UDC 512.552+003.26
MSC 16P10

Parameterized unified method for setting vector finite fields for multivariate cryptography[*]

A. A. Moldovyan, N. A. Moldovyan

St. Petersburg Federal Research Center of the Russian Academy of Sciences,
39, 14-ya liniya V. O., St. Petersburg, 199178, Russian Federation

For citation: Moldovyan A. A., Moldovyan N. A. Parameterized unified method for setting vector finite fields for multivariate cryptography. *Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes*, 2024, vol. 20, iss. 4, pp. 479–486. https://doi.org/10.21638/spbu10.2024.404

One of attractive paradigms of the public key multivariate cryptography is connected with application of the exponentiation operations in vector finite fields of different dimensions. The computationally heuristic method of specifying vector finite fields with a large number of implemented modifications is a problematic area of this paradigm. In this regard, a formalized method for the unified construction of vector finite fields is proposed.

Keywords: finite associative algebra, commutative algebra, vector finite field, power polynomials, exponentiation operation, post-quantum cryptography, multivariate cryptography.

1. Introduction. At present development of practical post-quantum public key cryptographic algorithms is a challenge of theoretical and practical cryptography [1, 2]. Multivariate public key cryptography (MPC) [3] represents an attractive direction of post-quantum cryptography. However, the size of public key in the MPC algorithms is extremely large. This fact introduces significant restrictions on the application areas of the said algorithms. A new method for developing the MPC algorithms has been introduced in the recent article [4], which allows for a potential public key size reduction of 10 times or more as compared with the known MPC algorithms for a fixed value of security level. The idea of that method is to construct the nonlinear mapping (used as public key in the form of a set of polynomials in many variables) with a secret trapdoor by an exponentiation operation in a vector finite field [5].

The article [4] presents the implementation of nonlinear mappings with a secret trapdoor using the vector finite fields in the form of m-dimensional finite commutative associative algebras in which the multiplication operation is defined by basis vector multiplication tables (BVMT) constructed using a computationally heuristic method. Expanding the capabilities of the paradigm by [4] is associated with the development of formalized methods for specifying vector finite fields, which will significantly increase the number of modifications of the latter, especially in the case of large values of m. For a fixed distribution of the basis vectors in a BVMT the number of the vector finite field modifications increases with the number of structural constants in the BVMT. Therefore, when developing formalized unified methods for constructing BVMTs (like methods from articles [6, 7]), one should provide for the possibility of parameterized specifying various distributions of structural constants across cells of BVMTs.

[*] This work was financially supported by the Russian Science Foundation, project no. 24-41-04006, https://rscf.ru/project/24-41-04006.

This article introduces a formalized unified method for costructing parameterizable BVMTs setting vector finite fields of dimensions m such that the number $m+1$ is prime. The unification of constructing BVMTs consists of using a single mathematical formula for the case of a given series of dimension values m, which is included in the formula as one of the parameters. Parameterizability consists in specifying the distribution of basis vectors and structural constants across BVMT cells depending on the second and third parameter of the said formula, correspondingly. By fixing the first two parameters and changing the third parameter, we get the opportunity to construct BVMTs with many structural constants that have different distributions, which determines a large number of possible modifications of vector finite fields of a given type.

2. Preliminaries. Consider representation of an m-dimensional vector A in the next two forms: i) $A=(a_1,a_2,\ldots,a_m)$ and ii) $A=\sum_{i=1}^{m}a_i\mathbf{e}_i$, where $a_1,a_2,\ldots,a_m\in GF\left(p^s\right)$ are coodinates; $\mathbf{e}_1$, $\mathbf{e}_2$, ..., $\mathbf{e}_m$ are basis vectors. If in an m-dimensional vector space (with operations of addition of vectors and of scalar multiplication) the vector multiplication operation is defined so that it is closed and distributive at the left and at the right relatively the addition operation, then we get a finite m-dimensional algebra (over some field $GF\left(p^s\right)$ with prime p and natural number s).

