Abstract—We introduce large groups of quadratic transformations of a vector space over the finite fields defined via symbolic computations with the usage of algebraic constructions of Extremal Graph Theory. They can serve as platforms for the protocols of Noncommutative Cryptography with security based on the complexity of word decomposition problem in noncommutative polynomial transformation group. The modifications of these symbolic computations in the case of large fields of characteristic two allow us to define quadratic bijective multivariate public keys such that the inverses of public maps has a large polynomial degree. Another family of public keys is based on the complexity of word decomposition problem in the protocols of Noncommutative Cryptography with security of Extremal Graph Theory. They can serve as platforms for symbolic computations with the usage of algebraic constructions of a vector space over the finite fields defined via monographs [4], [5], [6].

We use the known family of graphs $D(n, q)$ and $A(n, q)$ of increasing girth (see [8], [9] and further references) and their analogs $D(n, K)$ and $A(n, K)$ defined over finite commutative ring $K$ with unity for the construction of our public keys. Noteworthy to mention that for each prime power $q$, $q > 2$ graphs $D(n, q)$, $n = 2, 3, \ldots$ form a family of graphs of large girth (see [8]). There is well defined projective limit of these graphs which is a $q$-regular forest. In fact if $K$ is an integral domain both families $A(n, K)$ and $D(n, K)$ are approximations of infinite dimensional algebraic forests. Cubical transformation groups $GA(n, K)$ and $GD(n, k)$ of $K_n$ (see [10], [11]), were used for the design of key exchange protocols of Noncommutative Cryptography (see [11], [12], [13]), elements of this groups were used for the creation of stream ciphers.

I. ON POST QUANTUM, MULTIVARIATE AND NONCOMMUTATIVE CRYPTOGRAPHY

Post-Quantum Cryptography (PQC) is an answer to a threat coming from a full-scale quantum computer able to execute Shor’s algorithm. With this algorithm implemented on a quantum computer, currently used public key schemes, such as RSA and elliptic curve cryptosystems, are no longer secure. PQC is subdivided into Coding based Cryptography, Multivariate Cryptography, Noncommutative Cryptography, Hash based Cryptography. Isogeny based Cryptography and Lattice based Cryptography. Each of these six areas is based on the complexity of certain NP-hard problem. Noteworthy that fundamental assumption of cryptography that there are no polynomial-time algorithms for solving any NP-hard problem remains valid. So all six directions are well justified theoretically.

The tender of US National Institute of Standardisation Technology (NIST, 2017) is dedicated to the standardisation process of possible real life Post-Quantum Public keys. Already selected in July of 2022 four core areas of Post Quantum Cryptography are developed via methods of Lattice based Cryptography. This fact motivates researchers from other four core areas of Post Quantum Cryptography to continue design of new cryptographical primitives. Noteworthy that during the NIST project an interesting results on cryptanalysis of Unbalanced Rainbow Oil and Vinegar digital signatures schemes were found (see [1], [2], [3]). This scheme is defined via quadratic multivariate public rule, which refers to MiniRank problem. Examples of previously known multivariate public quadratic polynomials reader can find in classical monographs [4], [5], [6].

Graph based multivariate public keys with bijective encryption maps generated via special walks on incidence graph of projective geometry were proposed in [7] this year. It can be count as attempt to combine methods of Coding based and Multivariate Cryptographies. Classical multivariate public rule is a transformation of $n$-dimensional vector space over finite field $F_q$ which move vector $(x_1, \ldots, x_n)$ to the tuple $(g_1(x_1, \ldots, x_n), g_2(x_1, \ldots, x_n), \ldots, g_n(x_1, \ldots, x_n))$, where polynomials $g_i$ are given in their standard forms, i.e. lists of monomial terms in the lexicographical order. The degree of this transformation is the maximal value of $\text{deg}(g_i)$. Traditionally public rule has degree 2 or 3.

We use the known family of graphs $D(n, q)$ and $A(n, q)$ of increasing girth (see [8], [9] and further references) and their analogs $D(n, K)$ and $A(n, K)$ defined over finite commutative ring $K$ with unity for the construction of our public keys. Noteworthy to mention that for each prime power $q$, $q > 2$ graphs $D(n, q)$, $n = 2, 3, \ldots$ form a family of graphs of large girth (see [8]). There is well defined projective limit of these graphs which is a $q$-regular forest. In fact if $K$ is an integral domain both families $A(n, K)$ and $D(n, K)$ are approximations of infinite dimensional algebraic forests. Cubical transformation groups $GA(n, K)$ and $GD(n, k)$ of $K_n$ (see [10], [11]), were used for the design of key exchange protocols of Noncommutative Cryptography (see [11], [12], [13]), elements of this groups were used for the creation of stream ciphers.

II. ON GRAPHS, GROUPS AND QUADRATIC MAPS WITH THE INVERSES OF HIGH DEGREE

Let $K$ be a commutative ring. We define $A(n, K)$ as bipartite graph with the point set $P = K_n$ and line set $L = K_n$ (two copies of a Cartesian power of $K$ are used). We will use brackets and parenthesis to distinguish tuples from $P$ and $L$. So $(p) = (p_1, p_2, \ldots, p_n) \in P_n$ and $[l] = [l_1, l_2, \ldots, l_n] \in L_n$.

