Vector finite fields of characteristic two as algebraic support of multivariate cryptography

Alexandr Moldovyan, Nikolay Moldovyan

Abstract

The central issue of the development of the multivariate public key algorithms is the design of reversible non-linear mappings of n-dimensional vectors over a finite field, which can be represented in a form of a set of power polynomials. For the first time, finite fields $GF\left((2^d)^m\right)$ of characteristic two, represented in the form of m-dimensional finite algebras over the fields $GF(2^d)$ are introduced for implementing the said mappings as exponentiation operation. This technique allows one to eliminate the use of masking linear mappings, usually used in the known approaches to the design of multivariate cryptography algorithms and causing the sufficiently large size of the public key. The issues of using the fields $GF\left((2^d)^m\right)$ as algebraic support of non-linear mappings are considered, including selection of appropriate values of m and d. In the proposed approach to development of the multivariate cryptography algorithms, a superposition of two non-linear mappings is used to define resultant hard-to-reverse mapping with a secret trap door. The used two non-linear mappings provide mutual masking of the corresponding reverse maps, due to which the size of the public key significantly reduces as compared with the known algorithms-analogues at a given security level.

Keywords: finite fields, finite algebras, non-linear mapping, system of power equations, post-quantum cryptography, multivariate cryptography.

MSC 2010: 68P25, 68Q12, 68R99, 94A60, 16Z05, 14G50

doi:10.56415/csjm.v32.04

1 Introduction

Multivariate public-key cryptography (MPC) is one of the attractive directions of post-quantum cryptography [1]. It exploits the computational difficulty of solving systems of many power equations with many unknowns. Quantum computers are not efficient for solving the said problem, therefore, the MPC cryptalgorithms are secure against quantum attacks [1], [2]. The MPC algorithms have sufficiently high performance and a small size of digital signature and are promising for practical applications in the coming post-quantum era [3],[4]. However, the known MPC algorithms have a significant drawback for practical application, which is the very large size of the public key.

The present paper considers a novel concept of the design of MPC algorithms, which consists in the use of two non-linear mappings specified in the form of exponentiation operations in finite fields $GF\left((2^d)^m\right)$ defined in the form of finite m-dimensional algebras [5]. The main meaning of the used vector form [5] for specifying finite fields $GF\left((2^d)^m\right)$ is that the result of exponentiation operations can be effectively obtained as a calculation of the values of m polynomials over the field $GF\left(2^d\right)$. Selecting appropriate values of d and m allows a significant reduction of the public key size at a given security level.

2 Preliminaries

In the MPC algorithms, the public key is usually specified as a hard to reverse non-linear mapping Π of an n-dimensional vectors over a finite field $\mathbb{F}_q$ into a u-dimentional vectors over $\mathbb{F}_q$ $(u \geq n)$ [1], [3], the said non-linear mapping being set in the form of a set of u power polynomials (usually of degree two) in n variables and having a secret trapdoor. Using the latter, the owner of the public key can perform decryption of ciphertexts and generate digital signatures.

The development of an MPC algorithm is connected with specifying a set of u secret power polynomials $f_j\left(x_1, x_2, \ldots, x_n\right)$ over $\mathbb{F}_q$, where $j = 1, \ldots u$, which define a reversible nonlinear mapping $\Psi : \mathbb{F}_q^n \to \mathbb{F}_q^u$. Then, using two linear maps $\Lambda_1 : \mathbb{F}_q^n \to \mathbb{F}_q^n$ and $\Lambda_2 : \mathbb{F}_q^u \to \mathbb{F}_q^u$ (for example, implemented as multiplication of the n-dimensional and u-

dimensional vectors by $n\times n$ and $u\times u$ secret matrices, correspondingly), calculate the set of u polynomials $p_j\left(x_1, x_2, \ldots, x_n\right)$ over $\mathbb{F}_q$, where $j = 1, \ldots u$, which define the mapping:

$$\Pi = \Lambda_2 \circ \Psi \circ \Lambda_1. \tag{1}$$

From a known set of polynomials Π, it is easy to find the image $Z = \Pi(X)$ of some vector X, but it is computationally difficult to calculate the vector-preimage V for a given random vector R. However, the creator (owner) of the public key Π can effectively calculate the vector V:

$$V = \Lambda_1^{-1}\left(\Psi^{-1}\left(\Lambda_2^{-1}(R)\right)\right) = \Pi^{-1}(R). \tag{2}$$