For example, the multiplication operation of two m-dimensional vectors A and B can be defined by the following formula:

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

where every of the products $\mathbf{e}_i\mathbf{e}_j$ is replaced by a single-component vector $\lambda\mathbf{e}_k$ that is indicated in the intersection of the i^{th} row and j^{th} column of some BVMT [7].

In order to be able to define finite algebras that are fields, a necessary condition is the use of BVMTs that define the commutative associative operation of multiplication. However, this condition is not sufficient, which is confirmed by the BVMTs presented in the article [8]. An example of BVMTs of a general form for the case of different dimensions, according to which vector finite fields can be specified, is presented in [5]. The last article also formulated another necessary condition, which is that the value p^s-1 is divisible by m. Vector finite fields are not formed for all sets of values of structural constants present in the BVMTs. The required set of values of the constants is generated randomly, and the criterion for the formation of a vector finite fields is the presence of a vector of the order equal to $p^{sm}-1$.

In the MPC algorithms, the public key is formed as a set of u power (quadratic or cubic) polynomials in n variables, which define a hard to reverse non-linear mapping $\Psi:\mathbb{F}_q^n\to\mathbb{F}_q^u$ with a secret trapdoor. The public encryption is performed as mapping $Y=\Pi(X)$ of the plaintext represented in the form of n-dimensional vector $X=(x_1,x_2,\ldots,x_n)$ over a finite field $\mathbb{F}_q$ of relatively small order q, coordinates of which are variables in the polynomials of the public key. The ciphertext represents a u-dimensional ($u\geqslant n$) vector $Y=(y_1,y_2,\ldots,y_u)$ over $\mathbb{F}_q$ [9, 10]. Suppose a public key Π includes the polinomials $f_i\left(x_0,x_1,\ldots,x_{n-1}\right)$, where $i=1,2,\ldots,u$. Then for a given vector X we can calculate u values $y_1=f_1$, $y_2=f_2$, ..., $y_u=f_u$. Considering the latter values as coordinates of the vector Y we get the image Y of the vector X.

Usually the public key is generated in the following way. A set of u power polynomials $f_j^{(1)}$ ($j=1,2,\ldots,u$) in n variables is composed, which defines the mapping $\Psi(X)$ for which it is easy to find a computationally efficient inverse mapping $\Psi^{-1}(Y)$. Then, using a secret linear mapping $\Lambda:\mathbb{F}_q^u\to\mathbb{F}_q^u$, which is specified as a set of u linear polynomials $f_j^{(2)}$ over the finite field $\mathbb{F}_q$, and the set of polynomials $f_j^{(1)}$, it is calculated the set of polinomials f_i, which defined the mapping $\Pi(X) = \Lambda(\Psi(X))$ with a secret trapdoor, the latter being the knowledge of the mappings Ψ and Λ which provide possibility to reverse Π, i.e. to compute pre-image X as follows:

$$X = \Pi^{-1}(Y) = \Psi^{-1}\left(\Lambda^{-1}(Y)\right).$$

The sense of using a linear mapping is to mask the nonlinear mapping Ψ, for which the inverse mapping Ψ^{-1} can easily be found (in some MPC algorithms two masking linear mappings are used). The use of masking linear mappings results in the size of the public key being extremely large. A direct attack on the MPC algorithms consists in reversing the mapping Π by the way of solving a system of u power equations with set of n unknowns $\{x_1, x_2, \ldots, x_n\}$. The best methods for solving such systems use so called algorithms F4 [11] and F5 [12]. To ensure security level (to direct atacks) 2^{80} to 2^{256} the public key should include 26 to 110 power polynomials [9].

