BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 3(103), 2023, Pages 80–89
ISSN 1024–7696, E-ISSN 2587–4322

Finite algebras in the design of multivariate cryptography algorithms

Nikolay A. Moldovyan

Abstract. A new approach to the design of multivariate public-key cryptalgorithms is introduced. It envisages using non-linear mappings defined as squaring and cubic operations in finite fields represented as finite algebras. The developed approach allows significant reduction of the size of public key and thereby make post-quantum algorithms of multivariate cryptography much more practical. In the developed algorithms, the secret key includes a set of values of structural constants that determine the modifications of the finite fields used and the coefficients in the set of sixth degree polynomials that make up the public key.

Mathematics subject classification: 68P25, 68Q12, 68R99, 94A60, 16Z05, 14G50.
Keywords and phrases: finite fields, finite algebras, non-linear mapping, power polynomials, system of power equations, post-quantum cryptography, signature algorithm, public encryption system.

Introduction

The security of multivariate cryptography algorithms is based on the computational complexity of solving systems of many power (usually quadratic) equations with many unknowns. For solving the latter problem a quantum computer is not efficient, therefore the multivariate public-key cryptalgorithms (MPC) are post-quantum ones [1], and multivariate cryptography represents significant interest for practical application in the coming postquantum era [2, 3]. However, from a practical point of view, the MPC algorithms have a significant drawback, which is the extremely large size of the public key (up to several megabytes at a security level of 2^{256}).

The present paper introduces a new approach to the development of MPC algorithms, which allows reducing the size of the public key by 20 times or more at a given level of security. The proposed approach is characterized by the use of a non-linear mapping specified in the form of exponentiation operations to the second and third powers in finite fields $GF(p^m)$ set in the form of finite algebras [4]. The latter allows you to specify the calculation of the result of the said operations in the form of calculating the values of u polynomials of the second and third degrees, which are set over $GF(p)$. Such possibility, provided by the vector form of finite fields, is exploited in the proposed approach to development of the MPC algorithms.

DOI: https://doi.org/10.56415/basm.y2023.i3.p80

1 Preliminaries

In the MPC algorithms, the public key is calculated in the form of a set of power (usually quadratic and sometimes cubic) polynomials over a finite field $GF(q)$ (of rather small order $q = 4$ to 256) that specify a non-linear mapping Π of an input n-dimensional vector into a u-dimentional output vector ($u \geq n$) [1,5]. The coordinates of the input vector are variables in the polynomials. The coordinates of the output vector are computed as values of polynomials. The mapping Π is difficult to reverse, but it includes a secret trapdoor known to the owner of the public key. The latter is provided, for example, by the following method for calculating Π, which includes the next steps:

1. Compose over $GF(q)$ a set of u secret power polinomials $f'_j(x_1, x_2, \ldots, x_n)$, where $j = 1, \ldots u$, in n variables such that the non-linear mapping Ψ of the vector $X = (x_1, x_2, \ldots, x_n)$ into the vector $Y = (y_1, y_2, \ldots, y_u)$ (where $y_i = f'_i$) is easy to reverse, i. e., one can easily find a computationally efficient reverse mapping Ψ^{-1}.

2. Generate over $GF(q)$ two secret reversible matrices A and B of the sizes $n \times n$ and $u \times u$ correspondingly, which specify linear mappings Λ_1 and Λ_2 implemented by the following formulas $\Lambda_1(V) = XA$ and $\Lambda_2(Y) = YB$ describing multiplication of the vectors V and Y by matrices A and B.

3. Calculate the set of u power polinomials $f_j(x_1, x_2, \ldots, x_n)$, which specify the next non-linear mapping Π:

$$W = \Pi(V) = \Lambda_2 \circ \Psi \circ \Lambda_1(V) = \Lambda_2 \left(\Psi \left(\Lambda_1(V) \right) \right), \tag{1}$$

where $w_j = f_j$ for $j = 1, 2, \ldots u$. When Λ_1, Ψ, and Λ_2 are properly designed, the superpositon Π of these three mappings, given in the form of u power polynomials, is a computationally irreversible non-linear mapping with a secret trap door, the latter being the next superposition $\Lambda_1^{-1} \circ \Psi^{-1} \circ \Lambda_2^{-1}$ (note that Λ_2^{-1} and Λ_2^{-1} can be easily performed).

The reversible mappings Λ_1 and Λ_2 mask the structure of central non-linear mapping Ψ and are important parts of secret key (note that instead of Λ_1 and Λ_2 one can use two affine mappings). Designing an MPC is determined mainly by the construction of the central (see formula (1)) non-linear mapping Ψ [6, 7].