The incidence relation $I = A(n, K)$ (or corresponding bipartite graph $I$) is given by condition $pIl$ if and only if the equations of the following kind hold:
We can consider an infinite bipartite graph $A(K)$ with points $(p_1, p_2, \ldots, p_n, \ldots)$ and lines $[l_1, l_2, \ldots, l_n, \ldots]$. We proved that for each odd $n$ the indicator of $A(n, K)$ is at least $2n + 2$.

Another incidence relation $I = D(n, K)$ is defined below. The following interpretation of a family of graphs $D(n, K)$ in case of general commutative ring $K$ is convenient for the computations. Let us use the same notations for points and lines as in previous cases of graphs $A(n, K)$. Points and lines are elements of two copies of the affine space over $K$. Point $(p_1, p_2, \ldots, p_n)$ is incident with the line $[l_1, l_2, \ldots, l_n]$ if the following relations between their coordinates hold:

\begin{equation}
\begin{aligned}
p_2 - l_2 &= l_1 p_1, \\
p_3 - l_3 &= p_1 l_2, \\
p_4 - l_4 &= l_1 p_3, \\
\vdots \\
p_n - l_n &= p_{n-1} l_1 	ext{ for odd } n, \\
or \quad p_n - l_n &= l_{n-1} p_1 	ext{ for even } n.
\end{aligned}
\end{equation}

Let $\Gamma(n, K)$ be one of graphs $D(n, K)$ or $A(n, K)$. The graph $\Gamma(n, K)$ has so called linguistic colouring $\rho$ of the set of vertices. We assume that $\rho(x_1, x_2, \ldots, x_n) = x_1$ for the vertex $x$ (point or line) given by the tuple with coordinates $x_1, x_2, \ldots, x_n$. We refer to $x_1$ from $K$ as the colour of vertex $x$. It is easy to see that each vertex has a unique neighbour of the chosen colour. It means that the path in this graph is uniquely determined by initial vertex and the sequence of colours of the vertexes. Let $N_a$ and $J_a$ be operators of taking the neighbour with colour $a$ and jump operator changing the original colour of point or line for new colour $a$ from $K$.

Let $[y_1, y_2, \ldots, y_n]$ be the line $y$ of $\Gamma(n, K)$ with $\alpha(1), \alpha(2), \ldots, \alpha(t)$ and $\beta(1), \beta(2), \ldots, \beta(t)$ are the sequences of colours from $K[y_1]$ of the length at least $2$. We consider the sequence $0_v = y_1^1 = J_{\alpha(1)}(0_v), 2_v = N_{\beta(1)}(1_v)^3, 3_v = N_{\alpha(2)}(2_v), 4_v = N_{\beta(2)}(3_v), \ldots, 2t-2_v = N_{\beta(t-1)}(2t-3_v), 2t-1_v = N_{\alpha(t)}(2t-2_v), 2t_v = J_{\beta(t)}(2t-1_v)$. Assume that $v = 2t_v = [v_1, v_2, \ldots, v_n]$ where $v_i$ are from $K[y_1, y_2, \ldots, y_n]$.

We consider polynomial transformation $g(\alpha(1), \alpha(2), \ldots, \alpha(t), \beta(1), \beta(2), \ldots, \beta(t))$ for $t \geq 2$ of affine space $K_n$ of kind $y_1 \rightarrow y_1 + \beta(1), y_2 \rightarrow y_2 + \beta(2), \ldots, y_n \rightarrow y_n + \beta(n)$. It is easy to see that:

\begin{equation}
g(\alpha(1), \alpha(2), \ldots, \alpha(t), \beta(1), \beta(2), \ldots, \beta(t)) = \\
\gamma(1)\beta(t), \gamma(2)\beta(t), \ldots, \gamma(s)\beta(t), \sigma(1)\beta(t), \sigma(2)\beta(t), \ldots, \sigma(s)\beta(t).
\end{equation}

Proposition II.1. \cite{[11]} Transformations of kind $g$ generate a semigroup $S(\Gamma(n, K))$ of transformations of $K_n$.

Lemma II.1. \cite{[11]} The degree of transformation $g$ of the II.1 is at least $\deg(\alpha(i)) + 2\deg(\alpha(1) - \alpha(2)) + \ldots + \deg(\alpha(t - 1) - \alpha(t)) + \deg(\beta(1)) + \deg(\beta(t - 1) - \beta(t)) + \deg(\beta(t) - 3) + \ldots + \deg(\beta(t - 2) - \beta(t - 1))$.

Lemma II.2. \cite{[11]} Transformation $g$ as in the II.1 is bijective if and only if $\beta(t)(x) = a$ has a unique solution for each $a$ from $K$.

Proposition II.2. \cite{[11]} Transformations of kind $g$ generate a subgroup $S^2 \Gamma(n, K)$ of transformation of maximal degree 2.

Remark II.1. The inverse element of $g$ is defined as $g(\alpha(1), \alpha(2), \ldots, \alpha(t), \beta(1), \beta(2), \ldots, \beta(t))$.

Remark II.2. In the case of two quadratic transformations of $K_n$ of “general position” their composition will have degree 4.