A novel method for developing the MPC algorithms has been proposed recently in [4] for significantly reducing the public key size (by a factor of 10 or more). That method consists of implementing the set of power polynomials of the mapping Ψ determined by one or several exponentiation operations to a small degree. The paradigm by [4] allows eliminating the use of masking mappings that significantly increase the public key size. The inverse mapping Ψ^{-1} arises naturally as the operation of extracting roots (of respective degrees) in vector finite fields known only to the owner of the public key. A topology of a mapping Ψ is considered in [4], which includes exponentiation operations in 5-dimensional and 17-dimensional vector finite fields. In that topology the linear mapping (permutation of the coordinates of the transformed vectors) is also used, which, however, do not increase the size of public key. When using a single vector finite field, dimension of the latter is to be from 5 to 110 depending on the required security level.

For the MPC algorithms developed in line with the paradigm by [4], a common structural attack is calculation of the parameters of the secret modifications of the vector finite fields used to specify hard to inverse non-linear mapping Π by the known coefficients of the polynomials of the public key Π. Adding to the security to this structural attack can be provided by increasing the number of independent structural constants present in the BVMT by which the vector finite field is defined.

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 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 a large number of structural constants. In the paradigm by [4] it is assumed to use exponention 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 a 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 a large number of independent structural constants and finding the distributions of the latter. The Section 3 proposes a unified method for specifying BVMTs with parameterized distribution of the basis 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.

3. Specifying distribution of basis vectors. Using formula (1) one can easily show that a given BVMT defines associative multiplication operation, if the following equality holds for all possible triples $(\mathbf{e}_i, \mathbf{e}_j, \mathbf{e}_k)$:

$$(\mathbf{e}_i\mathbf{e}_j)\,\mathbf{e}_k = \mathbf{e}_i\,(\mathbf{e}_j\mathbf{e}_k)\,. \tag{2}$$

For dimensions m such that the value $m+1$ is prime, one can propose the common mathematical formula for generating BVMTs defining commutative associative algebras:

$$\mathbf{e}_i\mathbf{e}_j = \mathbf{e}_{(ijd) \bmod (m+1)}, \tag{3}$$

where parameter $d = 1, 2, \ldots, m$ specifies m different distributions of the basis vectors (i.e. m different BVMTs) for a fixed value of m. Table 1 shows the dimension values covered by formula (3) representing interest for specifying the vector finite field in the framework of the paradigm by [4]. The Proposition 1 is evident.

Table 1. **Values of m for defining vector finite fields with formulas (4) and (5)**

m	4	6	10	12	16	18	22	28	30	36	40	42	46	52	58
$m+1$	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59
m	60	66	70	72	78	82	88	96	100	102	106	108	112	126	130
$m+1$	61	67	71	73	79	83	89	97	101	103	107	109	113	127	131

Proposition 1. The BVMTs constructed by formula (3) specify commutative multiplication operation for arbitrary fixed values of the parameters m and d.

Proposition 2. The BVMT generated by formula (3) for arbitrary fixed values of the parameters m and d defines 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, $u_{d^{-1} \bmod (m+1)} = 1$.

Proof. Using formula (1) one can write

$$UA = AU = \sum_{i=1}^{m}\sum_{j=1}^{m} a_i u_j (\mathbf{e}_i\mathbf{e}_j) = \sum_{i=1}^{m}\sum_{j=1}^{m} a_i u_j \mathbf{e}_{(ijd) \bmod (m+1)} =$$

$$= \sum_{i=1}^{m} a_i u_{d^{-1} \bmod (m+1)} \mathbf{e}_{(id^{-1}d) \bmod (m+1)} = \sum_{i=1}^{m} a_i \mathbf{e}_i = A.$$

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

Proposition 3. The BVMTs constructed by formula (3) 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 (2) one gets:

$$(\mathbf{e}_i\mathbf{e}_j)\,\mathbf{e}_k = \mathbf{e}_{(ijd) \bmod (m+1)}\mathbf{e}_k = \mathbf{e}_{(ijdkd) \bmod (m+1)} = \mathbf{e}_{(ijkd^2) \bmod (m+1)},$$

$$\mathbf{e}_i\,(\mathbf{e}_j\mathbf{e}_k) = \mathbf{e}_i\mathbf{e}_{(jkd) \bmod (m+1)} = \mathbf{e}_{(ijkdd) \bmod (m+1)} = \mathbf{e}_{(ijkd^2) \bmod (m+1)}.$$