Using the public key Π, one can encrypt the input message represented in the form of n-dimensional vector M, producing the following ciphertext

$$C = \Pi(M).$$

The owner (and nobody other) of the public key Π decrypts the ciphertext, computing the preimage of the u-dimensional vector C by the next formula:

$$M = \Lambda_1^{-1} \circ \Psi^{-1} \circ \Lambda_2^{-1}(C).$$

To calculate a digital signature S to an electronic document M, the owner of public key Π performs the following signature generation algorithm:

1. Using a preagreed hash-function $h(\cdot)$, calculate the hash value from M and represent it in the form of u-dimensional vector H.

2. Calculate preimage S of the vector H: $S = \Lambda_1^{-1} \circ \Psi^{-1} \circ \Lambda_2^{-1}(H)$.

The signature S to the document M can be verified as follows:

1. Compute the image H' of the n-dimensional vector S: $H' = \Pi(S)$.

2. Calculate the hash value $h(M)$ and represent it as an u-dimensional vector H. If $H = H'$, then the signature S is genuine, otherwise the signature is rejected.

This article introduces a novel method for developing the MPC algorithms with a public key Π in which two different non-linear mappings Ψ_1 and Ψ_2 are specified on the base of exponentiation operations to the second and third powers in finite fields $GF(p^{m_1})$ and $GF(p^{m_2})$, where $1 < m_1 < m_2 < n$, $m_1 m_2 = n = u$. Thus, the mappings Ψ_1^{-1} and Ψ_2^{-1} can be performed using operations of finding roots of the second and third degrees in $GF(p^m)$. Such non-linear mappings provide mutual masking, therefore it is sufficient to use additionally only very simple linear mappings that do not increase the number of terms in the power polynomials specifying the public key Π. To provide possibility (requiered to specify Π as a set of power polynomials) to define non-linear mappings Ψ_1 and Ψ_2 as two sets of polynomials, the fields $GF(p^{m_1})$ and $GF(p^{m_2})$ are set in the form of finite algebras (in the vector form) over $GF(p)$.

An m-dimensional vector space over a finite field $GF(q)$, where q is a prime or a prime power, with the defined additionally multiplication operation that is left- and right-distributive over addition operation is called an m-dimensional algebra. The multiplication of two vectors $A = (a_1, a_2, a_3, a_4) = a_1\mathbf{e}_1 + a_2\mathbf{e}_2 + \cdots + a_m\mathbf{e}_m$, where $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_m$ are basis vectors, and $B = (b_1, b_2, b_3, b_4)$ is specified by the next formula:

$$AB = \sum_{i=1}^{m} \sum_{j=1}^{m} a_i b_j \left(\mathbf{e}_i \mathbf{e}_j\right),$$

where every product $\mathbf{e}_i\mathbf{e}_j$ is to be replaced by a one-component vector $\mu\mathbf{e}_k$ indicated in the cell at the intersection of the ith row and jth column of so called basis vector multilication table (BVMT). In [4] it had been shown that if $m \geq 2$ divides the value $q-1$, then it is possible to specify a BVMT such that the algebra is the finite field $GF(q^m)$. Table 1 shows the form of BVMTs with three different structural constants μ, ϵ, and τ, which was introduced for specifying the vector finite fields of arbitrary dimension $m \geq 2$.

2 Specifying the vector finite fields with large number of modifications

For a given dimension value m, there are BVMTs with different distributions of basis vectors for which vector fields can be specified. However, a particular kind of table cannot be used as a secret element because the number of these tables is relatively small. Therefore, the use of vector finite fields to set secret non-linear

Table 1

Setting the fields $GF(q^m)$ in the vector form [4] for $m \geq 2$.

