}^{f(i,y_{(j,k)}|t_g)}\mathbf{e}_{z_{(i,j,k)}},\end{aligned}$$

where the function $f\,(i,j\,|t_g)$ (with parameter t_g) in two integer variables $i,j \in \{0,1,\dots m-1$ is equal to 0 (if the cell of $\mathbf{T}^{(1)}_{t_g}$ in intersection of ith row with jth column (next, this cell will be called a [i,j]-cell) does not contain the structural constant λ_{t_g}) , or to 1 (if the [i,j]-cell of $\mathbf{T}^{(1)}_{t_g}$ contains the structural constant λ_{t_g}). Since $(\mathbf{e}_i\mathbf{e}_j)\,\mathbf{e}_k = \mathbf{e}_i\,(\mathbf{e}_j\mathbf{e}_k)$ (see proof of Proposition 3.3), for some index $x_{(i,j)}$ (depending on i and j) and some index $y_{(j,k)}$ (depending on j and k) we have

$$\lambda_{t_g}^{f(j,k|t_g)}\lambda_{t_g}^{f\left(i,y_{(j,k)}|t_g\right)}\mathbf{e}_{z_{(i,j,k)}} = \lambda_{t_g}^{f(i,j|t_g)}\lambda_{t_g}^{f\left(x_{(i,j)},k|t_g\right)}\mathbf{e}_{z_{(i,j,k)}}. \tag{7}$$

The values of $x = x(i,j)$, $y = x(j,k)$, and $z = z(i,j,k)$ do not depend on the value t_g, i.e. for the fixed value of d and fixed triple $(\mathbf{e}_i,\mathbf{e}_j,\mathbf{e}_k)$ for every of the values $t = 0,1,\dots m-1$ (including the values $t_1,t_2,\dots,t_h$) we get the same basis vector $\mathbf{e}_{z_{(i,j,k)}}$ depending on i, j, and k. Note that the [i,j]-cell of $\mathbf{T}^{(h)}_{t_1,t_2,\dots t_h}$ cotains the multiple structural constant equal to $\prod_{g=1}^{h}\lambda_{t_g}^{f(i,j\ |t_g)}$. Executing the multiplication operation specified by $\mathbf{T}^{(h)}_{t_1,t_2,\dots t_h}$, for arbitrary triple of the basis vectors $\mathbf{e}_i$, $\mathbf{e}_j$, and $\mathbf{e}_k$ we have:

$$(\mathbf{e}_i\mathbf{e}_j)\,\mathbf{e}_k = \left(\prod_{g=1}^{h}\lambda_{t_g}^{f(i,j|t_g)}\right)\mathbf{e}_{x_{(i,j)}}\mathbf{e}_k = \\ = \left(\prod_{g=1}^{h}\lambda_{t_g}^{f(i,j|t_g)}\right)\left(\prod_{g=1}^{h}\lambda_{t_g}^{f(x_{(i,j)},k|t_g)}\right)\mathbf{e}_{z_{(i,j,k)}};$$

$$\mathbf{e}_i\,(\mathbf{e}_j\mathbf{e}_k) = \mathbf{e}_i\left(\prod_{g=1}^{h}\lambda_{t_g}^{f(j,k|t_g)}\right)\mathbf{e}_{y_{(j,k)}} = \left(\prod_{g=1}^{h}\lambda_{t_g}^{f(j,k|t_g)}\right)\mathbf{e}_i\mathbf{e}_{y_{(j,k)}} = \\ = \left(\prod_{g=1}^{h}\lambda_{t_g}^{f(j,k|t_g)}\right)\left(\prod_{g=1}^{h}\lambda_{t_g}^{f(i,y_{(j,k)}|t_g)}\right)\mathbf{e}_{z_{(i,j,k)}}.$$

Taking into account equality (7), you get $(\mathbf{e}_i\mathbf{e}_j)\,\mathbf{e}_k = \mathbf{e}_i\,(\mathbf{e}_j\mathbf{e}_k)$ for all possible triples of basis vectors, i.e. the multiplication operation specified by $\mathbf{T}^{(h)}_{t_1,t_2,\ldots t_h}$ is associative (see formulas (1) and (4)). □

