Serdica J. Computing **1** (2007), 131–156

Serdica
Journal of Computing

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

ON GRAPH-BASED CRYPTOGRAPHY AND SYMBOLIC COMPUTATIONS

V. A. Ustimenko

Abstract. We have been investigating the cryptographical properties of infinite families of simple graphs of large girth with the special colouring of vertices during the last 10 years. Such families can be used for the development of cryptographical algorithms (on symmetric or public key modes) and turbocodes in error correction theory. Only few families of simple graphs of large unbounded girth and arbitrarily large degree are known.

The paper is devoted to the more general theory of directed graphs of large girth and their cryptographical applications. It contains new explicit algebraic constructions of infinite families of such graphs. We show that they can be used for the implementation of secure and very fast symmetric encryption algorithms. The symbolic computations technique allow us to create a public key mode for the encryption scheme based on algebraic graphs.

1. Introduction.

Since well known work by R. Tanner [29] families of graphs of large girth are instruments in Error Correction Theory (see [29, 13, 14] on the use of graphs of large girth for the creation of so-called turbocodes).

ACM Computing Classification System (1998): E.3.

Key words: encryption, graph based algorithms, private key, public key, stream ciphers, family of graphs of high girth, small world graphs.

The idea to use such families of simple graphs in Cryptography had been explored in [26, 27, 28, 29, 30, 31, 32, 33, 35]. The cryptoscheme for the "potentially infinite" text based on the family of graphs with special colouring of vertex set: the neighbours of each vertex are of different colours, there is a representative of each colour in the neighbourhood. It is clear that the graphs have to be regular i.e., the size of the neighbourhood does not depend on the choice of vertex.

For this purpose we identify the vertex of the graph with the plaintext, encryption procedure corresponds to the chain of adjacent vertices (walk without consecutive edges) starting from the plaintext, the information on such chain is given by the sequence of corresponding colours (the password). We assume that the end of the chain is the ciphertext. Let c_k be the cycle on k-vertices. The girth of the graph is the length of its smallest cycle.

For each $k \geq 3$ there is an infinite family of finite k-regular graphs G_i, $i = 1, 2, \ldots$ of increasing order $|V_i|$ and increasing girth g_i (see, for instance [29, 28]). In case of such a family with the colouring as above we can chose the length of the password s_i, where $c \leq s_i < g_i/2$ for some chosen j and integer constant $c < g_j/2$ and work with graphs G_i, $i \geq j$. So the potentially infinite plantspace will be V_i, $i \geq j$ and potentially infinite keyspace of the size $k^(k-1)^{s_i}$. Notice that the absence of short cycles ensure that different passwords convert chosen plaintext to different ciphertexts. The ciphertext will be always different from the plaintext. If the minimal size of connected component G_i, $i > j$ is growing with i, then the encryption scheme is not a block cipher but a stream cipher. We can consider more general encryption scheme defined by sequence of k_i-regular graphs G_i, $i = 1, \ldots$ of nondecreasing degree and increasing girth and order (see [28, 35]).

Let $e(G)$, $v = v(G)$ be the size (number of edges) and the order (number of vertices) of the graph G and $\mathrm{ex}(v, C_3, \ldots, C_{2k})$ be the maximal size of the graph of order v without cycles $C_3, \ldots, C_{2k}$. The following modification of Erdös' Even Circuit Theorem the reader can find in [6]:

$$\mathrm{ex}(v.C_3, \ldots, C_{2k}) \leq cv^{1+1/k} \tag{1}$$

where c is positive independent on v constant. This bound is known to be sharp for $k = 2, 3$ and 5.

If the size of members G_i of the family of graphs of increasing girth g_i is close to the above bound (in case of, so-called, graphs of large girth $g_i \geq C\log_{k_i}(v_i)$ then the size of plainspace and the maximal keyspace for the above encryption scheme are close to each other (see [29, 28]).