Thus, equality (2) holds true for all possible triples of basis vectors, hence, the multiplication operation is associative. □

4. Specifying distribution of structural constants. To provide the possibility of including structural constants in BVMTs, the next two extentions of formula (3) are proposed:

$$\mathbf{e}_i\mathbf{e}_j = \begin{cases} \rho_t \mathbf{e}_{(ijd) \bmod (m+1)}, & \text{if } t('i + 'd) \bmod m + t('j + 'd) \bmod m < m, \\ \mathbf{e}_{(ijd) \bmod (m+1)}, & \text{if } t('i + 'd) \bmod m + t('j + 'd) \bmod m \geqslant m, \end{cases} \tag{4}$$

$$\mathbf{e}_i\mathbf{e}_j = \begin{cases} \mathbf{e}_{(ijd) \bmod (m+1)}, & \text{if } t('i + 'd) \bmod m + t('j + 'd) \bmod m < m, \\ \lambda_t \mathbf{e}_{(ijd) \bmod (m+1)}, & \text{if } t('i + 'd) \bmod m + t('j + 'd) \bmod m \geqslant m, \end{cases} \tag{5}$$

where $t = 1, 2, \dots, m-1$ is a parameter specifying distributions of two independent structural constants (λ_t and ρ_t) for every of the fixed pair of the values of the parameters d and t; $'j$ and $'d$ are indices of the respective values i, j, and d modulo $(m+1)$, the indiced being calculated for a fixed primitive element in $GF(m+1)$. Totally, for every fixed value d formulas (4) and (5) specify $2(m-1)$ distributions of independent structural constants. It is easy to see that the algebras defined by the BVMTs generated by formulas (4) and (5) are commutative and include global two-sided unit U that has the single non-zero coordinate $u_{d^{-1} \bmod (m+1)} = \rho_t^{-1}$.

Proposition 4. The BVMT generated by formula (4) for arbitrary fixed values of the parameters m, d, and t defines the finite algebra with the global two-sided unit $U = (0, \dots, \rho_t^{-1}, \dots, 0)$ with $m-1$ zero coordinates and one coordinate eqal to $\rho_t^{-1} \in GF(p^s)$, namely, $u_{d^{-1} \bmod (m+1)} = \rho_t^{-1}$.

Proof. For $j = d^{-1} \bmod (m+1)$ we have $t('j + 'd) \bmod m = 0$ and formula (4) gives $\mathbf{e}_i\mathbf{e}_j = \rho_t\mathbf{e}_i$. Using formula (1), one gets:

$$UA = AU = \sum_{i=1}^{m}\sum_{j=1}^{m} a_i u_j (\mathbf{e}_i\mathbf{e}_j) = \sum_{i=1}^{m}\sum_{j=1}^{m} a_i u_j \rho_t \mathbf{e}_{(ijd) \bmod (m+1)} =$$

$$= \sum_{i=1}^{m} a_i u_{d^{-1} \bmod (m+1)} \rho_t \mathbf{e}_{(id^{-1}d) \bmod (m+1)} = \sum_{i=1}^{m} a_i \mathbf{e}_i = A.$$

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

Proposition 5. The BVMTs with one structural constant ρ_t distribution of which is specified by formula (4) set associative multiplication operation.

Proposition 6. The BVMTs with one structural constant λ_t distribution of which is specified by formula (5) set associative multiplication operation.