The public key represents the superposition (1) of secret mappings. However, the mapping Π is given as a set of power polynomials $p_j\left(x_1, x_2, \ldots, x_n\right)$, and the public encryption of a message M, represented in the form of n-dimensional vector, is performed as calculation of u coordinates of the u-dimensional vector $C = \Pi(M)$:

$$c_1 = p_1\left(x_1, x_2, \ldots, x_n\right); \quad c_2 = p_2\left(x_1, x_2, \ldots, x_n\right); \quad \ldots \quad .$$
$$c_u = p_u\left(x_1, x_2, \ldots, x_n\right).$$

If a ciphertext $C = (c_1, c_2, \ldots, c_u)$ is given, then a potential adversary can find the source message, solving the system of u power equations with n unknowns $x_1, x_2, \ldots, x_n$, which is defined by the latter formulas. Such attacks on the MPC algorithms are called direct. The best known direct attacks are based on using so-called algorithms F4 [6] and F5 [7].

The owner of the public key Π can decipher the ciphertext C as follows: $M = \Lambda_1^{-1} \circ \Psi^{-1} \circ \Lambda_2^{-1}(C)$.

A digital signature can be calculated in the form of n-dimensional vector S as follows:

1. Calculate the hash value from a message M to be signed and represent it in the form of u-dimensional vector H.

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

The signature verification algorithm includes the next two steps:

1. Compute the image H' of the signature S: $H' = \Pi(S)$.

2. Calculate the hash value from the message M and represent it as an u-dimensional vector H. If $H = H'$, then the signature S is genune, else the signature is false.

The role of linear mappings Λ_1 and Λ_2 is to mask a secret trapdoor that allows you to invert the mapping Π. The present paper consideres a new technique for designing the mapping Π, characterized in using two reversible nonlinear mappings Ψ_1^{-1} and Ψ_2^{-1} ensuring the rejection of the use of masking linear mappings. The said two mappings are set using exponentiation operations in the vector finite fields [5], namely, in the fields specified in the form of finite algebras over $\mathbb{F}_q$, where $q = 2^d$; $d \geq 5$.

Suppose an m-dimensional vector space is set over a finite field $GF(q)$, where q is a prime number or a power of a prime number. If a multiplication operation that is distributive at the left and at the right relatively addition operation is defined additionally, then we have m-dimensional finite algebra. We will use the following two notations of the vector A: $A = (a_1, a_2, \dots a_m) = a_1\mathbf{e}_1 + a_2\mathbf{e}_2 + \dots, a_m\mathbf{e}_m$, where $\mathbf{e}_1, \mathbf{e}_2 + \dots, \mathbf{e}_m$ are basis vectors. The multiplication of two vectors A and $B = (b_1, b_2, \dots b_m)$ is defined as follows:

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

where every product $\mathbf{e}_i\mathbf{e}_j$ is to be substituted by a one-component vector $\mu\mathbf{e}_k$ ($\mu \neq 1$ is called structural constant) indicated in the cell at the intersection of the ith row and jth column of so-called basis vector multilication table (BVMT). In [5], it had been shown, 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, where $\pi = \mu\epsilon\tau^{-1}$, presents a general form of BVMT with three different structural constants μ, ϵ, and τ, which was introduced for specifying the vector finite fields of arbitrary dimension $m \geq 2$ [5]. For a given value of m, there are various types of BVMTs by which vector fields can be specified. Every of these BVMTs can include from one to m different structural constants with their different distributions across the cells of the table. The vector fields are set by selecting suitable values of the structural constants.

Table 1. A general form of BVMT for defining the vector fields $GF(q^m)$ [5] ($m \geq 2$).

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

3 Specifying the vector finite fields $GF\left(\left(2^d\right)^m\right)$

In the introduced method for the development of the MPC algorithms, we use the vector finite fields set over the fields $GF\left(2^d\right)$, elements of which are the binary polynomials of the degree less or equal to $d-1$. The multiplication operation in $GF\left(2^d\right)$ is specified as multiplication of binary polynomials modulo a low-weight binary irreducible polynomial (in order to reduce the computational complexity of the multiplication in $GF\left(2^d\right)$). The values of d define the values of m for which the m-dimensional algebra is a vector field $GF\left(\left(2^d\right)^m\right)$, since for the latter, it is required to fulfill the condition $m|2^d-1$. Suitable values of d and m are shown in Table 2, where the cases $d = 8,\ 16,\ 24$ are of preferable interest from the practical point of view.