We associate with the sequence $\alpha(1), \alpha(2), \ldots, \alpha(t), \beta(1), \beta(2), \ldots, \beta(t)$ of II.2 another quadratic transformation $h = H(\alpha(1), \alpha(2), \ldots, \alpha(t), \beta(1), \beta(2), \ldots, \beta(t))$ constructed via the sequence of vertices $0_v, 1_v, 2_v, \ldots, 2t_v = N_{\beta(x(t-1))}(2t-3_v), 2t_v = N_\alpha(2t-2_v), 2t_v = J_{\beta(t)}(2t-1_v)$. We compute $2t_v = J_{\alpha(t)}(2t-1) = v$ where $a(t) = (y_1)^2 + \beta(t)$ and define $h$ as the quadratic map $y_1 \rightarrow v_i, i = 1, 2, \ldots, n$.

Theorem II.1. \cite{[26], [11]} Let $K$ be the finite field $F_q$, $q = 2^c$. Then transformation $h = H(\alpha(1), \alpha(2), \ldots, \alpha(t), \beta(1), \beta(2), \ldots, \beta(t))$ is a quadratic transformation of the vector space ($F_q)^n$. The polynomial degree of its inverse transformation is at least $2^c - 1$.

Let us consider the linear projection $\tau : K_n + d \rightarrow K_n$ of deleting last $d$ coordinates of the tuple.

The map $(p) \rightarrow (\tau(p)), [l] \rightarrow [\tau(l)]$ is an automorphism of the graph $\Gamma(n + d, K)$ onto $\Gamma(n, K)$. It induces the homomorphism $\theta$ of $S(\Gamma(n + d, K))$ onto $S(\Gamma(n, K))$ such that $\theta(2\Gamma(n + d, K)) = 2\Gamma(n, K))$.

Tame Homomorphism (TH) protocol \cite{[14]}. Alice selects ring $K$ of kind $F_q$ or $Z_q$ where $q$ is a prime power $> 2$, parameters $n$ and $d > 3$. She takes tuples of elements of $K$ of kind $\alpha(t) = (a(1), a(2), \ldots, a(t))$ and $b(t) = (b(1), b(2), \ldots, b(t))$, $i = 1, 2, \ldots, t$, $t \geq 2$ such that $a(1) \neq a(j + 1)$ and $b(j) \neq b(j + 1)$, $j = 1, 2, \ldots, t - 1$ together with affine transformation $T$ from $AGL_{n+d}(F_q)$ and $Y$ from $AGL_n(F_q)$. 
Alice computes the standard forms of elements \( a_i = T^{n+d}g^{i(\alpha(1), \alpha(2), \ldots, \alpha(t)), y_i + b(1), y_i + b(2), \ldots, y_i + b(t_i)) T^{-1} } \) and \( b_i = Y^n g^{i(\alpha(1), \alpha(2), \ldots, \alpha(t)), y_i + b(1), y_i + b(2), \ldots, y_i + b(t_i)) Y^{-1} } \). She sends pairs \((a_i, b_i)\), \(i = 1, 2, \ldots, t\) to Bob. Bob writes word \( w(z_1, z_2, \ldots, z_t) \) in formal alphabet \( z_1, z_2, \ldots, z_t \) of length at least \( t \) which uses each letter \( z_i \). He computes the specialisations \( w_A = w(a_1, a_2, \ldots, a_t) \) and \( c = w(a_1, a_2, \ldots, a_t) \) in the groups of polynomial transformations of vector spaces \( K^{n+2d} \) and \( K^n \).

Bob sends \( w_A \) to Alice and keeps \( c \) for himself. Alice computes \( T^{-1} w_A T = c \). Bob sends \( T^{-1} w_A T = c \), uses the homomorphism \( \theta \) for getting \( \theta(c) = 2c \). She computes the collision map as \( Y^2 c Y^{-1} \). Noteworthy that \( c \) is a quadratic map from the group of kind \( y_1 \to c_1(y_1, y_2, \ldots, y_n) \), \( y_2 \to c_2(y_1, y_2, \ldots, y_n) \), \( \ldots \), \( y_n \to c_n(y_1, y_2, \ldots, y_n) \).

**Remark II.3.** Adversary has to decompose the standard form \( w_A \) into the word in the alphabet of generators \( a_1, a_2, \ldots, a_t \). Solution of this task in a polynomial time even with usage of Quantum Computer is unknown. So this is NP hard problem of Postquantum Cryptography.

**Remark II.4.** The complexity is determined by the complexity of computation of composition of two polynomial maps of degree 2 written in their standard forms. It is \( O(n^3) \).

**Inverse \( TH \) protocol (see [14])**

Alice selects the same data as in presented above protocol. She computes the standard forms of elements \( a_i = T^{n+d}g^{i(\alpha(1), \alpha(2), \ldots, \alpha(t)), y_i + b(1), y_i + b(2), \ldots, y_i + b(t_i)) T^{-1} } \). Instead of \( b_i \) Alice computes their inverses \( c_i = b_i^{-1} \) and sends pairs \((a_i, c_i)\) to Bob. He selects \( j(1), j(2), \ldots, j(r) \), \( 1 \leq j(i) \leq t \) and forms \( w_A = a_{j(1)} a_{j(2)} \ldots a_{j(r)} \) for Alice. Bob keeps \( b = c_{j(r)} c_{j(r-1)} \ldots c_{j(1)} \) for himself. Alice computes \( T^{-1} w_A T = c \), uses the homomorphism \( \theta \) for getting \( \theta(c) = 2c \). She computes the element as \( a \) in \( Y^2 a Y^{-1} \). It is easy to see that \( a \) and \( b \) are mutually inverse quadratic transformations of \( K^n \).