The important feature of such encryption is the resistance to attacks, when adversary intercepts the pair plaintext – ciphertext (see [29]), because the best algorithm of finding the pass between given vertices (by Dijkstra, see [9] and latest modifications) has complexity $v \ln v$ where v is the order of the graph, i.e., size of the plainspace. The situation is similar to the checking of the primality of Fermat's numbers $2^{2^m}+1$: if the input given by the string of binary digits, then the problem is polynomial, but if the input is given by just a parameter m, then the task is NP-complete.

We have an encryption scheme with the flexible length of the password (length of the chain). If graphs are connected and the length of password is not restricted, then we can convert each potentially infinite plaintext into the chosen string. In case of so-called small world graphs we can do such conversion "as fast as it is possible".

Finally, in the case of algebraic graphs in sense of N. Biggs (see [2]), when the vertex set and neighbourhoods of each vertex are algebraic varieties over the same field, there is an option to use symbolic computations in the implementation of graph based algorithm. We can create public rules symbolically and use the above algorithm as public key tool (an example of the implementation of such public key encryption is in [36]). The first infinite family of algebraic graphs of large unbounded girth and arbitrary degree had been constructed in [18] (see [19] for the description of connected components). It had been used in different software (different finite fields) packages developed via university projects at the University of South Pacific (Fiji Islands) [35, 37, 39], which serves for 11 remote island states within Pacific Ocean, Sultan Qaboos University (Oman) [38, 30], University college of Cariboo (Canada, BC), Ocanagan college, affiliated with the UBC (Canada), University of Kiev-Mohyla Academy(Ukraine), University of Maria Curie Sklodowska (Poland). The comparison of the first implementation of the algorithm (case field F_{127}) with other stream cipher private key algorithm ($RC4$) the reader can find in [12].

The graph based encryption scheme had been motivated by the idea that each computation can be thought as finite automaton. So if we ignore the initial and accepting states of finite automaton we are getting the graph with labels on edges. The classical extremal graph theory deals with simple graphs, so our first step was restricted on graphs of symmetric binary relations without loops. The next step is reflected in [43] where the analog of P. Erdös' bound has been formulated for graphs of binary relations without loops and certain commutative diagrams. The analog of girth for directed graph is so-called *girth indicator*. The size of the graph is the total number of edges. Let $E_d(v)$ be the greatest size of directed graph of order v the width girth indicator $\geq d$. The following analog of Erdös' Even Circuit Theorem has been formulated:

$$E_d(v) \leq v^{1+1/d} \tag{2}$$

This bound turns out to be sharp not only for $d = 2, 3$ and 5 but for $d = 4, 6$ as well.

The paper [43] contains definitions of graphs of large girth (graphs with girth indicator d and size which is close to the above bound), small world graphs for this class of graphs, example of directed graphs based encryption. The bound and related definition the reader can find in Section 4 below.

In current paper we will continue the theory of directed based cryptography. Instead of colouring of vertices we will consider special "rainbow-like colouring" of edges in spirit of automata theory. In terms of such colouring we define graph based private and pubic algorithms (Section 6). We show that Cayley graphs admit the appropriate colouring. It means that a well known Ramanujan graphs of high girth defined in [23, 24, 25] (further spectra and girth evaluation [22]) can be used for the development of cryptographical algorithms (Sections 5, 6). Other examples of directed graphs with rainbow-like colouring of edges are connected with generalised polygons (finite geometries of simple groups over the Dynkin diagrams A_2, B_2 and G_2) (Section 7). The known examples of generalised polygons had been used in works of R. Tanner (turbocodes in Coding Theory), cryptographical applications of incidence graphs of generalised polygons (case of simple graphs) the reader can find in [34].

The practical advantage of directed graphs based cryptography in comparison with previously used case of simple graphs is much wider option to construct explicitly algebraic graphs over arbitrarily chosen commutative ring K (Section 8). Such K-theory lead to very fast cryptoalgorithm (operation in $K = Z_{p^n}$ are much faster than in case of F_{p^n} for large n). In remarks at the end of Section 8 we compare the speed of some new algorithms with classical stream cipher $RC4$ used for the encryption of large data and discuss some specific features of new encryption schemes. They have principally deferent properties in comparison with block ciphers (DES, AES etc). The last section contains conclusions.