$\cdot$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\cdots$	$\mathbf{e}_{m-1}$	$\mathbf{e}_m$
$\mathbf{e}_1$	$\tau\mathbf{e}_1$	$\tau\mathbf{e}_2$	$\tau\mathbf{e}_3$	$\tau\mathbf{e}_4$	$\tau\cdots$	$\tau\mathbf{e}_{m-1}$	$\tau\mathbf{e}_m$
$\mathbf{e}_2$	$\tau\mathbf{e}_2$	$\epsilon\mathbf{e}_3$	$\epsilon\mathbf{e}_4$	$\epsilon\cdots$	$\epsilon\mathbf{e}_{m-1}$	$\epsilon\mathbf{e}_m$	$\mu\epsilon\tau^{-1}\mathbf{e}_1$
$\mathbf{e}_3$	$\tau\mathbf{e}_3$	$\epsilon\mathbf{e}_4$	$\epsilon\cdots$	$\epsilon\mathbf{e}_{m-1}$	$\epsilon\mathbf{e}_m$	$\mu\epsilon\tau^{-1}\mathbf{e}_1$	$\mu\mathbf{e}_2$
$\mathbf{e}_4$	$\tau\mathbf{e}_4$	$\epsilon\cdots$	$\epsilon\mathbf{e}_{m-1}$	$\epsilon\mathbf{e}_m$	$\mu\epsilon\tau^{-1}\mathbf{e}_1$	$\mu\mathbf{e}_2$	$\mu\mathbf{e}_3$
$\cdots$	$\tau\cdots$	$\epsilon\mathbf{e}_{m-1}$	$\epsilon\mathbf{e}_m$	$\mu\epsilon\tau^{-1}\mathbf{e}_1$	$\mu\mathbf{e}_2$	$\mu\mathbf{e}_3$	$\mu\ldots$
$\mathbf{e}_{m-1}$	$\tau\mathbf{e}_{m-1}$	$\epsilon\mathbf{e}_m$	$\mu\epsilon\tau^{-1}\mathbf{e}_1$	$\mu\mathbf{e}_2$	$\mu\mathbf{e}_3$	$\mu\cdots$	$\mu\mathbf{e}_{m-2}$
$\mathbf{e}_m$	$\tau\mathbf{e}_m$	$\mu\epsilon\tau^{-1}\mathbf{e}_1$	$\mu\mathbf{e}_2$	$\mu\mathbf{e}_3$	$\mu\cdots$	$\mu\mathbf{e}_{m-2}$	$\mu\mathbf{e}_{m-1}$

mappings Ψ_1 and Ψ_2 involves BVMTs with a sufficiently large number of different structural constants as elements of the secret key.

Having performed many computations experiments, for a given value of the dimension m ($4 \leq m \leq 23$) we have obtained for Table 1 $m-3$ additional distributions of other structural constants. Besides, for other kinds of the BVMTs we have also found m different distributions of structural constants. Tables 2 and 3 show the examples of BVMTs suitable for setting secret mappings Ψ_1 and Ψ_2.

In the vector field $GF(p^5)$ (where $5|p-1$) specified by Table 2, the unit element is the vector $\left(\tau^{-1}, 0, 0, 0, 0\right)$ and the exponentiation of the vector $X = (x_1, x_2, x_3, x_4, x_5)$ to the power 2 can be implemented as computation of the values of the next four polynomials over $GF(p)$, where $Y = (y_1, y_2, y_3, y_4, y_5) = X^2$:

$$\begin{cases} y_1 = \tau x_1^2 + 2\pi x_2 x_5 + 2\pi x_3 x_4; \\ y_2 = 2\tau x_1 x_2 + 2\mu\sigma x_3 x_5 + \lambda\mu x_4^2; \\ y_3 = 2\tau x_1 x_3 + 3\epsilon\lambda x_2^2 + 2\lambda\mu x_4 x_5; \\ y_4 = 2\tau x_1 x_4 + 2\sigma\epsilon x_2 x_3 + \mu\sigma x_5^2; \\ y_5 = 2\tau x_1 x_5 + 2\epsilon\lambda x_2 x_4 + \epsilon\sigma x_3^2. \end{cases}$$

Table 2

Setting the field $GF(p^5)$ in the form of finite algebra ($\pi = \epsilon\lambda\mu\sigma\tau^{-1}$).

$\cdot$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_1$	$\tau\mathbf{e}_1$	$\tau\mathbf{e}_2$	$\tau\mathbf{e}_3$	$\tau\mathbf{e}_4$	$\tau\mathbf{e}_5$
$\mathbf{e}_2$	$\tau\mathbf{e}_2$	$\epsilon\lambda\mathbf{e}_3$	$\epsilon\sigma\mathbf{e}_4$	$\epsilon\lambda\mathbf{e}_5$	$\pi\mathbf{e}_1$
$\mathbf{e}_3$	$\tau\mathbf{e}_3$	$\epsilon\sigma\mathbf{e}_3$	$\epsilon\sigma\mathbf{e}_5$	$\pi\mathbf{e}_1$	$\lambda\sigma\mathbf{e}_2$
$\mathbf{e}_4$	$\tau\mathbf{e}_4$	$\epsilon\lambda\mathbf{e}_5$	$\pi\mathbf{e}_1$	$\lambda\mu\mathbf{e}_2$	$\lambda\mu\mathbf{e}_3$
$\mathbf{e}_5$	$\tau\mathbf{e}_5$	$\pi\mathbf{e}_1$	$\mu\sigma\mathbf{e}_2$	$\lambda\mu\mathbf{e}_3$	$\mu\sigma\mathbf{e}_4$