Consider the case of using the vector fields set over $GF\left(2^8\right)$ relating to the development of an MPC algorithm with a public key $\Pi = \Psi_2 \circ \Psi_1$ defining the mapping $\mathbb{F}_{256}^{85} \rightarrow \mathbb{F}_{256}^{85}$. The input 85-dimensional vector X is represented as concatenation of 17 vectors of dimension 5 ($j = 1, 2, \ldots, 17$):

$$X = (X_1, X_2, \ldots X_{17}), \text{ where } X_j = (x_1^{(j)}, x_2^{(j)}, \ldots x_5^{(j)}).$$

The mapping Ψ_1 is specified as exponentiation of every vector X_j to the power 257 in a unique vector field $GF\left(\left(2^8\right)^5\right)$. Since the integer 257

Table 2. Suitable values of d and m.

d	2^d-1	m	d	2^d-1	m
5	31	31	18	$3^3\cdot 7\cdot 19\cdot 73$	$7;9;19;$ $27;73$
6	$3^2\cdot 7$	$3;7;9;21$	20	$17\cdot 61681$	17
8	$3\cdot 5\cdot 17$	$3;5;15;17$	21	$7^2\cdot 127\cdot 337$	$7;49;127$
9	$7\cdot 73$	$7;73$	22	$3\cdot 23\cdot 89\cdot 683$	$3;23;89$
14	$3\cdot 43\cdot 127$	$3;43;127$	23	$47\cdot 178481$	47
15	$7\cdot 31\cdot 151$	$7;31$	24	$3^2\cdot 5\cdot 7\cdot 13\cdot$ $\cdot 17\cdot 241$	$5;7;9;$ $13;15;17$
16	$3\cdot 5\cdot 17\cdot 257$	$3;5;15;17$	...	...	...

is mutaully prime with the integer $2^{40}-1$ (order of the multiplicative group of $GF\left(\left(2^8\right)^5\right)$), the latter operation defines bijective nonlinear mapping $Y_j = \Psi_{1(j)}(X_j)$. The inverse mapping $X_j = \Psi^{-1}_{1(j)}(Y_j)$ can be performed as exponentiation to the power $b = 551894941568$, since $b \equiv 257^{-1} \bmod 2^{40}-1$.

To specify the 17 unique mappings $\Psi_{1(j)}$ ($j = 1, 2, \ldots, 17$), we define two different types of the vector fields $GF\left(\left(2^8\right)^5\right)$ using two different BVMTs with 5 structural constants ϵ, λ, μ, σ, and τ, shown in Tables 3 and 4. The values of the said constants are generated at random and independently for each of the mappings $\Psi_{1(j)}$.

The fact that a field is formed for a given set of values of structural constants is ensured by checking experimentally the existence of a field element whose order is equal to $2^{40}-1$. If there is no such element, then another set of random values of structural constants is generated and the specified check is repeated until the presence of a generator of a cyclic group of the order $2^{40}-1$ is established. The latter fact will mean the reversibility of every non-zero 5-dimensional vector, i.e., it will mean the formation of a vector field $GF\left(\left(2^8\right)^5\right)$.

For the values $j = 1, 2, 3, 5, 6, 8, 9, 10, 12, 13, 15, 16$, and 17, the mapping $\Psi_{1(j)}$ is defined as the exponentiation operation (represented in

the form of a set of polynomials over $GF(2^8)$) in the vector finite field $GF\left(\left(2^8\right)^5\right)$ set by the BVMT of the first kind represented by Table 3. For the values $j = 4, 7, 11$, and 14, the mapping $\Psi_{1(j)}$ is specified as a set of five polynomials over $GF(2^8)$, the values of which define the result of exponentiating to the degree 257 in the vector finite field $GF\left(\left(2^8\right)^5\right)$ set by the BVMT of the second kind represented by Table 4.

Table 3. The BVMT of the first kind for specifying the vector field $GF\left(\left(2^8\right)^5\right)$.