2. Requirements on simple graphs and explicit constructions.

The reader can find the missing graph theoretical definitions in [6, 7]. All graphs we consider are simple, i.e., undirected without loops and multiple edges. Let $V(G)$ and $E(G)$ denote the set of vertices and the set of edges of G, respectively. Then $|V(G)|$ is called the *order* of G, and $|E(G)|$ is called the *size* of G. A path in G is called *simple* if all its vertices are distinct. When it is convenient, we shall identify G with the corresponding anti-reflexive binary relation on $V(G)$, i.e., $E(G)$ is a subset of $V(G) \times V(G)$ and write vGu for the adjacent vertices u and v (or neighbours). The sequence of distinct vertices $v_0, v_1, \dots, v_t$, such that v_iGv_{i+1} for $i = 1, \dots, t-1$ is the pass in the graph. The length of a pass is the number of its edges. The distance $\mathrm{dist}(u, v)$ between two vertices is the length of the shortest pass between them. The diameter of the graph is the maximal distance between two vertices u and v of the graph. Let C_m denote the cycle of length m i.e., the sequence of distinct vertices $v_0, \dots, v_m$ such that v_iGv_{i+1}, $i = 1, \dots, m-1$ and v_mGv_1. The girth of a graph G, denoted by $g = g(G)$, is the length of the shortest cycle in G. The degree of vertex v is the number of its neighbours.

The incidence structure is the set V with partition sets P (points) and L (lines) and symmetric binary relation I such that the incidence of two elements implies that one of them is a point and another one is a line. We shall identify I with the corresponding simple graph.

Let G_i, $i = 1, 2, \dots$ be an infinite family of finite graphs of increasing order v_i, degree k_i, girth g_i and diameter d_i.

As we mentioned in the previous section the cryptographical applications require examples of regular binary relation graphs G_i, $i = 1, 2, \dots$ satisfying the following properties:

P1. Graphs of large girth, i.e., such that

$$g_i \geq \gamma \mathrm{log}_{k_i} v_i \tag{3}$$

where g_i, k_i and v_i are the girth, degree and order of the graph Γ_i, respectively, γ is the constant independent on i. So the size of such graphs is quite close to the bound (1).

P2. Small world graphs, i.e., graphs such that

$$d_i \leq \mathrm{clog}_{k_i} v_i \tag{4}$$

where d_i is the diameter of Γ_i and c is independent on i constant.

P3. Algebraic graphs defined over the finite commutative ring K.

Let us consider separately the case of family of graphs of unbounded degree (BD) and the case of unbounded degree (BD).

UD. The natural examples of algebraic graphs are so-called graphs of Lie type (see [8]), they defined via the Bruhat decomposition of finite simple graphs of Lie type. The problem is that the girth of them is bounded. The largest girth (16) corresponds to the incidence graph of generalised octagon related to ${}^2F_4(F_q)$, defined over the perfect field of characteristic 2. Most known explicit constructions of infinite families of regular small world graphs are of girth 4 (see, for instance).

In [19] the family of connected algebraic graphs $CD(n,q)$, $n \geq 2$, q is prime power ≥ 3 had been constructed. The order of q-regular bipartite graph $CD(n,q$ is $2q^n$ The girth $g(CD(n,q))$ of the graph $CD(n,q)$ had been bounded below by $4/3n$.

In [44] it was shown that if n is fixed but q is growing then graphs $CD(n,q)$ form a family of small world graphs. So we can take $q = p^n$, where p is fixed and n is growing and obtain the following statement.

Theorem 1. *For each prime number p, $p > 2$ there is a family of small world algebraic graphs over F_p with the girth $\geq d$ with the rainbow-like coloring.*

BD. Even the task of constructions of families of graphs of large girth of bounded degree is far from trivial.