The cube operation $Y = X^3$ in the field $GF(p^5)$ can be implemented as calculation of the next five polynomials of the third power:

$$\begin{cases} y_1 = \tau^2 x_1^3 + 6\epsilon\lambda\mu\sigma x_1 x_2 x_5 + 6\epsilon\lambda\mu\sigma x_1 x_3 x_4 + \\ \quad + 3\epsilon^2\lambda^2\mu\sigma x_2^2 x_4 + 3\epsilon^2\lambda\mu\sigma^2 x_2 x_3^2 + 3\epsilon\lambda\mu^2\sigma^2 x_3 x_5^2 + 3\epsilon\lambda^2\mu^2\sigma x_4^2 x_5; \\ y_2 = 3\tau^2 x_1^2 x_2 + 6\mu\sigma\tau x_1 x_3 x_5 + 3\lambda\mu\tau x_1 x_4^2 + \\ \quad + 3\epsilon\lambda\mu\sigma x_2^2 x_5 + 6\epsilon\lambda\mu\sigma x_2 x_3 x_4 + \epsilon\mu\sigma^2 x_3^3 + 3\lambda\mu^2\sigma x_4 x_5^2; \\ y_3 = 3\tau^2 x_1^2 x_3 + 3\epsilon\lambda\tau x_1 x_2^2 + 6\lambda\mu\tau x_1 x_4 x_5 + \\ \quad + 6\epsilon\lambda\mu\sigma x_2 x_3 x_5 + 3\epsilon\lambda\mu\sigma x_2 x_4^2 + 3\epsilon\lambda\mu\sigma x_3^2 x_4 + \lambda\mu^2\sigma x_5^3; \\ y_4 = 3\tau^2 x_1^2 x_4 + 6\epsilon\sigma\tau x_1 x_2 x_3 + 3\mu\sigma\tau x_1 x_5^2 + \\ \quad + \epsilon^2\lambda\sigma x_2^3 + 6\epsilon\lambda\mu\sigma x_2 x_4 x_5 + 3\epsilon\mu\sigma^2 x_3^2 x_5 + 3\epsilon\lambda\mu\sigma x_3 x_4^2; \\ y_5 = 3\tau^2 x_1^2 x_5 + 6\epsilon\lambda\tau x_1 x_2 x_4 + 3\lambda\sigma\tau x_1 x_3^2 + \\ \quad + 3\epsilon^2\lambda\sigma x_2^2 x_3 + 3\epsilon\lambda\mu\sigma x_2 x_5^2 + 6\epsilon\lambda\mu\sigma x_3 x_4 x_5 + \epsilon\lambda^2\mu x_4^3. \end{cases} \tag{2}$$

Note that every polynomial in (2) contains seven terms. It is obviously that all modifications of the vector field $GF(p^5)$ specified by Table 3 are isomorphic, but each of them has a unique representation of the cube operation as a set of five polynomials. It is the latter that is required for specifying secret nonlinear mapping Ψ_1. For specifying the nonlinear mapping Ψ_2 we will use representation of the squaring operation in $GF(p^{m_2})$ (where $m_2 = n/5$ and $m_2|p-1$) as a set of quadratic polynomials over $GF(p)$. We are going to present an implementation of the MPC algorithm, in various modifications of which the input vector has different dimension values $n = 5m_2$. Therefore, the mapping Ψ_2 will be specified using the vector fields $GF(p^{m_2})$ for different values of m_2. In all such cases the vector fields $GF(p^{m_2})$ can be specified using the unified BVMT shown in Table 1 in which we suppose $m-3$ additional structural constants. Other kinds of BVMTs also can be used to specify the mapping Ψ_2 like in the case $m_2 = 7$ shown in Table 3 (where $\pi = \delta\epsilon\lambda\mu\eta\rho\tau^{-1}$) with structural constants δ, ϵ, λ, μ, η, ρ, and τ.

Table 3

Setting the field $GF(p^7)$ with using 7 structural constants.