The following formula (8) and Proposition 4.3 are evident extensions of the formula (6) and Proposition 4.1, correspondingly:

$$\mathbf{e}_i\mathbf{e}_j = \begin{cases} \lambda'_t\mathbf{e}_{(i+j+d) \bmod m}, & \text{if } t(i+d) \bmod m + t(j+d) \bmod m < m; \\ \lambda_t\mathbf{e}_{(i+j+d) \bmod m}, & \text{if } t(i+d) \bmod m + t(j+d) \bmod m \geqslant m, \end{cases} \tag{8}$$

Proposition 4.3. *The BVMTs with two independent structural constants λ_t and $\lambda_t{}'$ distributions of which are specified by formula* (8) *set associative multiplication operation.*

Proof. The proof is almost the same as the proof of Proposition 4.1. □

It is also easy to see that Proposition 4.2 can be extended to the case of BVMTs with arbitrary fixed distribution of basis vectors and arbitrary number of distributions of structural constants, every of which specifies the associative multiplication operation (including the case of BVMTs generated by formula (8)).

Thus, the use of formula (8) provides possibility to specify BVMTs with $2m-2$ independent structural constants, i.e. to specify vector finite fields $GF\left((p^s)^m\right)$ with $O\left((p^s)^{2m-2}\right)$, where $O(\cdot)$ is order notation, different modifications for the fixed values of p, s, and m, when the distribution of the

basis vectors over cells of BVMT is fixed. One should note that the value of the product of the constants λ'_t define the value of the single non-zero coordinate of the unit vector U, namely,

$$u_{(m-d) \bmod m} = \prod_{t=1}^{m-1} \lambda_t'^{-1}.$$

5. Experimental verification.

Table 1 is a particular example covered by the proposed method, which corresponds to the values $d = 0$, $t = 1$ (sets the distribution of the structural constant μ) and $t = m - 1$ (sets the distribution of the constant ϵ), except for the constant τ distribution of which was found heuristically. The value of τ determines the vector that is the global two-sided unit U: $U = \left(\tau^{-1}, 0, 0, \ldots 0\right)$. For many other cases of generating BVMTs based on the developed method, which include one to $2m - 2$ different independent structural constants, we were able to find heuristically the distribution of the additional constant τ (this distribution had a form that depended on the value of the parameter d).

In all computational experiments, setting the finite algebras over the field $GF\left(p^s\right)$ order of which satisfies the condition $m|\left(p^s - 1\right)$ we were also able to find many different sets of the values of structural constants, which defined formation of the vector finite fields $GF\left(\left(p^s\right)^m\right)$. As an experimental criterion that a specified algebra is a vector finite field, we used the fact of the existence of a vector whose order is equal to $p^{sm} - 1$.

Table 2 is generated using formula (6) and parameters $d = 0$, $t = 2$ (distribution of the constant α), $t = 3$ (distribution of ρ), $t = 4$ (distribution of δ), and $t = 5$ (distribution of λ). The two-sided unit is $E = (1, 0, 0, 0, 0, 0)$.

Example 5.1. For the case $(p, s) = (211, 1)$ and $(\alpha, \delta, \lambda, \rho) = (7, 11, 1, 1)$ Table 2 sets the vector finite field $GF\left(211^7\right)$. The vector $(1, 2, 3, 4, 5, 6, 8)$ is an element of order $211^7 - 1 = 18619893262512570$.

Example 5.2. For the case $(p, s) = (379, 1)$ and $(\alpha, \delta, \lambda, \rho) = (1, 1, 37, 3)$ Table 2 sets the vector finite field $GF\left(379^7\right)$. The vector $(11, 22, 33, 44, 55, 66, 77)$ is an element of order $379^7 - 1 = 1123244937204690258$.

Obviously, Table 2 can be supplemented with the following independent structural constants:

i) $\alpha', \delta', \lambda'$, and ρ' with distributions defined by formula (8);

ii) ϵ, μ, and τ, with distributions shown in Table 1.

Table 2

The BVMT for setting the 7-dimensional vector finite fields.