**Remark II.5.** Correspondences can use the protocol as a cryptosystem working with plaintexts from \( K^n \). Alice can convert her message text \( x \) to ciphertext \( a(x) = y \). Bob decrypts \( y \) via the usage of his quadratic map \( b \). After the usage of up to \( n^2/2 \) sessions they renovate their encryption/decryption tools via the next session of the inverse \( TH \) protocol.

### III. CRYPTO SYSTEMS WITH QUADRATIC MULTIVARIATE RULES

#### A. On the public key over \( F_q \) and its temporal form

Alice selects finite field \( F_q \), \( q = 2^r \), dimension \( n \) of the vector space over \( F_q \), \( 1T \) and \( 2T \) from \( AGL_n(F_q) \) defined by matrices with most entries distinct from zero.

She chooses parameter \( t = O(n) \), elements \( \alpha(1), \alpha(2), \ldots, \alpha(t), \beta(1), \beta(2), \ldots, \beta(t) \) for which \( \alpha(i) \neq \alpha(i), \beta(i) \neq \beta(i + 1), i = 1, 2, \ldots, n \) and compute the standard form of \( F = 1Th(\alpha(1), \alpha(2), \ldots, \alpha(t), \beta(1), \beta(2), \ldots, \beta(t)) 2T \). She presents \( F \) of kind \( y_i \to f(y_1, y_2, \ldots, y_n), i = 1, 2, \ldots, n \) as public map. Public user Bob use this transformation to encrypt his plaintext \( p \) in time \( O(n^3) \). Alice knows the decomposition \( 1Th^2 T \) and sequences \( \alpha(i) \) and \( \beta(i) \), \( i = 1, 2, \ldots, t \). It allows her to decrypt in time \( O(n^2) \).

**Remark III.1.** II.1 insures that multivariate map \( 1Th^2 T \) has inverse of polynomial degree at least \( 2t^{-1} \). So if \( r \geq 16 \) then the cryptosystem is resistant to a differential linearisation attacks. We implement the case with \( r = 32 \). We suggest this classical type multivariate public key as the object for standardisation studies.

**Remark III.2. Temporal \( TH \) public rule.** Alice creates bijective \( F \) according presented above method. Together with Bob she executes \( TH \) protocol to elaborate the collision map and sends \( C + F \) to his partner. So correspondents can use "public key rule" \( F \) in a private mode. The usage of \( F \) just \( t(n) = \lceil n^2/2 \rceil \) times for the message encryption or electronic signatures times does not allow adversary to make the restoration of \( F \). After the exchange of \( t(n) \) vectors correspondents can start the new session.

#### B. On temporal multivariate public rules

Correspondences can execute the inverse \( TH \) protocol and get mutually inverse outputs \( a \) and \( b \) acting on the vector space. Alice generates the quadratic map \( F \) as it described in unit 3.1 with \( 1T = Y \). She sends the composition \( Y \) of a and \( H \) to Bob. He restores \( F \) as \( bY \). They can make \( O(1) \) sessions of the inverse protocol and get several outputs \( 1a, 2a, \ldots, s a \) and \( 1b, 2b, \ldots, sb \). After that Alice or Bob can renovate their initial public key \( F \) via the following procedure. One of correspondents sends the word \( (i(1), i(2), \ldots, i(t)) \), \( 1 \leq i(k) \leq s \) to his/her partner. Bob uses \( c^{i(1)} b^{i(t-1)} \ldots b^{i(1)} \) for the encryption. Alice gets \( b^{i(t)} b^{i(t-1)} \ldots b^{i(1)} F(p) = c \) from Bob. She computes \( a^{i(1)} a^{i(2)} \ldots a^{i(t)} (c) = d \) and solves the equation \( F(x) = d \) with the usage of her knowledge on \( \alpha(1), \alpha(2), \ldots, \alpha(t), \beta(1), \beta(2), \ldots, \beta(t) \) and affine transformations \( 1T \) and \( 2T \) of degree 1. Noteworthy that correspondents do not need to compute compositions of generators \( 1a \) or \( 1b \), they will apply them consecutively.

#### C. Modification with direct \( TH \) protocol

Correspondents can use \( s \)-times direct \( TH \) protocol with outputs \( 1c, 2c, \ldots, sc \). Alice computes the standard form of kind \( g = Y g^{(\alpha(1), \alpha(2), \ldots, \alpha(t), \beta(1), \beta(2), \ldots, \beta(t)) Y^{-1} } \). \( i = 1, 2, \ldots, s \) from \( Y^2 G(T(n), k) Y^{-1} \) and sends \( c^t + gI \) to Bob. Bob restores \( g \) in their standard forms. After the agreement on the word \( (i(1), i(2), \ldots, i(t)) \), \( 1 \leq i(k) \leq s \) via open channel they encrypt with the consecutive usage of \( g(i_1), g(i_2), \ldots, g(i_s) \) and \( F \). Recommended period of usage of words is \( \lceil n^2/2 \rceil \). It does not allow adversary to approximate the quadratic encryption transformation.