The studies of infinite families of graphs of large girth in the sense of N. Biggs [2] i.e., graphs G_i of bounded degree l_i and unbounded girth g_i such that $g_i \geq \gamma \log_{l_i - 1}(v_i)$ is an important direction in the theory of simple graphs. The above definition had been motivated by applied problems in Networking (see [10, 6] and further references).

As it follows from Even Circuit Theorem by Erdös' $\gamma \leq 2$, but no family has been found for which $\gamma = 2$. Bigger γ's correspond to the larger girth. The existence of such families was proven by P. Erdös' with his well known probabilistic method (see [6] and further references).

The first explicit examples of families with large girth were given by Margulis [23, 24, 25] with for some infinite families with arbitrary large valency. The constructions were Cayley graphs $X^{p,q}$ of group $SL_2(Z_q)$ with respect to special sets of $q+1$ generators, p and q are primes congruent to 1 mod 4. Then independently Margulis and Lubotsky, Phillips, and Sarnak [22] proved that for each p the constant γ for graphs $X^{p,q}$ with fixed p is $\geq 4/3$. In [4] Biggs and Boshier showed that this γ is asymptotically 4/3.

The family of $X^{p,q}$ is not a family of algebraic graphs because the neighbourhood of each vertex is not an algebraic variety over F_q. For each p, graphs $X^{p,q}$, where q is running via appropriate primes, form a family of small world graph of unbounded diameter.

The first family of connected algebraic graphs over F_q of large girth and arbitrarily large degree had been constructed in [19]. These graphs are $CD(k,q)$ as above, where k is growing integer ≥ 2 and odd prime power q is fixed. They had been constructed as connected component of graphs $D(k,q)$ defined earlier (see [18, 20]). For each q graphs $CD(k, q)$, $k \geq 2$ form a family of large girth with $\gamma = 4/3\log_{q-1}q$ of degree q.

Some new examples of simple algebraic graphs with memory of large girth and arbitrary large degree the reader can find in [41].

Notice that graphs $X^{p,q}$ are not an algebraic graphs because the neighbourhood of a vertex is not an algebraic variety over F_q of dimension ≥ 1.

Conjecture. For each finite field F_q of odd characteristic the family $CD(n, q)$, $n = 1, 2\ldots$ is an algebraic over F_q family of small world graphs of high girth of bounded degree.

The explicit constructions of algebraic families of small world graphs with girth ≥ 8 of bounded (or unbounded) degree was proven in [11]. The absence of short cycles insure the absence of cliques in these graphs. So they are essentially different from small world graph of symmetric binary relation on the set of all peoples on the earth: two persons know each other (clearly, each university department is an example of a clique).

3. Cryptosystem requirements and properties of graph based algorithms. Assume that an unencrypted message, *plaintext*, which can be image data, is a string of bits. It is to be transformed into an encrypted string or *ciphertext*, by means of a cryptographic algorithm and a *key*: so that the recipient can read the message, encryption must be *invertible*.

Conventional wisdom holds that in order to defy easy decryption, a cryptographic algorithm should produce seeming chaos: that is, ciphertext should look and test random. In theory an eavesdropper should not be able to determine any significant information from an intercepted ciphertext. Broadly speaking, attacks to a cryptosystem fall into 2 categories: *passive attacks*, in which adversary monitors the communication channel, and *active attacks*, in which the adversary may transmit messages to obtain information (e.g., ciphertext of chosen plaintext).

Attackers hope to determine the plaintext from the ciphertext they capture; an even more successful attacks will determine the key and thus comprise the whole set of messages.

An assumption first codified by Kerckhoffs in the nineteen century is that the algorithm is known and the security of algorithm rests entirely on the security of the key.

Cryptographers have been improving their algorithms to resist the following two major types of attacks:

i) *ciphertext only* – the adversary has access to the encrypted communications.

ii) *known plaintext* – the adversary has some plaintext and its corresponding ciphertext.