$\cdot$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$
$\mathbf{e}_1$	$\mathbf{e}_1$	$\delta\lambda\mathbf{e}_2$	$\lambda\rho\mathbf{e}_3$	$\alpha\delta\mathbf{e}_4$	$\lambda\rho\mathbf{e}_5$	$\delta\lambda\mathbf{e}_6$	$\alpha\delta\lambda\rho\mathbf{e}_0$
$\mathbf{e}_2$	$\mathbf{e}_2$	$\lambda\rho\mathbf{e}_3$	$\alpha\rho\mathbf{e}_4$	$\alpha\rho\mathbf{e}_5$	$\lambda\rho\mathbf{e}_6$	$\alpha\delta\lambda\rho\mathbf{e}_0$	$\alpha\rho\mathbf{e}_1$
$\mathbf{e}_3$	$\mathbf{e}_3$	$\alpha\delta\mathbf{e}_4$	$\alpha\rho\mathbf{e}_5$	$\alpha\delta\mathbf{e}_6$	$\alpha\delta\lambda\rho\mathbf{e}_0$	$\alpha\delta\mathbf{e}_1$	$\alpha\delta\mathbf{e}_2$
$\mathbf{e}_4$	$\mathbf{e}_4$	$\lambda\rho\mathbf{e}_5$	$\lambda\rho\mathbf{e}_6$	$\alpha\delta\lambda\rho\mathbf{e}_0$	$\lambda\rho\mathbf{e}_1$	$\delta\lambda\mathbf{e}_2$	$\lambda\rho\mathbf{e}_3$
$\mathbf{e}_5$	$\mathbf{e}_5$	$\delta\lambda\mathbf{e}_6$	$\alpha\delta\lambda\rho\mathbf{e}_0$	$\alpha\delta\mathbf{e}_1$	$\delta\lambda\mathbf{e}_2$	$\delta\lambda\mathbf{e}_3$	$\alpha\delta\mathbf{e}_4$
$\mathbf{e}_6$	$\mathbf{e}_6$	$\alpha\delta\lambda\rho\mathbf{e}_0$	$\alpha\rho\mathbf{e}_1$	$\alpha\delta\mathbf{e}_2$	$\lambda\rho\mathbf{e}_3$	$\alpha\delta\mathbf{e}_4$	$\alpha\rho\mathbf{e}_5$

Table 3 is generated using formula (8) and parameters $d = 0$, $t = 3$ (distribution of the constants α and α') and $t = 5$ (distribution of δ and δ').

Example 5.3. For the case $(p, s) = (73, 1)$ and $(\alpha, \alpha', \delta, \delta') = (17, 35, 1, 1)$ Table 3 sets the vector finite field $GF\left(73^8\right)$ with the two-sided unit $U = (48, 0, 0, 0, 0, 0, 0, 0)$. The vector $(1, 2, 3, 4, 5, 6, 7, 8)$ is an element of order $73^8 - 1 = 806460091894080$ which is a generator of the multiplicative group of the field $GF\left(73^8\right)$.

Example 5.4. For the case $(p, s) = (113, 1)$ and $(\alpha, \alpha', \delta, \delta') = (48, 107, 27, 1)$ Table 3 sets the vector finite field $GF\left(113^8\right)$ with the two-sided unit $U = (94, 0, 0, 0, 0, 0, 0, 0)$. The vector $(1, 2, 3, 4, 5, 6, 7, 8)$ is a generator of the multiplicative group of the field $GF\left(113^8\right)$.

Table 3

The BVMT for setting the 8-dimensional vector finite fields.