**D. Remark on the implementation**

We use computer simulation to generate maps of kind \( y = \tau_1 h = h(\alpha(1), \alpha(2), \ldots, \alpha(t), \beta(1), \beta(2), \ldots, \beta(t)) r_2(x) \)
related to graphs $A(n,K)$ and $D(n,K)$. $K$ is one of the commutative rings: Boolean ring $B(32)$, modular ring $Z_{32}^2$ and finite affine field $F_{32}^2$. We have implemented three cases of invertible affine transformations:

1) $\tau_1$ and $\tau_2$ are identities, its just evaluation of time
2) $\tau_1$ and $\tau_2$ are of kind $x_1 \to x_1 + a_2 x_2 + a_3 x_3 + \ldots + a_n x_n$ (linear time of computing execution of $\tau_1$ and $\tau_2$),
3) $\tau_1 = A_1 x_1 + b_1$ and $\tau_2 = A_2 x_1 + b_2$, nonsingular matrices $A_1, A_2$ have nonzero entries and vectors $b_1, b_2$ with mostly all coordinates differ from zero standard forms of the maps in the cases 2 and 3.

The program is written in C++ and compiled with the gcc compiler. We used an average PC with processor Pentium 3.00 GHz, 2GB memory RAM and system Windows 7. Tables from I to VI presents the time of encryption with symmetric algorithm and three different commutative ring.

IV. TREES OF INFINITE FOREST $D(F_0)$ AND OBFUSCATIONS OF QUADRATIC MULTIVARIATE RULES

We suggest modification quadratic $D(n,K)$ transformations presented before which is based on the descriptions of the connected components of these graphs. The description uses the following alternative definition of them.

The family of graphs $D(n,K)$, $n = 2, 3, \ldots$ where $K$ is arbitrary commutative ring defines the projective limit $D(K)$ with points

$$ (p) = (p_{10}, p_{11}, p_{12}, p_{21}, p_{22}, p_{22}'; \ldots), $$

(3)

and lines

$$ [l] = [l_{01}, l_{11}, l_{12}, l_{21}, l_{22}, l_{22}'; \ldots], $$

(4)

which can be thought as infinite sequences of elements in $K$ such that only finitely many components are nonzero.

A point $(p)$ of this incidence structure $I$ is incident with a line $[l]$, i.e. $(p)I[l]$, if their coordinates obey the following relations:

$$ p_{i,i} - l_{i,i} = p_{1,0} l_{i-1,i,i}, $$

$$ l_{i,i}' - l_{i,i}' = p_{i,i-1} l_{0,i}, $$

$$ p_{i,i} + 1 - l_{i,i+1} = p_{i,i} l_{0,i}, $$

$$ l_{i,i+1} - l_{i,i+1} = p_{i,i} l_{0,i}', $$

(5)

These four relations are well defined for $i > 1$, $p_{1,1} = p_{1,1}'$, $l_{1,1} = l_{1,1}'$.

Let $D$ be the list of indexes of the point of the graph $D(K)$ written in their natural order, i.e. sequence $(1,0), (1,1), (1,2), (2,1), (2,2), (2,2)' \ldots$ Let $kD$ be the list of $k$ first elements of $D$. The procedure of deleting coordinates of points and lines of $D(k,K)$ indexed by elements of $D - kD$ defines the homomorphism of $D(K)$ onto graph $D(k,K)$ with the partition sets isomorphic to the variety $K^n$ and defined by the first $k-1$ equations from the list (5).

Let $k \geq 6$, $t = [(k + 2)/4]$, and let $u = (u_1, u_{11}, \ldots, u_{tt}, u_{tt}, u_{tt+1,1}, u_{tt+1,1}, \ldots)$ be a vertex of $D(k,K)$. We assume that $u_1 = u_{1,0} (u_{0,1})$ if $u$ be a point (a line, respectively). It does not matter whether $u$ is a point or a line. For every $r$, $2 \leq r \leq t$, let $a_r = a_r(u) = \sum_{i=0}^{r} u_{i} u_{i}' u_{r-i, r-i} - u_{i+1,i} u_{r-i, r-i-1}$ and $a = a(u) = (a_2, a_3, \ldots, a_4)$.

The following statement was proved in [17] for the case $F = K_2$. Its generalization on arbitrary commutative rings is straightforward, see [18].

**Proposition IV.1.** Let $K$ be a commutative ring with unity and $u$ and $v$ be vertices from the same connected component of $D(k,K)$. Then $a(u) = a(v)$. Moreover, for any $t - 1$ ring elements $x_i \in K$, $2 \leq i \leq [(k + 2)/4] - t$, there exists a vertex $v$ of $D(k,K)$ for which $a(v) = (x_2, x_3, \ldots, x_t) = (x)$.

So the classes of equivalence for the relation $\tau = \{ (u,v) | a(u) = a(v) \}$ on the vertexes of the graph $D(n,K)$ are unions of connected components.

**Theorem IV.1.** [18] For each commutative ring with unity, the graph $D(k,K)$ is edge transitive.

Equivalences classes of $\tau$ form an imprimitivity systems of automorphism group of $D(k,K)$. Graph $C(n,K)$ was introduced in [9] as the restriction of incidence relation of $D(k,K)$ on a solution set of system of homogeneous equations $a_2(x) = 0$, $a_3(x) = 0$, $a_t(x) = 0$. The dimension of this algebraic variety is $n - t = d$. Thus $d = [4/3n]+1$ for $n = 0, 2, 3 \mod 4$, $d = [4/3n]+2$ for $n = 1 \mod 4$. For convenience we assume that $C(n,K) = C_d(K)$ symbol $CD(k,K)$ stands for the connected component of graph $D(k,K)$. The following statement holds.

**Theorem IV.2.** (see [11] and further references).

The diameter of the graph $C_m(K)$, $m \geq 2$, $K$ is a commutative ring with unity of odd characteristic, is bounded by parameter $f(m)$ which does not depend on $K$.