Proof. Consider formula (5). Due to Proposition 3 the left part of (4) is equal to $\lambda' \mathbf{e}_{(ijkd^2) \bmod (m+1)}$ and the right part of (4) is equal to $\lambda'' \mathbf{e}_{(ijkd^2) \bmod (m+1)}$. 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 (5) in the next form:

$$\mathbf{e}_i\mathbf{e}_j = \begin{cases} \mathbf{e}_{(ijd) \bmod (m+1)}, & \text{if } i' + j' < m, \\ \lambda_t \mathbf{e}_{(ijd) \bmod (m+1)}, & \text{if } i' + j' \geqslant m. \end{cases}$$

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 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 (5) 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 next two subcases.

2.1. If $j' + k' < m$ (the product $\mathbf{e}_j\mathbf{e}_k$ does not include structural constant λ), 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 scalar multiplier 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 next 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. The multiplying $\mathbf{e}_i$ by $(\mathbf{e}_j\mathbf{e}_k)$ gives the second time the scalar factor λ_t, since from initial conditions of the fourth case we have $i' + (j' + k') \bmod m \geqslant m$. Hence, 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 (2) also holds true, i.e. the multiplication operation specified by formula (5) is associative. □

5. Experimental verification. For the values $m = 4$, 6 and 10, we experimentally constructed BVMTs corresponding to different sets of values of the parameters d and t. In all cases, in algebras defined by a BVMT with one structural constant, the multiplication operation was commutative and associative. The imposition of various distributions of structural constants (for values $t = 1$ to $m - 1$) into a single BVMT with the distribution of basis vectors, given by formula (3) for a fixed value of d, preserved the indicated properties of the multiplication operation (an expected and fairly obvious fact). The suitability of the resulting BVMTs for specifying vector finite fields by selecting random sets of values of structure constants has been experimentally confirmed. As a criterion for the formation of an algebra (over $GF\,(p^s)$), which is a finite field, we used the finding of a vector of order $p^{sm} - 1$. The single non-zero coordinate of the unit vector U is equal to $u_{d^{-1} \bmod (m+1)} = \prod_{t=1}^{m-1} \rho_t^{-1}$, where $\rho_t \in GF\,(p^s)$.

Table 2 is constructed using formulas (4) and (5) with the following values of parameters $d = 4$, $t = 1$ (distribution of the constants ρ_1 and λ_1) and $t = 5$ (distribution of ρ_5 and λ_5).

Table 2. **The BVMT defining a 6-dimensional vector finite field over $GF(103)$**

$\mathbf{e}$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$
$\mathbf{e}_1$	$\rho_1\rho_3\lambda_5\mathbf{e}_4$	$\rho_1\rho_3\rho_5\mathbf{e}_1$	$\rho_1\rho_3\lambda_5\mathbf{e}_5$	$\lambda_1\rho_3\lambda_5\mathbf{e}_2$	$\rho_1\rho_3\lambda_5\mathbf{e}_6$	$\lambda_1\rho_3\rho_5\mathbf{e}_3$
$\mathbf{e}_2$	$\rho_1\rho_3\rho_5\mathbf{e}_1$	$\rho_1\rho_3\rho_5\mathbf{e}_2$	$\rho_1\rho_3\rho_5\mathbf{e}_3$	$\rho_1\rho_3\rho_5\mathbf{e}_4$	$\rho_1\rho_3\rho_5\mathbf{e}_5$	$\rho_1\rho_3\rho_5\mathbf{e}_6$
$\mathbf{e}_3$	$\rho_1\rho_3\lambda_5\mathbf{e}_5$	$\rho_1\rho_3\rho_5\mathbf{e}_3$	$\rho_1\lambda_3\lambda_5\mathbf{e}_1$	$\rho_1\rho_3\lambda_5\mathbf{e}_6$	$\rho_1\lambda_3\lambda_5\mathbf{e}_4$	$\lambda_1\lambda_3\lambda_5\mathbf{e}_2$
$\mathbf{e}_4$	$\lambda_1\rho_3\lambda_5\mathbf{e}_2$	$\rho_1\rho_3\rho_5\mathbf{e}_4$	$\rho_1\rho_3\lambda_5\mathbf{e}_6$	$\lambda_1\rho_3\rho_5\mathbf{e}_1$	$\lambda_1\rho_3\rho_5\mathbf{e}_3$	$\lambda_1\rho_3\rho_5\mathbf{e}_5$
$\mathbf{e}_5$	$\rho_1\rho_3\lambda_5\mathbf{e}_6$	$\rho_1\rho_3\rho_5\mathbf{e}_5$	$\rho_1\lambda_3\lambda_5\mathbf{e}_4$	$\lambda_1\rho_3\rho_5\mathbf{e}_3$	$\lambda_1\lambda_3\lambda_5\mathbf{e}_2$	$\lambda_1\lambda_3\rho_5\mathbf{e}_1$
$\mathbf{e}_6$	$\lambda_1\rho_3\rho_5\mathbf{e}_3$	$\rho_1\rho_3\rho_5\mathbf{e}_6$	$\lambda_1\lambda_3\lambda_5\mathbf{e}_2$	$\lambda_1\rho_3\rho_5\mathbf{e}_5$	$\lambda_1\lambda_3\rho_5\mathbf{e}_1$	$\lambda_1\lambda_3\rho_5\mathbf{e}_4$