$\cdot$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_1$	$\lambda\mu\mathbf{e}_4$	$\lambda\mu\mathbf{e}_5$	$\tau\mathbf{e}_1$	$\lambda\sigma\mathbf{e}_2$	$\epsilon\lambda\mu\sigma\tau^{-1}\mathbf{e}_3$
$\mathbf{e}_2$	$\lambda\mu\mathbf{e}_5$	$\epsilon\mu\mathbf{e}_1$	$\tau\mathbf{e}_2$	$\epsilon\lambda\mu\sigma\tau^{-1}\mathbf{e}_3$	$\epsilon\mu\mathbf{e}_4$
$\mathbf{e}_3$	$\tau\mathbf{e}_1$	$\tau\mathbf{e}_2$	$\tau\mathbf{e}_3$	$\tau\mathbf{e}_4$	$\tau\mathbf{e}_5$
$\mathbf{e}_4$	$\lambda\sigma\mathbf{e}_2$	$\epsilon\lambda\mu\sigma\tau^{-1}\mathbf{e}_3$	$\tau\mathbf{e}_4$	$\lambda\sigma\mathbf{e}_5$	$\epsilon\sigma\mathbf{e}_1$
$\mathbf{e}_5$	$\epsilon\lambda\mu\sigma\tau^{-1}\mathbf{e}_3$	$\epsilon\mu\mathbf{e}_4$	$\tau\mathbf{e}_5$	$\epsilon\sigma\mathbf{e}_1$	$\epsilon\sigma\mathbf{e}_2$

Table 4. The BVMT of the second kind for specifying the vector field $GF\left(\left(2^8\right)^5\right)$.

$\cdot$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_1$	$\tau\mathbf{e}_1$	$\tau\mathbf{e}_2$	$\tau\mathbf{e}_3$	$\tau\mathbf{e}_4$	$\tau\mathbf{e}_5$
$\mathbf{e}_2$	$\tau\mathbf{e}_2$	$\epsilon\lambda\mathbf{e}_3$	$\epsilon\sigma\mathbf{e}_4$	$\epsilon\lambda\mathbf{e}_5$	$\epsilon\lambda\mu\sigma\tau^{-1}\mathbf{e}_1$
$\mathbf{e}_3$	$\tau\mathbf{e}_3$	$\epsilon\sigma\mathbf{e}_4$	$\epsilon\sigma\mathbf{e}_5$	$\epsilon\lambda\mu\sigma\tau^{-1}\mathbf{e}_1$	$\lambda\sigma\mathbf{e}_2$
$\mathbf{e}_4$	$\tau\mathbf{e}_4$	$\epsilon\lambda\mathbf{e}_5$	$\epsilon\lambda\mu\sigma\tau^{-1}\mathbf{e}_1$	$\lambda\mu\mathbf{e}_2$	$\lambda\mu\mathbf{e}_3$
$\mathbf{e}_5$	$\tau\mathbf{e}_5$	$\epsilon\lambda\mu\sigma\tau^{-1}\mathbf{e}_1$	$\mu\sigma\mathbf{e}_2$	$\lambda\mu\mathbf{e}_3$	$\mu\sigma\mathbf{e}_4$

Selection of the power 257 for specifying the mapping $\Psi_{1(j)}$ is determined by the purpose of defining a bijective nonlinear mapping of 5-dimensional vectors as calculation of five quadratic polynomials including three terms. Indeed, from Table 1, taking into account that in $GF(2^8)$ we have $v + v = 0\ \forall v \in GF(2^8)$, the exponentiation of

the vector V in $GF\left(\left(2^8\right)^5\right)$ to the degre 2^i, where $i = 1, 2, \ldots, 8$, can be performed as calculation of monomials of the form $k_1^{(i)} v_1^{2^i}$, $k_2^{(i)} v_2^{2^i}$, $\ldots$ $k_5^{(i)} v_5^{2^i}$ (where coefficients $k^{(i)}$ represent products of some powers of structural constants):