**Corollary IV.1.** If $K$ is a commutative ring with unity of odd characteristics then $CD(n,K) = C(n,K)$.

Let us rename coordinates $y_{1,0}, y_{1,1}, y_{1,2}, y_{2,1}, \ldots$ of symbolic line $y$ of $D(n,K)$ accordingly to the natural order on them as $y_1, y_2, \ldots, y_n$ and write equations of the graph in the form 5. It allows as to write connectivity invariants of the line $y = [y_1, y_2, \ldots, y_n]$ as $a_i([y]) = a_i(y_1, y_2, \ldots, y_n)$ where $i = 2, 3, \ldots, t$. Similar notations we will use in the case of points. For the nonlinear map $F$ of $K^n$ with bounded degree given in its standard form we define trapdoor accelerator $F = 1TG_A^2T$ as the triple $1T, 2T, G_A$ of transformations of $K^n$, where $1T$, $i = 1, 2$ are elements of $AG_{\infty}(K)$, $G = G_A$ is nonlinear map on $K^n$ depending on the piece of information $A$ which allows to compute the reimage for nonlinear $G$ in time $O(n^2)$. (see [20]). In this paper we assume that $A$ is given
### TABLE I
**Generation time for the map (MS) $D(n, F_{2^3}) \cdot \text{length of the path } (2^t - 2)$, Case I**

<table>
<thead>
<tr>
<th>n</th>
<th>16</th>
<th>32</th>
<th>64</th>
<th>128</th>
<th>256</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>10</td>
<td>22</td>
<td>30</td>
<td>50</td>
<td>98</td>
</tr>
<tr>
<td>32</td>
<td>60</td>
<td>138</td>
<td>289</td>
<td>590</td>
<td>1189</td>
</tr>
<tr>
<td>64</td>
<td>1042</td>
<td>2259</td>
<td>4831</td>
<td>9983</td>
<td>20267</td>
</tr>
<tr>
<td>128</td>
<td>15819</td>
<td>33844</td>
<td>74338</td>
<td>160211</td>
<td>331893</td>
</tr>
</tbody>
</table>

### TABLE II
**Generation time for the map (MS) $D(n, F_{2^3}) \cdot \text{length of the path } (2^t - 2)$, Case II**

<table>
<thead>
<tr>
<th>n</th>
<th>16</th>
<th>32</th>
<th>64</th>
<th>128</th>
<th>256</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>25</td>
<td>45</td>
<td>97</td>
<td>209</td>
<td>417</td>
</tr>
<tr>
<td>32</td>
<td>281</td>
<td>645</td>
<td>1369</td>
<td>2813</td>
<td>5709</td>
</tr>
<tr>
<td>64</td>
<td>3226</td>
<td>8394</td>
<td>19451</td>
<td>41565</td>
<td>85780</td>
</tr>
<tr>
<td>128</td>
<td>55072</td>
<td>139364</td>
<td>357359</td>
<td>824163</td>
<td>1758056</td>
</tr>
</tbody>
</table>

### TABLE III
**Generation time for the map (MS) $D(n, F_{2^3}) \cdot \text{length of the word}$, Case III**

<table>
<thead>
<tr>
<th>n</th>
<th>16</th>
<th>32</th>
<th>64</th>
<th>128</th>
<th>256</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>71</td>
<td>136</td>
<td>263</td>
<td>518</td>
<td>1030</td>
</tr>
<tr>
<td>32</td>
<td>1220</td>
<td>2324</td>
<td>4535</td>
<td>8962</td>
<td>17824</td>
</tr>
<tr>
<td>64</td>
<td>21884</td>
<td>40412</td>
<td>77476</td>
<td>151587</td>
<td>299839</td>
</tr>
<tr>
<td>128</td>
<td>453793</td>
<td>812136</td>
<td>152678</td>
<td>2946017</td>
<td>5792884</td>
</tr>
</tbody>
</table>

### TABLE IV
**Generation time for the map (MS) $A(n, F_{2^3}) \cdot \text{length of the word}$, Case I**

<table>
<thead>
<tr>
<th>n</th>
<th>16</th>
<th>32</th>
<th>64</th>
<th>128</th>
<th>256</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>4</td>
<td>11</td>
<td>22</td>
<td>46</td>
<td>93</td>
</tr>
<tr>
<td>32</td>
<td>53</td>
<td>130</td>
<td>286</td>
<td>597</td>
<td>1230</td>
</tr>
<tr>
<td>64</td>
<td>992</td>
<td>298</td>
<td>4642</td>
<td>10065</td>
<td>20931</td>
</tr>
<tr>
<td>128</td>
<td>15642</td>
<td>33487</td>
<td>74242</td>
<td>167452</td>
<td>364704</td>
</tr>
</tbody>
</table>

### TABLE V
**Generation time for the map (MS) $A(n, F_{2^3}) \cdot \text{length of the word}$, Case II**

<table>
<thead>
<tr>
<th>n</th>
<th>16</th>
<th>32</th>
<th>64</th>
<th>128</th>
<th>256</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>18</td>
<td>57</td>
<td>125</td>
<td>257</td>
<td>538</td>
</tr>
<tr>
<td>32</td>
<td>306</td>
<td>786</td>
<td>1773</td>
<td>3758</td>
<td>7713</td>
</tr>
<tr>
<td>64</td>
<td>3190</td>
<td>8856</td>
<td>23228</td>
<td>53193</td>
<td>113146</td>
</tr>
<tr>
<td>128</td>
<td>54029</td>
<td>137191</td>
<td>368458</td>
<td>950847</td>
<td>2164035</td>
</tr>
</tbody>
</table>