Example 1. For the case $(\rho_1, \lambda_1) = (71, 29)$ and $\rho_3 = \lambda_3 = \rho_5 = \lambda_5 = 1$ Table 2 sets the vector finite field $GF\left(103^6\right)$ with the two-sided unit $(0, 74, 0, 0, 0, 0)$. The vector $(1, 2, 3, 4, 5, 6)$ is an element of the order $103^6 - 1 = 1194052296528$.

Example 2. For the case $(\rho_5, \lambda_5) = (91, 77)$ and $\rho_1 = \lambda_1 = \rho_3 = \lambda_3 = 1$ Table 2 sets the vector finite field $GF\left(103^6\right)$ with the two-sided unit $(0, 60, 0, 0, 0, 0)$. The vector $(1, 2, 3, 4, 5, 6)$ is an element of the order $103^6 - 1$.

Example 3. For the case $(\lambda_1, \lambda_3, \lambda_5) = (35, 19, 13)$ and $\rho_1 = \rho_3 = \rho_5 = 1$ Table 2 sets the vector finite field $GF\left(103^6\right)$ with the two-sided unit $(0, 1, 0, 0, 0, 0)$. The vector $(1, 2, 3, 4, 5, 6)$ is an element of the order $103^6 - 1$.

6. Conclusion. The introduced unified method with paramerization of distributions of basis vectors and structural constants suites well for designing non-linear hard to inverse mappings Π with secret trapdoor implemented as exponentiation operations in vector finite fields with a secret set of structural constants. Depending on the used topology of the Π mapping the vector finite fields of dimensions 6 to 102 can be potentially applied, when implementing the paradigm by [4] for developing the MPC algorithms. Seach for other parameterized unified methods for generating BVMTs for the same destination also represents interest. One of research tasks is finding additional distributions of structural constants in BVMTs generated by the introduced method (possibly by a heuristic way).

A task representing independent interest is to develop a theoretic criterion for suitability of a BVMT with the given distribution of the basis vectors for specifying vector finite fields.

References

1. Alagic G., Cooper D., Dang Q., Dang T., Kelsey J., Lichtinger J., Liu Y., Miller C., Moody D., Peralta R., Perlner R., Robinson A., Smith-Tone D., Apon D. *Status report on the third round of the NIST post-quantum cryptography standardization process.* NIST Interagency/Internal Report (NISTIR). Gaithersburg, MD, National Institute of Standards and Technology Publ., 2022, 90 p. https://doi.org/10.6028/NIST.IR.8413

2. *Post-Quantum Cryptography.* 13th International Workshop, PQCrypto 2022, Virtual Event, September 28–30, 2022. Proceedings. Lecture Notes in Computer Science. New York, Springer Verlag, 2022, vol. 13512, 523 p.

