Extremal algebraic graphs, quadratic multivariate public keys and temporal rules

Vasyl Ustymenko
0000-0002-2138-2357
Royal Holloway University of London
United Kingdom
Email: Vasyl.Ustymenko@rhul.ac.uk

Aneta Wróblewska
0000-0001-9724-4586
University of Maria Curie-Skłodowska,
Lublin, Poland
Email: aneta.wroblewska@mail.umcs.pl

***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 defined over arbitrary commutative ring with unity. We suggest the usage of constructed protocols for the private delivery of quadratic encryption maps instead of the public usage of these transformations, i.e. the idea of temporal multivariate rules with their periodical change.**

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-Qantum Public keys. Already selected in July of 2022 four cryptosystems 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 knowm multivariate quadratic public keas 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 $(x_1, \dots, x_n)$ to the tuple $(g_1(x_1, \dots, x_n), g_2(x_1, \dots, x_n), \dots, g_n(x_1, \dots, x_n))$, 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 $\deg(g_i)$. 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 $D(n, q)$, $n = 2, 3, \dots$ 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 $(p) = (p_1, p_2, \dots, p_n) \in P_n$ and $[l] = [l_1, l_2, \dots, l_n] \in L_n$. 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:

This research is partially supported by British Academy Fellowship for Researchers at Risk 2022

$$
\begin{aligned}
p_2 - l_2 &= l_1 p_1, \\
p_3 - l_3 &= p_1 l_2, \\
p_4 - l_4 &= l_1 p_3, \\
p_5 - l_5 &= p_1 l_4, \\
&\dots \\
p_n - l_n &= p_1 l_{n-1} \text{ for odd } n, \\
\text{or } p_n - l_n &= l_1 p_{n-1} \text{ for even } n.
\end{aligned} \tag{1}
$$

We can consider an infinite bipartite graph $A(K)$ with points $(p_1, p_2, \dots, p_n, \dots)$ and lines $[l_1, l_2, \dots, l_n, \dots]$. We proved that for each odd n girth 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 case of graphs $A(n, K)$. Points and lines are elements of two copies of the affine space over K. Point $(p_1, p_2, \dots, p_n)$ is incident with the line $[l_1, l_2, \dots, l_n]$ if the following relations between their coordinates hold:

$$
\begin{aligned}
p_2 - l_2 &= l_1 p_1, \\
p_3 - l_3 &= p_1 l_2, \\
p_4 - l_4 &= l_1 p_3, \\
&\dots \\
l_i - p_i &= p_1 l_{i-2} \text{ if } i \text{ congruent to 2 or 3 modulo 4}, \\
\text{or } l_i - p_i &= l_1 p_{i-2} \text{ if } i \text{ congruent to 1 or 0 modulo 4}.
\end{aligned} \tag{2}
$$

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 ρ of the set of vertices. We assume that $\rho(x_1, x_2, \dots, x_n) = x_1$ for the vertex x (point or line) given by the tuple with coordinates $x_1, x_2, \dots, x_n$. 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 $[y_1, y_2, \dots, y_n]$ be the line y of $\Gamma(n, K[y_1, y_2, \dots, y_n])$ and $(\alpha(1), \alpha(2), \dots, \alpha(t))$ and $(\beta(1), \beta(2), \dots, \beta(t))$ are the sequences of colours from $K[y_1]$ of the length at least 2. We consider the sequence ${}^0v = y, {}^1v = J_{\alpha(1)}({}^0v), {}^2v = N_{\beta(1)}({}^1v), {}^3v = N_{\alpha(2)}({}^2v), {}^4v = N_{\beta(2)}({}^3v), \dots, {}^{2t-2}v = N_{\beta(t-1)}({}^{2t-3}v), {}^{2t-1}v = N_{\alpha(t)}({}^{2t-2}v), {}^{2t}v = J_{\beta(t)}({}^{2t-1}v)$. Assume that $v = {}^{2t}v = [v_1, v_2, \dots, v_n]$ where v_i are from $K[y_1, y_2, \dots, y_n]$. We consider polynomial transformation $g(\alpha(1), \alpha(2), \dots, \alpha(t), \beta(1), \beta(2), \dots, \beta(t))$, $t \geq 2$ of affine space K_n of kind $y_1 \to y_1 + \beta(t), y_2 \to v_2(y_1, y_2), y_3 \to v_3(y_1, y_2, y_3), \dots, y_n \to v_n(y_1, y_2, \dots, y_n)$.