### TABLE VI
**Generation time for the map (MS) $A(n, F_{2^3}) \cdot \text{length of the word}$, Case III**

<table>
<thead>
<tr>
<th>n</th>
<th>16</th>
<th>32</th>
<th>64</th>
<th>128</th>
<th>256</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>73</td>
<td>146</td>
<td>285</td>
<td>573</td>
<td>1145</td>
</tr>
<tr>
<td>32</td>
<td>1266</td>
<td>2417</td>
<td>4698</td>
<td>9265</td>
<td>18403</td>
</tr>
<tr>
<td>64</td>
<td>2214</td>
<td>40945</td>
<td>78549</td>
<td>153781</td>
<td>304237</td>
</tr>
<tr>
<td>128</td>
<td>460198</td>
<td>819495</td>
<td>1532275</td>
<td>2970741</td>
<td>5836936</td>
</tr>
</tbody>
</table>
as a tuple of characters \((d(1), d(2), \ldots, d(m))\) in the alphabet \(K\).

We use graphs \(D(n, K)\) and \(D(n, K[y_1, y_2, \ldots, y_n])\) to define family of quadratic multivariate maps \(F\) of kind \(y_1 \rightarrow f_1(y_1, y_2, \ldots, y_n), y_2 \rightarrow f_2(y_1, y_2, \ldots, y_n), \ldots, y_n \rightarrow f_n(y_1, y_2, \ldots, y_n)\) with trapdoor accelerator \(F = T_1G_AT_2, T_1, T_2 \in AGL_n(K)\).

We take the line \([y_1, y_2, \ldots, y_n]\) of the graph \(D(n, K[y_1, y_2, \ldots, y_n])\) for the colour \(\alpha_1\) from \(K\) we compute \([z] = J_{\alpha_1}([y]) = [\alpha_1 y_1, y_2, \ldots, y_n] = [z_1, z_2, \ldots, z_n]\) and compute \(a_i = \alpha_r([z]) = \alpha_r(\alpha_1 y_1, y_2, \ldots, y_n)\) for \(r = 2, 3, \ldots\)

We form the quadratic expression \(B = (y_1^2 + C(y_2, y_3, \ldots, y_n))\) with \(C(y_2, y_3, \ldots, y_n) = \lambda_2 \alpha_2 + \lambda_3 \alpha_3 + \cdots + \lambda_s \alpha_s + 1\) with nonzero \(\lambda_i\) from \(K\) and \(s = 2\) if the order of \(K^s\) is odd and \(s = 1\) in all other cases. We form the walk in the graph \(D(n, K[y_1, y_2, \ldots, y_n])\) starting from the line \([z]\) of colour \(\alpha_1\) and consecutive vertexes of colours \(y_1 + \beta_1, \alpha_2, y_1 + \beta_1, \alpha_3, \ldots, \alpha_{i-1}, y_1 + \beta_1 - 1, \alpha_i\) such that \(\alpha_i \neq \alpha_{i-1}\) for \(i = 1, 2, \ldots, l - 1\).

We form the path with the starting line \(v_1 = J_{\alpha_1}([y]), v_2 = N_{\alpha_2}(v_1), v_3 = N_{\alpha_3}(v_2), \ldots, v_{2l-1} = N_{\alpha_l}(v_{2l-2})\) and consider \(v_0 = J_B(v_{2l-1}) = u\). The vertex \(u\) allows us to define the following transformation \(G = G_A, A = (\alpha_1, \alpha_2, \ldots, \alpha_l; \beta_1, \beta_2, \ldots, \beta_{l-1}, B(y_1, y_2, \ldots, y_n))\) of \(K^n\) to itself

\[
y_1 \rightarrow (y_1)^s + C(y_1, y_2, \ldots, y_n),
\[
y_2 \rightarrow u_2(y_1, y_2),
\[
\ldots
\[
y_n \rightarrow u_2(y_1, y_2, \ldots, y_n).
\]

We identify \(A = 1^n A\) with the array \((\alpha_1, \alpha_2, \ldots, \alpha_l; \beta_1, \beta_2, \ldots, \beta_{l-1}, \lambda_1, \lambda_2, \lambda_r)\)

\[
B(y_1, y_2, \ldots, y_n)
\]

**Proposition IV.2.** Let \(T_1\) and \(T_2\) are bijective transformations from \(AGL_n(K)\) and \(K\) is arbitrary commutative ring with unity. Then the standard form of \(F = T_1G_AT_2, l = O(n)\) has a trapdoor accelerator given by coefficients of \(T_1\) and \(T_2\) together with the array \(A\) described above.