3. Ding J., Petzoldt A., Schmidt D. S. *Multivariate public key cryptosystems. Advances in information security.* New York, Springer, 2020, vol. 80, 253 p. https://doi.org/10.1007/978-1-0716-0987-3

4. Moldovyan A. A., Moldovyan N. A. Vector finite fields of characteristic two as algebraic support of multivariate cryptography. *Computer Science Journal of Moldova*, 2024, vol. 32, no. 1 (94), pp. 46–60. https://doi.org/10.56415/csjm.v32.04

5. Moldovyan N. A., Moldovyanu P. A. Vector form of the finite fields $GF\left(p^m\right)$. *Bulletin of Academy of Sciences of Moldova. Mathematics*, 2009, no. 3 (61), pp. 57–63.

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

7. Moldovyan N. A. A unified method for setting finite non-commutative associative algebras and their properties. *Quasigroups and Related Systems*, 2018, vol. 26, no. 2, pp. 263–270.

8. Moldovyan N. A., Moldovyan D. N. A novel method for developing post-quantum cryptoschemes and a practical signature algorithm. *Applied Computing and Informatics*, 2021. https://doi.org/10.1108/ACI-02-2021-0036

9. Ding J., Petzoldt A. Current state of multivariate cryptography. *IEEE Security and Privacy Magazine*, 2017, vol. 15, no. 4, pp. 28–36.

10. Shuaiting Q., Wenbao H., Li Y., Luyao J. Construction of extended multivariate public key cryptosystems. *International Journal of Network Security*, 2016, vol. 18, no. 1, pp. 60–67.

11. Faugére J.-C. A new efficient algorithm for computing Grőbner basis (F4). *Journal of Pure Appl. Algebra*, 1999, vol. 139, no. 1–3, pp. 61–88.

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

Received: June 17, 2024.
Accepted: October 4, 2024.

Authors' information:

Alexandr A. Moldovyan — Dr. Sci. in Engineering, Professor, Chief Researcher; https://orcid.org/0000-0001-5480-6016, maa1305@yandex.ru

Nikolay A. Moldovyan — Dr. Sci. in Engineering, Professor, Chief Researcher; https://orcid.org/0000-0002-4483-5048, nmold@mail.ru

Параметризованный унифицированный метод задания векторных конечных полей для многомерной криптографии[*]

А. А. Молдовян, Н. А. Молдовян

Санкт-Петербургский Федеральный исследовательский центр РАН,
Российская Федерация, 199178, Санкт-Петербург, 14-я линия В. О., 39

Для цитирования: *Moldovyan A. A., Moldovyan N. A.* Parameterized unified method for setting vector finite fields for multivariate cryptography // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2024. Т. 20. Вып. 4. С. 479–486. https://doi.org/10.21638/spbu10.2024.404

Одна из привлекательных парадигм многомерной криптографии с открытым ключом связана с применением операций возведения в степень в векторных конечных полях различных размерностей. Проблемной областью данной парадигмы является вычислительно-эвристический метод задания векторных конечных полей с большим количеством реализуемых модификаций. В связи с этим предлагается формализованный метод унифицированного построения векторных конечных полей.

Ключевые слова: конечная ассоциативная алгебра, коммутативная алгебра, векторное конечное поле, степенные многочлены, операция экспоненциирования, постквантовая криптография, многомерная криптография.

Контактная информация:

Молдовян Александр Андреевич — д-р техн. наук, проф., гл. науч. сотр.; https://orcid.org/0000-0001-5480-6016, maa1305@yandex.ru

Молдовян Николай Андреевич — д-р техн. наук, проф., гл. науч. сотр.; https://orcid.org/0000-0002-4483-5048, nmold@mail.ru

[*] Исследование выполнено за счет гранта Российского научного фонда № 24-41-04006, https://rscf.ru/project/24-41-04006/.