It is easy to see that:

$$
\begin{aligned}
&g(\alpha(1), \alpha(2), \dots, \alpha(t), \beta(1), \beta(2), \dots, \beta(t)) \cdot \\
&\cdot g(\gamma(1), \gamma(2), \dots, \gamma(s), \sigma(1), \sigma(2), \dots, \sigma(t)) = \\
&= g(\alpha(1), \alpha(2), \dots, \alpha(t), \gamma(1)(\beta(t)), \gamma(2)(\beta(t)), \dots, \\
&\gamma(s)(\beta(t)), \beta(1), \beta(2), \dots, \beta(s), \sigma(1)(\beta(t)), \\
&\sigma(2)(\beta(t)), \dots, \sigma(s)(\beta(t)).
\end{aligned}
$$

Proposition II.1. *[11] Transformations of kind* $g = g(\alpha(1), \alpha(2), \dots, \alpha(t), \beta(1), \beta(2), \dots, \beta(t))$, $t \geq 2$ *generate a semigroup* $S(\Gamma(n, K))$ *of transformations of* K_n.

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

Lemma II.2. *[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. *[11] Transformations of kind* ${}^n g = g(\alpha(1), \alpha(2), \dots, \alpha(t), \beta(1), \beta(2), \dots, \beta(t))$, $t \geq 2$ *such that* $\deg(\alpha(i)) = 0$ *and* $\beta(i) = y_1 + c(i)$, $c(i) \in K$ *generate a subgroup* ${}^2G(\Gamma(n, K))$ *of transformation of maximal degree* 2.

Remark II.1. *The inverse element of* ${}^n g = g(\alpha(1), \alpha(2), \dots, \alpha(t), \beta(1), \beta(2), \dots, \beta(t))$, $t \geq 2$ *as in the II.2 can be written as* ${}^n g(\alpha(t), \alpha(t-1), \dots, \alpha(1), \beta(t-1)(\beta(t) - 1), \beta(t-2)(\beta(t)^{-1}, \dots, \beta(1)(\beta(t)^{-1}), \beta(t)^{-1})$.

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

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

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

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

Tame Homomorphism (TH) protocol (see [14]).

Alice selects ring K of kind F_q or Z_q where q is a prime power > 2 , parameters n and d, $d > 3$. She takes tuples of elements of K of kind $a(t_i) = ({}^i\alpha(1), {}^i\alpha(2), \dots, {}^i\alpha(t_i))$ and $b(t_i) = ({}^ib(1), {}^ib(2), \dots, {}^ib(t_i))$, $i = 1, 2, \dots, t$, $t \geq 2$ such that ${}^i\alpha(j) \neq {}^i\alpha(j+1)$ and ${}^ib(j) \neq {}^ib(j+1)$, $j = 1, 2, \dots, t_{i-1}$ 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 $a_i = T^{n+d}g({}^i\alpha(1), {}^i\alpha(2), \ldots, {}^i\alpha(t_i), y_1 + {}^ib(1), y_1 + {}^ib(2), \ldots y_1 + {}^ib(t_i))T^{-1}$ and $b_i = Y^n g({}^i\alpha(1), {}^i\alpha(2), \ldots, {}^i\alpha(t_i), y_1 + {}^ib(1), y_1 + {}^ib(2), \ldots y_1 + {}^ib(t_i))Y^{-1}$. 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 $K^{n+d}$and K^n. Bob sends w_A to Alice and keeps c for himself. Alice computes $T^{-1}w_A T = {}^1c$, uses the homomorphism θ for getting $\theta({}^1c) = {}^2c$. She computes the collision map as Y^2cY^{-1}. Noteworthy that c is a quadratic map from the group of kind $y_1 \to c_1(y_1, y_2, \ldots, y_n)$, $y_2 \to c_2(y_1, y_2, \ldots, y_n)$,..., $y_n \to c_n(y_1, y_2, \ldots, y_n)$.