$\cdot$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$	$\mathbf{e}_7$
$\mathbf{e}_1$	$\tau\mathbf{e}_1$	$\tau\mathbf{e}_2$	$\tau\mathbf{e}_3$	$\tau\mathbf{e}_4$	$\tau\mathbf{e}_5$	$\tau\mathbf{e}_6$	$\tau\mathbf{e}_7$
$\mathbf{e}_2$	$\tau\mathbf{e}_2$	$\epsilon\mu\rho\mathbf{e}_4$	$\epsilon\mu\rho\mathbf{e}_6$	$\mu\eta\rho\mathbf{e}_5$	$\delta\epsilon\mu\mathbf{e}_7$	$\pi\mathbf{e}_1$	$\mu\eta\rho\mathbf{e}_3$
$\mathbf{e}_3$	$\tau\mathbf{e}_3$	$\epsilon\mu\rho\mathbf{e}_6$	$\epsilon\lambda\rho\mathbf{e}_5$	$\pi\mathbf{e}_1$	$\delta\epsilon\lambda\mathbf{e}_2$	$\delta\epsilon\lambda\mathbf{e}_7$	$\epsilon\lambda\rho\mathbf{e}_4$
$\mathbf{e}_4$	$\tau\mathbf{e}_4$	$\mu\eta\rho\mathbf{e}_5$	$\pi\mathbf{e}_1$	$\delta\mu\eta\mathbf{e}_7$	$\delta\mu\eta\mathbf{e}_3$	$\delta\lambda\eta\mathbf{e}_2$	$\mu\eta\rho\mathbf{e}_6$
$\mathbf{e}_5$	$\tau\mathbf{e}_5$	$\delta\epsilon\mu\mathbf{e}_7$	$\delta\epsilon\lambda\mathbf{e}_2$	$\delta\mu\eta\mathbf{e}_3$	$\delta\epsilon\mu\mathbf{e}_6$	$\delta\epsilon\lambda\mathbf{e}_4$	$\pi\mathbf{e}_1$
$\mathbf{e}_6$	$\tau\mathbf{e}_6$	$\pi\mathbf{e}_1$	$\delta\epsilon\lambda\mathbf{e}_7$	$\delta\lambda\eta\mathbf{e}_2$	$\delta\epsilon\lambda\mathbf{e}_4$	$\delta\lambda\eta\mathbf{e}_3$	$\lambda\eta\rho\mathbf{e}_5$
$\mathbf{e}_7$	$\tau\mathbf{e}_7$	$\mu\eta\rho\mathbf{e}_3$	$\epsilon\lambda\rho\mathbf{e}_4$	$\mu\eta\rho\mathbf{e}_6$	$\pi\mathbf{e}_1$	$\lambda\eta\rho\mathbf{e}_5$	$\lambda\eta\rho\mathbf{e}_2$

In the vector field $GF(p^7)$ (where $7|p-1$) specified by Table 3, the unit element is the vector $\left(\tau^{-1}, 0, 0, 0, 0, 0, 0\right)$ and the squaring of a vector $W = (w_1, w_2, w_3, w_4, w_5, w_6, w_7)$, i.e. the operation $Z = (z_1, z_2, z_3, z_4, z_5, z_6, z_7) = W^2$, can be performed as calculation of the values of the next seven polynomials:

$$\begin{cases} z_1 = \tau w_1^2 + 2\pi\left(w_2 w_6 + w_3 w_4 + w_5 w_7\right); \\ z_2 = 2\tau w_1 w_2 + 2\delta\epsilon\lambda w_3 w_5 + 2\delta\lambda\eta w_4 w_6 + \lambda\eta\rho w_7^2; \\ z_3 = 2\tau w_1 w_3 + 2\mu\eta\rho w_2 w_7 + 2\delta\mu\eta w_4 w_5 + \delta\lambda\eta w_6^2; \\ z_4 = 2\tau w_1 w_4 + \epsilon\mu\rho w_2^2 + 2\epsilon\lambda\rho w_3 w_7 + 2\delta\epsilon\lambda w_5 w_6; \\ z_5 = 2\tau w_1 w_5 + 2\mu\eta\rho w_2 w_4 + 2\lambda\eta\rho w_6 w_7 + \epsilon\lambda\rho w_3^2; \\ z_6 = 2\tau w_1 w_6 + 2\epsilon\mu\rho w_2 w_3 + 2\mu\eta\rho w_4 w_7 + \delta\epsilon\mu w_5^2; \\ z_7 = 2\tau w_1 w_7 + 2\delta\epsilon\mu w_2 w_5 + 2\delta\epsilon\lambda w_3 w_6 + \delta\mu\eta w_4^2. \end{cases} \tag{3}$$

Note that every polynomial in (3) contains four terms. The structural constants are used as secret elements, therefore their values are generated at randon. Then a check is performed for the presence of an algebra element having order equal to $(p^m - 1)$. If such an element cannot be found, then the value of one of the structural constants (different from τ) is modified and the indicated check is repeated until the algebra element G of order $(p^m - 1)$ is found for the current combination of values of the structural constants. It is obvious that under the specified condition, the m-dimensional vector G is a generator of a cyclic group containing all nonzero elements of the algebra, i.e. the latter is the finite field $GF\left(p^m\right)$ set, for example, by Tables 2 and 3.