$\cdot$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$	$\mathbf{e}_7$
$\mathbf{e}_0$	$\alpha'\delta'\mathbf{e}_0$	$\alpha'\delta'\mathbf{e}_1$	$\alpha'\delta'\mathbf{e}_2$	$\alpha'\delta'\mathbf{e}_3$	$\alpha'\delta'\mathbf{e}_4$	$\alpha'\delta'\mathbf{e}_5$	$\alpha'\delta'\mathbf{e}_6$	$\alpha'\delta'\mathbf{e}_7$
$\mathbf{e}_1$	$\alpha'\delta'\mathbf{e}_1$	$\alpha'\delta\mathbf{e}_2$	$\alpha\delta'\mathbf{e}_3$	$\alpha'\delta\mathbf{e}_4$	$\alpha'\delta\mathbf{e}_5$	$\alpha\delta'\mathbf{e}_6$	$\alpha'\delta\mathbf{e}_7$	$\alpha\delta\mathbf{e}_0$
$\mathbf{e}_2$	$\alpha'\delta'\mathbf{e}_2$	$\alpha\delta'\mathbf{e}_3$	$\alpha\delta'\mathbf{e}_4$	$\alpha'\delta\mathbf{e}_5$	$\alpha\delta'\mathbf{e}_6$	$\alpha\delta'\mathbf{e}_7$	$\alpha\delta\mathbf{e}_0$	$\alpha\delta'\mathbf{e}_1$
$\mathbf{e}_3$	$\alpha'\delta'\mathbf{e}_3$	$\alpha'\delta\mathbf{e}_4$	$\alpha'\delta\mathbf{e}_5$	$\alpha'\delta\mathbf{e}_6$	$\alpha'\delta\mathbf{e}_7$	$\alpha\delta\mathbf{e}_0$	$\alpha'\delta\mathbf{e}_1$	$\alpha'\delta\mathbf{e}_2$
$\mathbf{e}_4$	$\alpha'\delta'\mathbf{e}_4$	$\alpha'\delta\mathbf{e}_5$	$\alpha\delta'\mathbf{e}_6$	$\alpha'\delta\mathbf{e}_7$	$\alpha\delta\mathbf{e}_0$	$\alpha\delta'\mathbf{e}_1$	$\alpha'\delta\mathbf{e}_2$	$\alpha\delta'\mathbf{e}_3$
$\mathbf{e}_5$	$\alpha'\delta'\mathbf{e}_5$	$\alpha\delta'\mathbf{e}_6$	$\alpha\delta'\mathbf{e}_7$	$\alpha\delta\mathbf{e}_0$	$\alpha\delta'\mathbf{e}_1$	$\alpha\delta'\mathbf{e}_2$	$\alpha\delta'\mathbf{e}_3$	$\alpha\delta'\mathbf{e}_4$
$\mathbf{e}_6$	$\alpha'\delta'\mathbf{e}_6$	$\alpha'\delta\mathbf{e}_7$	$\alpha\delta\mathbf{e}_0$	$\alpha'\delta\mathbf{e}_1$	$\alpha'\delta\mathbf{e}_2$	$\alpha\delta'\mathbf{e}_3$	$\alpha'\delta\mathbf{e}_4$	$\alpha'\delta\mathbf{e}_5$
$\mathbf{e}_7$	$\alpha'\delta'\mathbf{e}_7$	$\alpha\delta\mathbf{e}_0$	$\alpha\delta'\mathbf{e}_1$	$\alpha'\delta\mathbf{e}_2$	$\alpha\delta'\mathbf{e}_3$	$\alpha\delta'\mathbf{e}_4$	$\alpha'\delta\mathbf{e}_5$	$\alpha\delta'\mathbf{e}_6$

Table 4, where $\tau' = \tau^{-1}$, presents a case with additional constant τ (found heuristically). Distribution of the basis vectors and of the constants α $(t = 5)$ and δ $(t = 4)$ corresponds to formula (6) with the parameter $d = 4$. The two-sided unit is the vector $U = (0, 0, 0, 0, \tau^{-1}, 0, 0, 0)$.

Table 4

The BVMT $(m = 8;\ d = 4)$ with distribution of the heuristic constant τ.

$\cdot$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$	$\mathbf{e}_7$
$\mathbf{e}_0$	$\alpha\tau'\mathbf{e}_4$	$\mathbf{e}_5$	$\alpha\mathbf{e}_6$	$\mathbf{e}_7$	$\tau\mathbf{e}_0$	$\alpha\mathbf{e}_1$	$\mathbf{e}_2$	$\alpha\mathbf{e}_3$
$\mathbf{e}_1$	$\mathbf{e}_5$	$\delta\mathbf{e}_6$	$\mathbf{e}_7$	$\delta\mathbf{e}_0$	$\tau\mathbf{e}_1$	$\delta\mathbf{e}_2$	$\mathbf{e}_3$	$\alpha\delta\tau'\mathbf{e}_4$
$\mathbf{e}_2$	$\alpha\mathbf{e}_6$	$\mathbf{e}_7$	$\alpha\mathbf{e}_0$	$\alpha\mathbf{e}_1$	$\tau\mathbf{e}_2$	$\alpha\mathbf{e}_3$	$\alpha\tau'\mathbf{e}_4$	$\alpha\mathbf{e}_5$
$\mathbf{e}_3$	$\mathbf{e}_7$	$\delta\mathbf{e}_0$	$\alpha\mathbf{e}_1$	$\delta\mathbf{e}_2$	$\tau\mathbf{e}_3$	$\alpha\delta\tau'\mathbf{e}_4$	$\mathbf{e}_5$	$\alpha\delta\mathbf{e}_6$
$\mathbf{e}_4$	$\tau\mathbf{e}_0$	$\tau\mathbf{e}_1$	$\tau\mathbf{e}_2$	$\tau\mathbf{e}_3$	$\tau\mathbf{e}_4$	$\tau\mathbf{e}_5$	$\tau\mathbf{e}_6$	$\tau\mathbf{e}_7$
$\mathbf{e}_5$	$\alpha\mathbf{e}_1$	$\delta\mathbf{e}_2$	$\alpha\mathbf{e}_3$	$\alpha\delta\tau'\mathbf{e}_4$	$\tau\mathbf{e}_5$	$\alpha\delta\mathbf{e}_6$	$\mathbf{e}_7$	$\alpha\delta\mathbf{e}_0$
$\mathbf{e}_6$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\alpha\tau'\mathbf{e}_4$	$\mathbf{e}_5$	$\tau\mathbf{e}_6$	$\mathbf{e}_7$	$\mathbf{e}_0$	$\alpha\mathbf{e}_1$
$\mathbf{e}_7$	$\alpha\mathbf{e}_3$	$\alpha\delta\tau'\mathbf{e}_4$	$\alpha\mathbf{e}_5$	$\alpha\delta\mathbf{e}_6$	$\tau\mathbf{e}_7$	$\alpha\delta\mathbf{e}_0$	$\alpha\mathbf{e}_1$	$\alpha\delta\mathbf{e}_2$