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 $O(n^7)$.*

Inverse TH protocol (see [14])

Alice selects the same data as in presented above protocol. She computes the standard forms of elements $a_i = T^{n+d}g({}^i\alpha(1), {}^i\alpha(2), \ldots, {}^i\alpha(t_i), y_1 + {}^ib(1), y_1 + {}^ib(2), \ldots y_1 + {}^ib(t_i))T^{-1}$. 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 $T^{-1}w_A T = {}^1c$, uses the homomorphism θ for getting $\theta({}^1c) = {}^2c$. She computes the element a as Y^2cY^{-1}. It is easy to see that a and b are mutually inverse quadratic transformations of K^n.

Remark II.5. *Correspondents can use the protocol as a cryptosystem working with plaintexts from K_n. Alice can convert her message 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 new session of the inverse TH protocol.*

III. Cryptosystems 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 ${}^1Th^2T$ 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 ${}^1Th^2T$ has inverse of polynomial degree at least 2^{r-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 $t(n) = [n^2/2]$ 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

Correspondents 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 ${}^1a, {}^2a, \ldots, {}^sa$ 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 the word $(i(1), i(2), \ldots, i(t))$, $1 \leq i(k) \leq s$ to his/her partner. Bob uses $b^{i(t)}b^{i(t-1)} \ldots b^{i(1)}F$ 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 ${}^ia$ or ${}^ib$, 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 $g_i = Yg(\alpha(1), \alpha(2), \ldots, \alpha(t), \beta(1), \beta(2), \ldots, \beta(t))Y^{-1}$, $i = 1, 2, \ldots, s$ from $Y^2G(\Gamma(n, K)Y^{-1}$ and sends $c^i + g_i$ to Bob. Bob restores g_i 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 he encrypts with the consecutive usage of $g_{i(1)}, g_{i(2)}, \ldots, g_{i(s)}$ and F. Recommended period of usage of words is $[n^2/2]$. 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 $y = \tau_1 h = h(\alpha(1), \alpha(2), \ldots, \alpha(t), \beta(1), \beta(2), \ldots, \beta(t))\tau_2(x)$

related to graphs $A(n,K)$ and $D(n,K)$. K is one of the commutative rings: Boolean ring $B(32)$, modular ring Z_2^{32} and finite field F_2^{32}. We have implemented three cases of invertible affine transformations:

1) τ_1 and τ_2 are identities, its just evaluation of time execution of core quadratic transformation,
2) τ_1 and τ_2 are of kind $x_1 \to x_1+a_2x_2+a_3x_3+\cdots+a_nx_n$ (linear time of computing execution of τ_1 and τ_2),
3) $\tau_1 = A_1x+b_1$ and $\tau_2 = A_2x+b_2$, 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 $D(F_q)$ 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

$$\begin{aligned}(p) = (&p_{10}, p_{11}, p_{12}, p_{21}, p_{22}, p'_{22}, \ldots,\\ &p'_{ii}, p_{i,i+1}, p_{i+1,i}, p_{i+1,i+1}, \ldots),\end{aligned} \tag{3}$$

and lines

$$\begin{aligned}[l] = [&l_{01}, l_{11}, l_{12}, l_{21}, l_{22}, l'_{22}, \ldots,\\ &l'_{ii}, l_{ii+1}, l_{i+1,i}, l_{i+1,i+1}, \ldots].\end{aligned} \tag{4}$$

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:

$$\begin{aligned}p_{i,i} - l_{i,i} &= p_{1,0}l_{i-1,i},\\ p'_{i,i} - l'_{i,i} &= p_{i,i-1}l_{0,1},\\ p_{i,i+1} - l_{i,i+1} &= p_{i,i}l_{0,1},\\ p_{i+1,i} - l_{i+1,i} &= p_{1,0}l'_{i,i},\end{aligned} \tag{5}$$

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 $u = (u_i, u_{11}, \ldots, u_{tt}, u'_{tt}, u_{t,t+1}, u_{t+1,t}, \ldots)$ 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 $a_r = a_r(u) = \Sigma_{i=0,r}(u_{ii}u'_{r-i,r-i} - u_{i,i+1}u_{r-i,r-i-1})$ and $a = a(u) = (a_2, a_3, \ldots, a_t)$.