$$
\begin{aligned}
V^2 &= (v_1, v_2, \ldots, v_5)^2 = \left(\epsilon\mu v_2^2,\ \epsilon\sigma v_5^2,\ \tau v_3^2,\ \lambda\mu v_1^2,\ \lambda\sigma v_4^2\right);\\
V^4 &= \left(V^2\right)^2 = \left(\epsilon^3\mu\sigma^2 v_5^4,\ \epsilon\lambda^2\sigma^3 v_4^4,\ \tau^3 v_3^4,\ \epsilon^2\lambda\mu^3 v_2^4,\ \lambda^3\mu^2\sigma v_1^4\right);\\
V^8 &= \left(V^4\right)^2 = \left(\epsilon^3\lambda^4\mu\sigma^6 v_4^8,\ \epsilon\lambda^6\mu^4\sigma^3 v_1^8,\ \tau^7 v_3^8,\ \epsilon^6\lambda\mu^3\sigma^4 v_5^8,\ \epsilon^4\lambda^3\mu^6\sigma v_2^8\right);\\
V^{16} &= \left(\epsilon^3\lambda^{12}\mu^9\sigma^6 v_1^{16}, \epsilon^9\lambda^6\mu^{12}\sigma^3 v_2^{16}, \tau^{15} v_3^{16}, \epsilon^6\lambda^9\mu^3\sigma^{12} v_4^{16},\right.\\
&\qquad \left.\epsilon^{12}\lambda^3\mu^6\sigma^9 v_5^{16}\right);\\
V^{32} &= \left(\epsilon^{19}\lambda^{12}\mu^{25}\sigma^6 v_2^{32}, \epsilon^{25}\lambda^6\mu^{12}\sigma^{19} v_5^{32}, \tau^{31} v_3^{32}, \epsilon^6\lambda^{25}\mu^{19}\sigma^{12} v_1^{32},\right.\\
&\qquad \left.\epsilon^{12}\lambda^{19}\mu^6\sigma^{25} v_4^{32}\right);\\
V^{64} &= \left(\epsilon^{51}\lambda^{12}\mu^{25}\sigma^{38} v_5^{64}, \epsilon^{25}\lambda^{38}\mu^{12}\sigma^{51} v_4^{64}, \tau^{63} v_3^{64}, \epsilon^{38}\lambda^{25}\mu^{51}\sigma^{12} v_2^{64},\right.\\
&\qquad \left.\epsilon^{12}\lambda^{51}\mu^{38}\sigma^{25} v_1^{64}\right);\\
V^{128} &= \left(\epsilon^{51}\lambda^{76}\mu^{25}\sigma^{102} v_4^{128}, \epsilon^{25}\lambda^{102}\mu^{76}\sigma^{51} v_1^{128}, \tau^{127} v_3^{128},\right.\\
&\qquad \left.\epsilon^{102}\lambda^{25}\mu^{51}\sigma^{76} v_5^{128}, \epsilon^{76}\lambda^{51}\mu^{102}\sigma^{25} v_2^{128}\right);\\
V^{256} &= \left(\epsilon^{51}\lambda^{204}\mu^{153}\sigma^{102} v_1, \epsilon^{153}\lambda^{102}\mu^{204}\sigma^{51} v_2, v_3, \epsilon^{102}\lambda^{153}\mu^{51}\sigma^{204} v_4,\right.\\
&\qquad \left.\epsilon^{204}\lambda^{51}\mu^{102}\sigma^{153} v_5\right).
\end{aligned}
$$

Using Table 3, calculation of the vector $U = (u_1, u_2, \ldots, u_5) = V^{257} = V^{256}V$ gives the next result:

$$
\begin{aligned}
u_1 &= \epsilon^{154}\lambda^{103}\mu^{204}\sigma^{51} v_2^2 + \left(\tau + \epsilon^{51}\lambda^{204}\mu^{153}\sigma^{102}\tau\right) v_1 v_3 +\\
&\quad + \left(\epsilon^{205}\lambda^{51}\mu^{102}\sigma^{154} + \epsilon^{103}\lambda^{153}\mu^{51}\sigma^{205}\right) v_5 v_4;\\
u_2 &= \left(\epsilon^{102}\lambda^{154}\mu^{51}\sigma^{205} + \epsilon^{51}\lambda^{205}\mu^{153}\sigma^{103}\right) v_4 v_1 +\\
&\quad + \left(\tau + \epsilon^{153}\lambda^{102}\mu^{204}\sigma^{51}\tau\right) v_3 v_2 + \epsilon^{205}\lambda^{51}\mu^{102}\sigma^{154} v_5^2;\\
u_3 &= \left(\epsilon^{205}\lambda^{52}\mu^{103}\sigma^{154}\tau^{-1} + \epsilon^{51}\lambda^{204}\mu^{153}\sigma^{102}\tau^{-1}\right) v_5 v_1 +\\
&\quad + \left(\epsilon^{103}\lambda^{154}\mu^{52}\sigma^{205}\tau^{-1} + \epsilon^{154}\lambda^{103}\mu^{205}\sigma^{52}\tau^{-1}\right) v_2 v_4 + \tau v_3^2;
\end{aligned}
$$