**Proof.** We have to justify that the reimage \(x \in \chi = G_A(x)\) can be computed in time \(O(n^2)\). The procedure of its computation is the following:

1. Let the value \(v\) of \(G_A\) is given. We have to compute the connectivity invariants \(a_2(u), a_3(u), \ldots, a_r(u)\) of the \(\alpha_1\) and \(\alpha_2, \alpha_3, \ldots, \alpha_r\) of the line 
2. The computation of linear combination \(b = \lambda_2 \alpha_2(u) + \lambda_3 \alpha_3(u) + \cdots + \lambda_s \alpha_s(u) + \lambda_1\)
3. The computation of the solution \(y_1 = c\) of the equation \(y_1^2 + b = c\)
4. We form the parameters \(d_1 = c + \beta_{l-1}, d_2 = c - \beta_{l-2}, d_3 = c + \beta_{l-3}, d_4 = c - \beta_{l-2}, \ldots, d_{2l-2} = c\), of “reverse path” with the starting line \([u]\).
5. Conducting recurrent computations \(N_{d_1}(u) = (u, N_{d_1}(u), N_{d_1}(u), \ldots, N_{d_1}(u))\)
6. Computing of the reimage \(J_B(2^n u)\). The complexity of the algorithm is \(O(n^2)\). So the map has a trapdoor accelerator.

The standard forms of transformations \(F = T_1G_AT_2\) can be used as a public keys. In fact this family is an obfuscation of quadratic multivariate public keys suggested in [15].

The idea of \(D(n, K)\) based encryption with the usage of connectivity invariants was suggested in [16].

The following cases are selected by us for the implementation \(K = F_q, q > 2, K = Z_m,\) where \(m\) is large composite positive integer and \(K = B(m, 2)\), i.e. Boolean ring of order \(2^m\).

**V. Conclusion**

Multivariate Cryptography in wide sense is about constructions and investigations of Public Keys in a form of nonlinear Multivariate rule defined over some finite commutative ring \(K\). These rule \(F\) has to be written as transformation \(x_i \rightarrow f_i, i = 1, 2, \ldots, n, f_i \in K[x_1, x_2, \ldots, x_n]\) over commutative ring \(K\). Bijective \(F\) can be used for the encryption of tuples (plaintexts) from the affine space \(K^n\). Multivariate rules can serve as instruments for creation of digital signatures. In the case of bijective transformation decryption process can be thought as application of inverse rule \(G\). The degree of \(G\) can be defined as maximum of degrees of polynomials \(G(x_i), i = 1, 2, \ldots, n\). For the usage of given publicly \(F\) as efficient and secure instrument its degree of has to be bounded by some constant \(c\) (traditionally \(c = 2\)) but the polynomial degree of the inverse \(G\) has to be high.

The key owner (Alice) suppose to have some additional piece \(T\) of private information about pair \((F, G)\) to decrypt ciphertext obtained from the public user (Bob). Recall that family the family \(F_n, n = 2, 3, \ldots\) has trapdoor accelerator \(nT\) if the knowledge of the piece of information \(nT\) allows to compute reimage \(x = F_n(x)\) in time \(O(n^2)\). Of course the concept of trapdoor accelerator is just instrument to search for practical trapdoor functions. As you know that the existence of theoretical trapdoor functions is just a conjecture. In fact it is closely connected to Main Conjecture of Cryptography about the fact that \(P \neq NP\). Without the knowledge of \(T\) one has to solve nonlinear system of equations which generally is \(NP\)-hard problem. Finding of the inverse \(F_n\) is an \(NP\)-hard problem if these maps are in so called "general position". In the case of specific maps additional argumentation of the complexity to find inverses \(G_n\) can be useful.

We present such heuristic arguments in the case of \(D(n, K)\) based encryption defined for arbitrary commutative ring \(K\) with unity with at least 3 elements and presented in previous section. Graphs \(D(n, K)\) have partition sets \(K^n\) (set of points and set of lines) and incidence relation between points and lines is given by system of linear equations over \(K\).

To define trapdoor accelerator for standard forms \(F_n, n = 2, 3, \ldots\) we use special walks on graphs \((D(n, K))\) and \(D(n, K[x_1, x_2, \ldots, x_n])\). The constructed map \(F_n\) acts on the selected partition set \(K^n\). In the case of trivial affine transformations \(T_1\) and \(T_2\) the relation \(F_n(x) = y\) for \(x = (x_1, x_2, \ldots, x_n)\) and \(y = (y_1, y_2, \ldots, y_n)\) vertices \(x\) and \(y\) \((f(y_1, y_2, \ldots, y_n), y_2, y_3, \ldots, y_n)\) are joint in
the graph $D(n, K)$ by the path of length $> cn$, where $c$ is a positive constant and $f \in K[y_1, y_2, \ldots, y_n]$ is known quadratic expression. Finding the path will give us the trapdoor accelerator for the computation of preimages. This can be done by Dijkstra’s algorithm of complexity $v \ln(v)$ where $v$ is the order of graphs. It could not be done in polynomial time because of $v = 2|K|^n$ and $|K| \geq 3$. Noteworthy that the usage of nontrivial $T_1$ and $T_2$ will complicate the cryptanalysis.

We presented $D(n, K)$ based platform $H(n, K)$ of quadratic transformations. So correspondents Alice and Bob can use $H(n, K)$ protocols and elaborate collision map $C, C \in H(n, K)$. So Alice can create $F_n$ and send $C + F_n$ to Bob instead of public announcement of this multivariate transformation. It gives the option to change the encryption tool periodically.

Alternatively Alice and Bob use the inverse $H(n, K)$ protocol to elaborate mutually inverse elements $H$ and $H^{-1}$ in their possessions. So Bob can change the rule $F_n$ for the quadratic $H^{-1}F_n$ via left multiplication. These actions form a basis for algorithms with temporal public rules presented in the paper.

REFERENCES