The following statement was proved in [17] for the case $K = F_q$. 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 $x_i \in K$, $2 \leq i \leq \lfloor (k+2)/4 \rfloor = t$, 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 $\tau = \{(u,v) \mid a(u) = a(v)\}$ 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 τ 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 $a_2(x) = 0$, $a_3(x) = 0$, $\ldots$, $a_t(x) = 0$. 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 ${}^iT$, $i = 1,2$ are elements of $AGL_n(K)$, $G = G_A$ 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) $D(n, F_{2^{32}})$,LENGTH OF THE PATH $(2t-2)$, CASE I

n	16	32	64	128	256
16	10	22	30	50	98
32	60	138	289	590	1189
64	1042	2259	4831	9983	20267
128	15819	33844	74338	160211	331893

TABLE II

GENERATION TIME FOR THE MAP (MS) $D(n, F_{2^{32}})$,LENGTH OF THE PATH $(2t-2)$, CASE II

n	16	32	64	128	256
16	25	45	97	209	417
32	281	645	1369	2813	5709
64	3226	8394	19451	41565	85780
128	55072	139364	357359	824163	1758056

TABLE III

GENERATION TIME FOR THE MAP (MS) $D(n, F_{2^{32}})$,LENGTH OF THE WORD, CASE III

n	16	32	64	128	256
16	71	136	263	518	1030
32	1220	2324	4535	8962	17824
64	21884	40412	77476	151587	299839
128	453793	812136	152678	2946017	5792884

TABLE IV

GENERATION TIME FOR THE MAP (MS) $A(n, F_{2^{32}})$,LENGTH OF THE WORD, CASE I

n	16	32	64	128	256
16	4	11	22	46	93
32	53	130	286	597	1230
64	992	298	4642	10065	20931
128	15642	33487	74242	167452	364704

TABLE V

GENERATION TIME FOR THE MAP (MS) $A(n, F_{2^{32}})$,LENGTH OF THE WORD, CASE II

n	16	32	64	128	256
16	18	57	125	257	538
32	306	786	1773	3758	7713
64	3190	8856	23228	53193	113146
128	54029	137191	368458	950847	2164035

TABLE VI

GENERATION TIME FOR THE MAP (MS) $A(n, F_{2^{32}})$,LENGTH OF THE WORD, CASE III

n	16	32	64	128	256
16	73	146	285	573	1145
32	1266	2417	4698	9265	18403
64	2214	40945	78549	153781	304237
128	460198	819495	1532275	2970741	5836936

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 $y_1 \to f_1(y_1, y_2, \ldots, y_n)$, $y_2 \to f_2(y_1, y_2, \ldots, y_n)$, $\ldots$, $y_n \to f_n(y_1, y_2, \ldots, y_n)$ with trapdoor accelerator $F = T_1 G_A T_2$, $T_1, T_2 \in AGL_n(K)$.

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 α_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 $a_r = a_r([z]) = a_r(\alpha_1, y_2, \ldots, y_n)$, for $r = 2, 3, \ldots$. We form the quadratic expression $B = (y_1^s + C(y_2, y_3, \ldots, y_n)$ where $C(y_2, y_3, \ldots, y_n) = \lambda_2 a_2 + \lambda_3 a_3 + \cdots + \lambda_t a_t + \lambda_1$ with nonzero λ_i from K and $s = 2$ if the order of K^* 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 α_1 and consecutive vertexes of colours $y_1 + \beta_1, \alpha_2, y_1 + \beta_1, \alpha_3, \ldots, \alpha_{l-1}, y_1 + \beta l - 1, \alpha_l$ such that $\alpha_i \neq \alpha_{i+1}$, $\beta_i \neq \beta_{i+1}$ for $i = 1, 2, \ldots, l-1$.