$$u_4 = \epsilon^{51}\lambda^{205}\mu^{154}\sigma^{102}v_1^2 + \left(\epsilon^{205}\lambda^{51}\mu^{103}\sigma^{153} + \epsilon^{154}\lambda^{102}\mu^{205}\sigma^{51}\right)v_2v_5 + \\ + \left(\epsilon^{102}\lambda^{153}\mu^{51}\sigma^{204}\tau + \tau\right)v_3v_4;$$
$$u_5 = \left(\epsilon^{153}\lambda^{103}\mu^{205}\sigma^{51} + \epsilon^{51}\lambda^{205}\mu^{154}\sigma^{102}\right)v_1v_2 + \\ + \left(\epsilon^{204}\lambda^{51}\mu^{102}\sigma^{153}\tau + \tau\right)v_3v_5 + \epsilon^{204}\lambda^{52}\mu^{102}\sigma^{154}v_4^2. \tag{3}$$

In a similar way, the exponentiating to the degree 257 in the vector finite field $GF\left(\left(2^8\right)^5\right)$ set by Table 4 can be represented as the calculation of the values of five trinomials over the field $GF\left(2^8\right)$. The proposed nonlinear mapping $\Psi_1(X)$ is specified as performing seventeen mappings $\Psi_{1(j)}$, when the vector X is represented in the form of cancatenation of the vectors $X_1, X_2, \ldots, X_{17}$:

$$\Psi_1\left(X_1, X_2, \ldots, X_{17}\right) = \left(\Psi_{1(1)}\left(X_1\right), \Psi_{1(2)}\left(X_2\right), \ldots, \Psi_{1(17)}\left(X_{17}\right)\right),$$

where every coordinate of the output 85-dimensional vector $Y = \Psi_1\left(X\right)$ is calculated as a value of some trinomial over $GF\left(2^8\right)$. The inverse mapping $X = \Psi_1^{-1}\left(Y\right)$ is performed by the formula

$$X = \left(X_1, X_2, \ldots, X_{17}\right) = \Psi_1^{-1}\left(Y_1, Y_2, \ldots, Y_{17}\right) = \\ = \left(\Psi_{1(1)}^{-1}\left(X_1\right), \Psi_{1(2)}^{-1}\left(X_2\right), \ldots, \Psi_{1(17)}^{-1}\left(X_{17}\right)\right),$$

where mappings $\Psi_{1(j)}^{-1}\left(X_j\right)$ are performed as exponentiation to the power $b = 551894941568$ in seventeen different modifications of the field $GF\left(\left(2^8\right)^5\right)$. Every of the said modifications is characterized in using a unique set of values of structural constants ϵ, λ, μ, σ, and τ.

The nonlinear mapping Ψ_2 is specified, using five unique mappings $\Psi_{2(j)}$ performed as exponentiations to the power 257 in five unique modifications of the field $GF\left(\left(2^8\right)^{17}\right)$, implementation of every of the exponentiations being performed as computation of seventeen different power polynomials (over $GF\left(2^8\right)$) every of which contains nine terms. The vector finite field $GF\left(\left(2^8\right)^{17}\right)$ is set by BVMTs with the basis vector distribution shown in Table 1 and with 17 different structural constants (for prime values of the dimension m it is sufficiently simple to find distributions of m different structural constants, for which the multiplication operation is commutative and associative).

Suppose the 85-dimensional vector $Y = (Y_1, Y_2, \dots Y_5)$ is represented as concatenation of 5 vectors $Y_i = \left(y_1^{(i)}, y_2^{(i)}, \dots y_{17}^{(i)}\right)$ of the dimension 17 ($i = 1, 2, \dots, 5$). The mapping Ψ_2 is specified as exponentiation of every vector Y_i to the power 257 in a unique vector field $GF\left(\left(2^8\right)^{17}\right)$. Since the integer 257 is mutually prime with the integer $2^{136} - 1$ (order of the multiplicative group of $GF\left(\left(2^8\right)^{17}\right)$), the latter operation defines bijective nonlinear mapping $Z_i = \Psi_{2(i)}(Y_i)$. The inverse mapping $Y_i = \Psi_{1(i)}^{-1}(Z_i)$ can be performed as exponentiation to the power

$$b' = 437256221213893845035582997502984957786 88,$$

since $b' \equiv 257^{-1} \bmod 2^{136} - 1$. To specify five unique mappings $\Psi_{2(i)}$ ($i = 1, 2, \dots, 5$), one is to set five different sets of the values of structural constants in the BVMT specifying the vector field $GF\left(\left(2^8\right)^{17}\right)$. The values of the said constants are generated at random but so that the said field is set. Thus, the mapping $Z = \Psi_2(Y)$ is described as follows:

$$Z = (Z_1, Z_2, \dots, Z_5) = \Psi_2(Y_1, Y_2, \dots, Y_5) = \\ \left(\Psi_{2(1)}(Y_1), \Psi_{2(2)}(Y_2), \dots, \Psi_{2(5)}(Y_5)\right),$$

where every coordinate of the output 85-dimensional vector $Z = \Psi_2(Y)$ is calculated as a value of some power polynomial (containing 9 terms) over $GF\left(2^8\right)$. We do not provide a set of 17 square polynomials describing the mappings $\Psi_{2(i)}$, since this would require a rather cumbersome table with 17 structural constants. This can be done similarly to the case of description of the mappings $\Psi_{1(j)}$. Note that the polynomials describing the mappings $\Psi_{2(i)}$ contain 9 terms of the second degree. (It is reasonable to leave a detailed consideration of this issue, including the generation of a BVMT for the case $m = 17$ with 17 different distributions of structural constants, for the stage of software implementation of the algorithm.)

The inverse mapping $Y = \Psi_2^{-1}(Z)$ is performed by the formula

$$Y = (Y_1, Y_2, \dots, Y_5) = \Psi_2^{-1}(Z_1, Z_2, \dots, Z_5) = \\ = \left(\Psi_{2(1)}^{-1}(Z_1), \Psi_{2(2)}^{-1}(Z_2), \dots, \Psi_{2(5)}^{-1}(Z_5)\right),$$

where mappings $Y_i = \Psi_{2(i)}^{-1}(Z_i)$, for $i = 1, 2, \ldots, 5$, are performed as exponentiation to the power b' in five different modifications of the field $GF\left(\left(2^8\right)^{17}\right)$. Every of the said modifications is characterized by using a unique set of values of 17 structural constants.

Obviously, the generated public key Π represents a set of 85 polynomials (of the 4th degree), whose variables are the coordinates of the input vector X. Every polynomial contains 81 terms, the latter being ordered in the lexicographic order of the products of the variables. Assuming the term ordering convention, each polynomial can be specified as a set of 8-bit coefficients. Therefore, the size of public key is equal to $85 \cdot 81 = 6885$ bytes ($\approx$7 kB. The 170-byte secret key represents the set of 170 structural constants used to specify 17 modifications of the field $GF\left(\left(2^8\right)^5\right)$ and 5 modificatios of the field $GF\left(\left(2^8\right)^{17}\right)$.

Each public key coefficient is the product of some set of structural constants. However, the calculation of structural constants from known coefficients is associated with the solution of a system of equations of high degree (>50; see formulas (3)), which includes 170 unknowns. The latter represents a specific structural attack against the introduced MPC algorithm, which is similar to a standard direct attack representing solving a system of 85 equations (set by the public-key polynomials) of the 4th degree with 85 unknowns. Due to the supposed computational difficulty of the said structural attack, the calculation of mappings Ψ_1 and Ψ_2 (such that $\Pi = \Psi_2 \circ \Psi_1$) by the public key seems to be a computationally infeasible task.

4 Discussion

Using the data in Table 1, by analogy with the proposed algorithm, other MPC algorithms can be developed. Besides, linear mappings (for example, permutations of the coordinates of the input vector) can be used additionally, which do not lead to an increase in the number of terms in the public key polynomials. It is also of interest to specify non-linear mappings in the form of exponentiation operations in vector fields $GF\left((p)^m\right)$ with an odd characteristic p.

In general, the proposed approach provides quite ample opportuni-

Table 5. The minimum number of equations in $GF(q)$ for the case $u = n$ [1].

$L = \ldots$	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

ties for developing algorithms with a relatively small size of the public key, when providing a given security level. When estimating the security of the MPC algorithms, two types of attacks are distinguished: i) direct attacks and ii) structural ones. An attack of the first type consists in solving a system of power equations given by the public key polynomials for some vector $Z = (z_1, z_2, \ldots, z_u)$. The solution gives preimadge $X = (x_1, x_2, \ldots, x_n)$ of the vector Z, i. e., $X = \Pi^{-1}(Z)$. The computational difficulty of the best direct attack defines the upper limit of the MPC algorithms' security. The best-known methods for solving a system of many power equations with many unknowns use the algorithms F4 [6] and F5 [7]. The computational difficulty of the complexity of those methods depends exponentially on the number of equations and weakly depends on the degree of the equations and on the order of the field in which the equations are given. Table 5 shows the minimum number of equations (for the case $n = u$) that are required to get a given security level.