6. Conclusion

The proposed unified method for setting a class of BVMT with parameterized distributions of the basis vectors and of the structural constants is of significant interest for application in the development of the multivariate cryptography algorithms, since it eliminates some limitations that occur with the computationally heuristic method of specifying vector finite fields of large dimensions. However, the latter can be used to search for additional structural constants whose distributions are not covered by the developed method, like constant τ in Tables 1 and 4. The search for parameterizable unified methods for setting BVMTs of new types is also of interest.

Acknowledgement. The author sincerely thanks the anonymous Referee for his valuable comments due to which the content of the article has been sigificantly improved.

References

[1] **J. Ding, A. Petzoldt**, *Current state of multivariate cryptography*, IEEE Security and Privacy Magazine, **15** (2017), no. 4, 28 – 36.

[2] **J. Ding, A. Petzoldt, D.S. Schmidt**, *Multivariate Public Key Cryptosystems. Advances in Information Security.* Springer. New York. **80** (2020).

[3] **J.-C. Faugére**, *A new efficient algorithm for computing Gröbner basis* ($F4$), *J. Pure Appl. Algebra*, **139** (1999), no. 1-3, 61 – 88

[4] **J.-C. Faugére**, *A new efficient algorithm for computing Grőbner basis without reduction to zero* ($F5$), In: Proceedings of the International Symposium on Symbolic and Algebraic Computation, (2002) p. 75–83, 2002.

[5] **A.A. Moldovyan, N.A. Moldovyan**, *Vector finite fields of characteristic two as algebraic support of multivariate cryptography*, Computer Sci. J. Moldova. **32** (2024), no. 1(94), 46 – 60.

[6] **D.N. Moldovyan**, *A unified method for setting finite none-commutative associative algebras and their properties*, Quasigroups and Related Systems, **27** (2019), no. 2, 293 – 308.

[7] **N.A. Moldovyan**, *Unifed method for defining fnite associative algebras of arbitrary even dimensions*, Quasigroups and Related Systems, **26** (2018), no. 2, 263 – 270.

[8] **N.A. Moldovyan, D.N. Moldovyan**, *A novel method for developing post-quantum cryptoschemes and a practical signature algorithm*, Applied Computing and Informatics, (2021). DOI: 10.1108/ACI-02-2021-0036

[9] **N.A. Moldovyan, P.A. Moldovyanu**, *Vector form of the finite fields* $GF(p^m)$, Bull. Acad. Sci. Moldova. Mathematics. (2009), no. 3(61), 57 – 63.

[10] *Post-Quantum Cryptography. 13th International Workshop, PQCrypto 2022*, Lecture Notes Computer Sci., **13512**, (2022).

[11] **Q. Shuaiting, H. Wenbao, Li Yifa, J. Luyao**, *Construction of extended multivariate public key cryptosystems*, Intern. J. Network Security, **18** (2016), no. 1, 60 – 67.

Received June 01, 2024

St. Petersburg Federal Research Center of the Russian Academy of Sciences
14-th line 39, 199178, St. Petersburg, Russia
e-mail: nmold@mail.ru