3 The proposed MPC algorithm

The used public key has the structure

$$Z = \mathit{\Pi}(V) = \Psi_2 \circ \mathit{\Lambda}_t \circ \Psi_1 \circ \mathit{\Lambda}_\times(V),$$

where dimensions of input (V) and output (Z) vectors are equal (we specify $n = u = 5m_2$) and linear mappings $\mathit{\Lambda}_\times$ and $\mathit{\Lambda}_t$ are such that they do not increase the number of terms in the set of polynomials specifying the nonlinear mapping representing the public key $\mathit{\Pi}$.

The mapping $\mathit{\Lambda}_\times(V)$ is specified as pairwise multiplication (in the field $GF(p)$) of the coordinates of the input vector $V = (v_1, v_2, \ldots v_n)$ and secret vector $K = (k_1, k_2, \ldots k_n)$, i. e., by the formula

$$\mathit{\Lambda}_\times(V) = X = (v_1 k_1, v_2 k_2, \ldots v_n k_n).$$

The mapping $\mathit{\Lambda}_t(Y)$ is specified as the permutation of the coodinates of the input n-dimensional vector

$$Y = (y_1, y_2, \ldots y_n) = (Y_1, Y_2, \ldots, Y_{m_2}) =$$
$$= \left(y_1^{(1)}, y_2^{(1)}, y_3^{(1)}, y_4^{(1)}, y_5^{(1)}, y_1^{(2)}, y_2^{(2)}, y_3^{(2)}, y_4^{(2)} y_5^{(2)}, \ldots, y_1^{(m_2)}, y_2^{(m_2)}, y_3^{(m_2)}, y_4^{(m_2)}, y_5^{(m_2)}\right),$$

where $Y_i = \left(y_1^{(i)}, y_2^{(i)}, y_3^{(i)}, y_4^{(i)}, y_5^{(i)}\right)$, $i = 1, 2, \ldots, m_2$, are 5-dimensional vectors. Namely, the next formulas describe the linear mapping Λ_t:

$$\begin{aligned} &\Lambda_t(Y) = W = (w_1, w_2, \ldots, w_n) = (W_1, W_2, W_3, W_4, W_5) = \\ &= \left(w_1^{(1)}, w_2^{(1)}, \ldots, w_{m_2}^{(1)}, w_1^{(2)}, w_2^{(2)}, \ldots, w_{m_2}^{(2)}, \quad \ldots \quad, w_1^{(5)}, w_2^{(5)}, \ldots, w_{m_2}^{(5)}\right); \\ &\text{where } W_j = \left(w_1^{(j)}, w_2^{(j)}, \ldots, w_{m_2}^{(j)}\right) \quad \text{for } j = 1, 2, 3, 4, 5; \\ &\text{and } w_i^{(j)} = y_j^{(i)} \quad \text{for } i = 1, 2, \ldots, m_2. \end{aligned} \tag{4}$$

The mapping $Y = \Psi_1(X)$ is performed, representing the input and output vectors $X = (X_1, X_2, \ldots, X_{m_2})$ and $Y = (Y_1, Y_2, \ldots, Y_{m_2})$ as respective ordered sets of the 5-dimensional vectors $X_i = \left(x_1^{(i)}, x_2^{(i)}, \ldots, x_5^{(i)}\right)$ and $Y_i = \left(y_1^{(i)}, y_2^{(i)}, \ldots, y_5^{(i)}\right)$, where for $i = 1, 2, \ldots, m_2$ calculating the vectors Y_i with cube operations in the $GF(p^5)$ fields (m_2 different fields $GF(p^5)$ are specified with unique secret sets of structural constants), i. e., by the formula $Y_i = X_i^3$.

The mapping $Z = \Psi_2(W)$ is performed, representing the input vectors $W = (W_1, W_2, W_3, W_4, W_5)$ and output vectors $Z = (Z_1, Z_2, Z_3, Z_4, Z_5)$ as respective ordered sets of the m_2-dimensional vectors $W_j = \left(w_1^{(j)}, w_2^{(j)}, \ldots w_{m_2}^{(j)}\right)$ and $Z_j = \left(z_1^{(j)}, z_2^{(j)}, \ldots z_{m_2}^{(j)}\right)$, where $j = 1, 2, \ldots, 5$, and calculating the vectors Z_j with squaring operations in the $GF(p^{m_2})$ fields (five different modifications of the field $GF(p^{m_2})$ are specified with unique secret sets of structural constants), i. e., by the formula $Z_j = Y_j^2$.