In the introduced algorithm, we have $n = u = 85$ and $q = 256$, therefore, the security against direct attack can be evaluated as 2^{192}. Modifications of the MPC algorithms, Rainbow [8] (signature finalist of the NIST competition for development of the post-quantum public-key standards) and GeMSS [9] (alternative algorithm participated in the third round of the NIST competition), have the size of public key equal to ≈260 kB and ≈1300 kB for the case of the 2^{192} security level, correspondingly (≈40 and ≈190 times more than the proposed algorithm).

Thus, the proposed method represents a significant interest in developing the MPC algorithms with a practical size of the public key.

In addition, the size of the secret key (170 bytes) is also significantly smaller against Rainbow (≈600 kB) and GeMSS (≈35 kB). Obviously, the essential advantage of algorithms Rainbow and GeMSS is that the resistance to structural attacks of various modifications of the algorithms was considered within a fairly long period of time. Study of the security of the introduced algorithm against potential structural attacks is connected with the following two items:

i) due to significantly different designs, the known structural attacks are hardly applicable to the proposed algorithm;

ii) new stuructural attacks are to be considered.

A natural structural attack against the proposed algorithm is the calculation (by the known coefficients of the public key polynomials) of 170 structural constants used to define 17 modifications of the vector field $GF\left(\left(2^8\right)^5\right)$ and 5 modifications of the field $GF\left(\left(2^8\right)^{17}\right)$. This structural attack is similar to the direct attack, since it is connected with solving a system of many power equations with many unknowns, given in $GF(2^8)$. In this structural attack, we have 6885 power equations and 170 unknowns. A potential attacker may attempt to select different subsets of power equations, for which the solution has a lower computational complexity. However, taking into account the significantly larger number of unknowns (170 versus 85), we can expect that the complexity of this structural attack will be higher compared to the direct attack.

In fact, the proposed specific algorithm is an illustration of the proposed new paradigm for constructing MPC algorithms, and there are significant reserves for the development of new algorithms and their modification taking into account structural attacks that may appear in the future.

The development of new structural attacks on the algorithms developed in the framework of the proposed approach and their detailed consideration represent independent research tasks.

It is also of interest to use exponentiation operations in the vector finite fields $GF\left((2^d)^m\right)$ to specify a nonlinear mapping within the framework of the generally accepted approach to the development of the MPC algorithms [1]–[3].

5 Conclusion

For the first time the exponentiation operations in vector finite fields of characteristic two have been proposed to implement nonlinear mappings in the MPC algorithms, the public key being formed as a superposition of two different nonlinear mappings, which is given as a set of power polynomials of the fourth degree. The introduced approach seems promising for the development of practical post-quantum algorithms, including digital signature algorithms for possible submission to the NIST competition in framework of the call for additional proposals [4].

References

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

[2] Q. Shuaiting, H. Wenbao, Li Yifa, and J. Luyao, "Construction of Extended Multivariate Public Key Cryptosystems," *International Journal of Network Security*, vol. 18, no. 1, pp. 60–67, 2016.

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

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

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

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

[7] 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, pp. 75–83.

[8] Rainbow Signature. One of three NIST Post-quantum Signature Finalists, 2021. [Online]. Available: https://www.pqcrainbow.org/.

[9] GeMSS: A Great Multivariate Short Signature. [Online]. Available: https://www-polsys.lip6.fr/Links/NIST/GeMSS.html.

A. A. Moldovyan[1], N. A. Moldovyan[2]

Received February 1, 2023
Revised February 6, 2023
Accepted September 20, 2023

[1,2]St. Petersburg Federal Research Center of
the Russian Academy of Sciences (SPC RAS),
St. Petersburg Institute for Informatics and
Automation of the Russian Academy of Sciences
14 Liniya, 39, St.Petersburg, 199178
Russia

[1]Alexandr Moldovyan
ORCID: https://orcid.org/0000-0001-5480-6016
E–mail: maa1305@yandex.ru

[2]Nikolay Moldovyan
ORCID: https://orcid.org/0000-0002-4483-5048
E–mail: nmold@mail.ru