We form the path with the starting line $v_1 = J_{\alpha_1}([y])$, $v_2 = N_{y_1+\beta_1}(v_1)$, $v_3 = N_{\alpha_2}(v_2)$, $\ldots$, $v_{2t-1} = N_{\alpha_t}(v_{2t-2}$ and consider $v_t = J_B(v_{2t-1}) = u$. 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

$y_1 \to (y_1)^s + C(y_1), y_2, \ldots, y_n),$

$y_2 \to u_2(y_1, y_2),$

$\ldots$

$y_n \to u_2(y_1, y_2, \ldots, y_n).$

We identify $A = {}^1A$ 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 $F = T_1 G_{l^A} T_2$, $l = O(n)$ 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 of $v = G_A(x)$ 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 line $u = [\alpha_l, v_2, v_3, \ldots, v_n]$.
2) The computation of linear combination $b = \lambda_2 a_2(u) + \lambda_3 a_3(u) + \cdots + \lambda_r a_r(u) + \lambda_1$.
3) The computation of the solution $y_1 = c$ of the equation ${y_1}^2 + b = v_1$.
4) We form the parameters $d_1 = c + \beta_{l-1}$, $d_2 = \alpha_{l-1}$, $d_3 = c + \beta_{l-2}$, $d_4 = \alpha_{l-2}$, $\ldots$, $d_{2l-2} = \alpha_1$, of "reverse path" with the starting line $[u]$.
5) Conducting recurrent computations $N_{d_1}(u) = {}^1u$, $N_{d_2}({}^2u)$, $\ldots$, , $N_{d_{2l-1}}({}^{2l-2}u)$.
6) Computing of the reimage $J_c({}^{2l-2}u)$. The complexity of the algorithm is $O(n^2)$. So the map has a trapdoor accelerator.

The standard forms of transformations $F = T_1 G_A T_2$ 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 $x_i \to f_i$, $i = 1, 2, \ldots, n$, $f_i \in K[x_1, x_2, \ldots, x_n]$ 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 of $y = F_n(x)$ 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_n one has to solve nonlinear system of equations which generally is NP-hard problem. Finding of the inverse for 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 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 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 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

[1] A. Canteaut and F. X. Standaert (Eds.), *40th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Eurocrypt 2021, LNCS 12696, Zagreb, Croatia, October 17–21, 2021, Proceedings, Part I, Springer, 2021, 839p, https://doi.org/10.1007/978-3-030-77886-6

[2] J. Ding, J. Deaton, , Vishakha, B.-Y. Yang, *The nested subset differential attack a practical direct attack against LUOV which forges a signature within 210 minutes*, Eurocrypt 2021, Part 1, pp. 329-347, https://doi.org/10.1007/978-3-030-77870-5_12

[3] W. Beullens, *Improved cryptanalysis of UOV and Rainbow*, Eurocrypt 2021, Part 1, pp. 348-373, https://doi.org/10.1007/978-3-030-77870-5_13

[4] L. Goubin, J. Patarin, B.-Y. Yang, *Multivariate cryptography, Encyclopedia of Cryptography and Security* (2nd Ed.) 2011, pp. 824-828, https://doi.org/10-.1007/978-1-4419-5906-5_421

[5] J. Ding, A. Petzolt and D. S. Schmidt, *Multivariate public key cryptosystems*, Springer, ADIS, vol. 80, 2020, https://doi.org/10.1007/978-1-0716-0987-3_2

[6] N. Koblitz, *Algebraic aspects of cryptography*, Springer, 1998, p. 206, https://doi.org/10.1007/978-3-662-03642-6_1

[7] V. Ustimenko, *Linear codes of Schubert type and quadratic public keys of Multivariate Cryptography*, IACR e-print archive, 2023/175, https://eprint.iacr.org/2023/175

[8] F.Lazebnik , V. Ustimenko and A.J.Woldar, *A new series of dense graphs of high girth*, Bulletin of the AMS 32 (1) (1995), pp. 73-79, https://doi.org/10.1090/s0273-0979-1995-00569-0

[9] V. Ustimenko, *On the extremal graph theory and symbolic computations*, Dopovidi National Academy of Sci, Ukraine, 2013, No. 2, pp. 42-49.

[10] V. Ustimenko, M. Klisowski, *On Noncommutative Cryptography with cubical multivariate maps of predictable density*, In "Intelligent Computing", Proceedings of the 2019 Computing Conference, Volume 2, Part of Advances in Intelligent Systems and Computing(AISC), volume 99, pp. 654-674, https://doi.org/10.1007/978-3-030-22868-2_47

[11] V. Ustimenko, *Graphs in terms of Algebraic Geometry, symbolic computations and secure communications in Post-Quantum world*, University of Maria Curie Sklodowska Editorial House, Lublin, 2022, 198 p.