Nowadays the security of the plaintext rests on encryption algorithm (or private key algorithm), depended on chosen key (password), which has good resistance to attacks of type (i), and algorithm for the key exchange with good resistance to attacks of type (ii) (public key algorithm).

The revolutionary classical result on private key algorithm was obtained by C. Shannon at the end of 40th (see [15, 16] or [28]. He constructed so-called *absolutely secure* algorithms, whose keys and strings of random bits at least as long as a message itself, achieve the seeming impossibility: an eavesdropper is not able to determine any significant information from obtained ciphertext. The simplest classical example is the following one-time pad: if p_i is the i-th bit of the plaintext, k_i is the i-th bit of the key, and c_i is the first bit of the ciphertext, then $c_i = p_i + k_i$, where $+$ is exclusive or, often written XOR, and is simply addition modulo 2. One time pads must be used exactly once: if a key is ever reused, the system becomes highly vulnerable.

It is clear that the encryption scheme as above, like most private key algorithm, is irresistible to attacks of type (ii) – you need just subtract p_i from c_i and get the key.

The theoretical resistance of well-known RSA algorithms to attacks of type (ii) rests on our believe that nobody can factor numbers fast.

In the case of our encryption schemes based on k-regular simple graph of girth g the idea based on fact that finding a pass between 2 given vertices at a distance $d < g/2$ of infinite k- regular tree require non polynomial expression $f(k,d)$ for the number of steps (natural branching process give us $k(k-1)^{d-1}$ steps (number of passes between plaintext and ciphertext), the faster general algorithm is unknown). If the distance d is unknown the problem getting harder, the complexity $f(k,d)$ is growing, when d is increasing (see [34], in more details). Recall, that for each k there is an infinite family of finite k-regular graphs of increasing girth.

For instance, in case of q-regular bipartite graphs $D(k,q)$, $k \geq 2$, q is prime power ≥ 3 we have q^n points and q^n lines, girth is $\geq (n+4)$. So we can work with passes of length $(n+4)/2$. In this case the plainspace (say the set of points) has cardinality $v = q^n$, so the size of key space is $\mathrm{Key} = q(q-1)^{(n+4)/2}$. If q is large, then Key is approximately $v^{1/2}$. In case of graphs $CD(k,q)$ we have Key is approximately $v^{2/3}$.

Let us consider the infinite family of finite generalised 6-gons. They are $(q+1)$-regular bipartite graphs with partition sets of cardinality $1+q+q^2+q^3+$

$q^4 + q^5$ each, girth 12 and diameter 5. We shall assume that prime power $q > 2$ is increasing. In this case we can chose 5 as length of the password. So, the size of plainspase is $v = 1 + q + q^2 + q^3 + q^4 + q^5$ and the key space has cardinality $\mathrm{Key} = (q + 1)q^4$. We can notice that Key/v is going to 1, when q is going to infinity.

In fact the above complexity estimates are applicable to directed graph based algorithms as well.

4. Binary relations and related rainbow-like graphs. The missing theoretical definitions on directed graphs the reader can find on [27]. Let Φ be an irreflexive binary relation over the set V, i.e., $\Phi \in V \times V$ and for each v pair (v, v) is not the element of Φ.

We say that u is the neighbour of v if $(v, u) \in \Phi$ We use term *binary relation graph* for the graph Γ of irreflexive binary relation ϕ over finite set V such that for each $v \in V$ sets $\{x|(x, v) \in \phi\}$ and $\{x|(v, x) \in \phi\}$ have same cardinality. It is a directed graph without loops and multiple edges, see [27] for more general definitions).

Let Γ be the graph of binary relation. The *pass* between vertices a and b is the sequence $a = x_0 \to x_1 \to \dots x_s = b$ of length s, where x_i, $i = 0, 1, \dots s$ are distinct vertices.