It can be seen from formulas (4) that every m_2-dimensional vector W_j includes exactly one coordinate of every of the input 5-dimensional vectors. Thus, every of the polynomials of Π depends on every coordinate of the input vector V, contains $\alpha = 49\,(m_2 + 1)\,/2$ terms and has power equal to six. Suppose in every of the said polynomials the terms are ordered in lexicographic order of products of six variables (this part of the terms is public), then the public key can be represented as a set of $\beta = \alpha n = 5\alpha m_2$ coefficients $c_i^{(j)} \in GF(p)$, where $j = 1, 2, \ldots, n$ and $i = 1, 2, \ldots, \alpha$, in n power polynomials.

To send a secret meaningful (i. e., information-redundant) message M, represented in the form of n-dimensional vector over $GF(p)$, via a public channel, one can encrypt M by formula $C = \Pi(M)$ and send the ciphertext C to the owner of the public key Π. The latter knows the secret trapdoor in the form of the next three inverse mappings $\Lambda_\times^{-1}$, Ψ_1^{-1}, and Ψ_2^{-1} (note that Λ_t^{-1} is not secret).

The mapping $W = \Psi_2^{-1}(Z)$ is performed, representing the input and output vectors $Z = (Z_1, \ldots, Z_5)$ and $W = (W_1, \ldots, W_5)$ as ordered sets of the m_2-dimensional vectors $W_j = \left(w_1^{(j)}, w_2^{(j)}, \ldots, w_{m_2}^{(j)}\right)$ and $Z_j = \left(z_1^{(j)}, z_2^{(j)}, \ldots, z_{m_2}^{(j)}\right)$, where $j = 1, 2, \ldots, 5$, and calculating the vectors W_j with the exponentiation operations (in $GF(p^{m_2})$) by the formula $W_j = \pm Z_j^b$, where $b = (p^{m_2} + 1)\,/4$ (the reader can easily derive this formula for the used case $p^{m_2} \equiv 3 \bmod 4$). Note that one gets two different square roots from every of the five values Z_j, therefore, the mapping $W = \Psi_2^{-1}(Z)$ produces 32 different preimages of the vector Z. Thus, when executing decryption, all of the latter are to be used to perform the following decryption steps (which include operations that give an unambiguous result), untill a meaningful message is obtained. On average, this reduces the decryption speed by ≈ 4 times.

The mapping $X = \Psi_1^{-1}(Y)$ is performed, representing the input and output vectors $Y = (Y_1, Y_2, \dots, Y_{m_2})$ and $X = (X_1, X_2, \dots, X_{m_2})$ as respective ordered sets of the 5-dimensional vectors $Y_i = \left(y_1^{(i)}, y_2^{(i)}, \dots, y_5^{(i)}\right)$ and $X_i = \left(x_1^{(i)}, x_2^{(i)}, \dots, x_5^{(i)}\right)$, where $i = 1, 2, \dots, m_2$, and calculating the vectors X_i with exponentiation operations in the respective $GF(p^5)$ fields, i. e., by the formula $X_i = \pm Y_i^d$, where $d = 3^{-1} \bmod \left(p^5 - 1\right)$. Note that the latter condition dictates the need to use the field characteristic p such that 3 does not divide the integer $p^5 - 1$.

The mapping $V = \Lambda_\times^{-1}(X)$ is implemented as pairwise multiplication of the vector X and vector $K' = \left(k_1^{-1}, k_2^{-1}, \dots, k_n^{-1}\right)$, the latter being defined by secret vector K.

Thus the owner of public key is able to restore the source message M by the next formula:

$$M = \Lambda_\times^{-1}\left(\Psi_1^{-1}\left(\Lambda_t^{-1}\left(\Psi_2^{-1}(C)\right)\right)\right).$$

In order to speed up the decryption of the ciphertext, the Ψ_2 mapping can be set using the cube operations in the field $GF(p^{m_2})$, however this leads to an increase in the size of the public key, for example, to the value of ≈60 (and ≈156) Kilobytes for $m_2 = 5$ (and $m_2 = 7$). Within the framework of the proposed approach, a higher performance of the decryption procedure with a small size of the public key can be provided by specifying mappings Ψ_1 and Ψ_2 based on cube operations performed in finite fields of characteristic two, but consideration of this issue is beyond the scope of this article.

4 Security estimation

Like in other MPC algorithm, the direct attack on the proposed algorithm is solving a system of $5m_2$ power equations in the $5m_2$ unknowns, the latter being coordinates of input vector V used as variables in the plynomials composing the public key Π. This system is given by equating the polynomial values to the corresponding coordinates of the output vector Z. The best known methods for solving such systems of arbitrary equations are based on using so called F4 and F5 algorithms [8,9] and their computational complexity exponentiationally depends on the number of equations and weakly depends on the order of the field in which the equations are given and on the value of the degree of polynomials. Table 4 [1] illustrates security level L of the MPC algorithms to direct attack in dependence on the number of equations and on the order of the field (in the case when number of equations is equal to number of unknowns).