[12] A. G. Myasnikov, V. Shpilrain and A. Ushakov, *Non-commutative cryptography and complexity of group-theoretic problems*, American Mathematical Society, 2011, https://doi.org/10.1090/surv/177/05

[13] B. Tsaban, *Polynomial-time solutions of computational problems in noncommutative-algebraic cryptography* , J. Cryptol. 28, No. 3 (2015), pp. 601-622, https://doi.org/10.1007/s00145-013-9170-9

[14] V. Ustimenko, *On new symbolic key exchange protocols and cryptosystems based on a hidden tame homomorphism*, Dopovidi National Academy of Sci, Ukraine, 2018, n10, pp. 26-36, https://doi.org/10.15407/dopovidi2018.10.026

[15] V. Ustimenko and A. Wroblewska, *Dynamical systems as the main instrument for the constructions of new quadratic families and their usage in cryptography*, Annales UMCS Informatica AI XII, 3 (2012) pp. 65–74, https://doi.org/10.2478/v10065-012-0030-2

[16] V. A. Ustimenko, *Graphs with special arcs and cryptography*, Acta Applicandae Mathematicae, vol. 71, N2, November 2002, pp. 117-153, https://doi.org/10.1023/a:1020686216463

[17] Lazebnik, F., Ustimenko, V.A. and A.J. Woldar, *A characterisation of the components of the graph $D(k,q)$*, Discrete Mathematics, 157 (1996), pp. 271-283, https://doi.org/10.1016/s0012-365x(96)83019-6

[18] V. Ustimenko, *Linguistic dynamical systems, graphs of large girth and cryptography*, Journal of Mathematical Sciences, Springer, vol.140, N3 (2007) pp. 461-471, https://doi.org/10.1007/s10958-007-0453-2

[19] Anshel, M. Anshel and D. Goldfeld, *An algebraic method for public-key cryptography*, Math. Res.Lett. 6(3–4), pp. 287–291 (1999), 169 https://doi.org/10.4310/mrl.1999.v6.n3.a3

[20] S.R. Blackburn and S.D. Galbraith, *Cryptanalysis of two cryptosystems based on group actions*, In: Advances in Cryptology—ASIACRYPT '99. Lecture Notes in Computer Science, vol. 1716, pp. 52–61. Springer, Berlin (1999), https://doi.org/10.1007/978-3-540-48000-6_6

[21] K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J.S. Kang and C. Park, *New public-key cryptosystem using braid groups*, In: Advances in Cryptology—CRYPTO 2000, Santa Barbara, CA. Lecture Notes in Computer Science, vol. 1880, pp. 166-183. Springer, Berlin (2000), https://doi.org/10.1007/3-540-44598-6_10

[22] G. Maze, C. Monico and J. Rosenthal, *Public key cryptography based on semigroup actions*, Adv.Math. Commun. 1(4), pp. 489–507 (2007), https://doi.org/10.3934/amc.2007.1.489

[23] P.H. Kropholler, S.J. Pride , W.A.M. Othman K.B. Wong and P.C. Wong, *Properties of certain semigroups and their potential as platforms for cryptosystems*, Semigroup Forum (2010) 81: pp. 172–186, https://doi.org/10.1007/s00233-010-9248-8

[24] J.A. Lopez Ramos, J. Rosenthal, D. Schipani and R. Schnyder, *Group key management based on semigroup actions*, Journal of Algebra and its applications, 2017, vol.16 (08):1750148, https://doi.org/10.1142/s0219498817501481

[25] G.Kumar and H. Saini, *Novel noncommutative cryptography scheme using extra special group*, Security and Communication Networks ,Volume 2017, Article ID 9036382, 21 pages, https://doi.org/10.1155/2017/9036382

[26] A. Wroblewska, *Linguistic dynamical systems based on algebraic graphs and their application in cryptography*, PhD Thesis, Institute of Fundamental Technological Research Polish Academy of Sciences, Warsaw, Poland, 2017, https://oldwww.ippt.pan.pl/_download/doktoraty/2016wroblewska_a_doktorat.pdf