Security level of different modifications (specified by different values m_2) of the proposed MPC algorithm to the direct attack is shown in Table 5, where the values

Table 4

The minimum number of equations in $GF(q)$ to get the required security level [1].

$L = \dots$	2^{80}	2^{100}	2^{128}	2^{192}	2^{256}
$q = 16$	30	39	51	80	110
$q = 31$	28	36	49	75	103
$q = 256$	26	33	43	68	93

of p satisfy the following conditions: i) $5|p-1$; ii) $m_2|p-1$, iii) $p^{m_2} \equiv 3 \bmod 4$, and iv) number 3 does not divide the integer $p^5 - 1$. Structural attacks proposed for the known MPC algorithms seem to be ineffective for the proposed one due to a significant difference in its structure.

As a structural attack on the proposed algorithm, one can propose the calculation of the structural constants used to set m_2 modifications of the field $GF(p^5)$ and 5 modifications of the field $GF(p^{m_2})$ and n coordinates of the secret vector from the known coefficients in the power equations describing the mapping Π. Such structural attack is connecting with solving a specific system of $\approx 25nm_2$ equations of the sixth power with $3n$ unknowns. Estimation of the security level to this structural attack and development of other kinds of structural attacks represent a topic of an independent research.

Also of interest is another topic of independent research, which is the development of the MPC algorithms with standard masking linear mappings (see formula (1)) and setting a central non-linear mapping using squaring and cube operations in finite vector fields.

Table 5

Some parameters of the developed MPC algorithm.

m_2	p	n	size of public key, Kb	size of secret key, bytes	L
5	251	25	≈ 4	75	$\approx 2^{80}$
7	71	35	≈ 7	< 110	2^{80}
11	1871	55	≈ 20	≈ 250	$>2^{128}$
13	131	65	≈ 23	≈ 200	$\approx 2^{192}$
19	191	95	≈ 47	≈ 300	2^{256}

Conclusion

For the first time the operations in finite vector fields have been proposed as basic element for development of the public-key algorithms of multivariate cryptography. For a fixed dimension m and fixed BVMT, different combinations of the values of m structural constants can be used to specify sufficiently large number of different modifications of the vector finite field $GF(p^m)$. A specific algorithm that implements this approach is proposed and an estimate of the security level of various modifications of the proposed algorithm is given.

Within the framework of the proposed approach, it seems very interesting to use vector fields $GF\left((2^z)^m\right)$ defined over binary-polynomial fields $GF\left(2^z\right)$, and this item represents a topic of future research.

References

[1] Ding J., Petzoldt A. *Current State of Multivariate Cryptography.* IEEE Security and Privacy Magazine, 2017, **15**, no. 4, pp. 28–36.

[2] 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), 2022. National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.IR.8413, (accessed January 2, 2023).

[3] *Post-Quantum Cryptography: Digital Signature Schemes.* 2022, [online], https://csrc.nist.gov/Projects/pqc-dig-sig/standardization/call-for-proposals

[4] Moldovyan N. A., Moldovyanu P. A. *Vector Form of the Finite Fields $GF(p^m)$.* Bulletin of Academy of Sciences of Moldova. Mathematics, 2009, **No. 3(61)**, 57–63.

[5] Hashimoto Y. *Recent Developments in Multivariate Public Key Cryptosystems.* In: Takagi, T., Wakayama, M., Tanaka, K., Kunihiro, N., Kimoto, K., Ikematsu, Y. (eds) International Symposium on Mathematics, Quantum Theory, and Cryptography. Mathematics for Industry. Springer, Singapore. 2021, **33**, 209–229. https://doi.org/10.1007/978-981-15-5191-8_16

[6] Shuaiting Q., Wenbao H., Yifa Li, Luyao J. *Construction of Extended Multivariate Public Key Cryptosystems.* International Journal of Network Security. 2016, **18**, 60–67.

[7] Ding J., Petzoldt A., Schmidt D.S. *Oil and Vinegar.* In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer, New York. 2020, **80**, 89-151. https://doi.org/10.1007/978-1-0716-0987-3_5

[8] Faugére J.-C. *A new efficient algorithm for computing Grőbner basis (F4).* J. Pure Appl. Algebra, 1999, **139(1-3)**, 61–88.

[9] Faugére J.-C. *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, pp. 75–83.

Nikolay A. Moldovyan
St. Petersburg Federal Research Center of the Russian
Academy of Sciences (SPC RAS), 14 Liniya V.O., 39,
St.Petersburg, 199178, Russia
E-mail: *nmold@mail.ru*

Received January 18, 2023