We say that the pair of passes $a = x_0 \to x_1 \to \cdots \to x_s = b$, $s \geq 1$ and $a = y_0 \to y_1 \to \cdots \to y_t = b$, $t \geq 1$ form an (s, t)- commutative diagram $O_{s,t}$ if $x_i \neq y_j$ for $0 < i < s$, $0 < j < t$.

We refer to the number $s + t$ as the rank of $O_{s,t}$. It is ≥ 3, because the graph does not contain multiple edges.

We introduce the *girth* of binary relation graph Γ as the minimal rank of its $O_{s,t}$ diagram with $s + r \geq 3$. Notice, that the graph of binary relation of girth t may have a directed cycle $O_s = O_{s,0}$: $v_0 \to v_1 \to \dots v_{s-1} \to v_0$, where v_i, $i = 0, 1, \dots, s - 1$, $s \leq t$ are distinct vertices.

In the case of symmetric irreflexive relations the above general definition of the girth agrees with the standard definition of the girth of simple graph i.e the length of its minimal cycle, For simple graphs index and girth are equal.

For the investigation of commutative diagrams we introduce *girth indicator* gi, which is the minimal value for $\max(s, t)$ for parameters s, t of commutative diagram $O_{s,t}$, $s + t \geq 13$. Notice, that two vertices v and u at distance $<$ gi are connected by unique pass from u to v of length $<$ gi.

In case of symmetric binary relation $\mathrm{gi} = d$ implies that the girth of the graph is $2d$ or $2d - 1$. it does not contain even cycle $2d - 2$. In general case $\mathrm{gi} = d$

implies that $g \geq d+1$. So if the case of family of graphs with unbounded girth indicator, the girth is also is unbounded. We have also gi $\geq g/2$.

We will use term *the family of graphs of large girth* for the family of regular graphs Γ_i of degree k_i and order v_i such that $\mathrm{gi}(\Gamma_i)$ and $\mathrm{ind}(\Gamma_i)$ are $\geq c\log_{k_i}(v_i)$, where c' is the independent on i constant. So the size of such graphs is quite close to the bound (2).

As it follows from the definition $g(\Gamma_i) \geq c'\log_{k_i}(v_i)$ for appropriate constant c'. So, it agrees with the well known definition for simple graphs (see the Section 2).

5. Graphs with special colouring of vertices and edges, case of large girth. We shall use term *the family of algebraic graphs* for the family of graphs $\Gamma(K)$, K belongs to some infinite class F of commutative rings, such that the neighbourhood of each vertex of $\Gamma(K)$ and the vertex set itself are quasiprojective varieties over K of dimension ≥ 1 (see [2] for the case of simple graphs).

Such a family can be treated as special Turing machine with the internal and external alphabet K.

We say that the graph Γ of binary relation Φ has a rainbow-like colouring over the set of colours C if for each v, $v \in V$ we have a colouring function ρ_v, which is a bijection from the neighbourhood $St(v)$ of v onto C, such that the operator $N_c(v)$ of taking the neighbour of v with colour c is the bijection of V onto V.

We say that the rainbow-like colouring ρ is invertible if there is a rainbow-like colouring of Φ^{-1} over C' such that ${N_c}^{-1} = N'_{c'}$ for some colour $c' \in C'$.

Example 1. *Cayley graphs*

Let G be the group and S be subset of distinct generators, then the binary relation $\phi = \{(g_1, g_2)|g_i \in G, i = 1, 2, g_1{g_2}^{-1} \in S$: admit the rainbow-like colouring $\rho(g_1, g_2) = g_1{g_2}^{-1}$

This rainbow-like colouring is invertible because the inverse graph $\phi^{-1} = \{(g_2, g_1)|g_1{g_2}^{-1} \in S\}$ admit the rainbow-like colouring $\rho^{'}(g_2, g_1) = g_2{g_1}^{-1} \in S^{-1}$.

Example 2. *Parallelotopic graphs and latin squares*

Let G be the graph with the colouring $\mu : V(G) \to C$ of the set of vertices $V(G)$ into colours from C such that the neighbourhood of each vertex looks like rainbow, i.e., consists of $|C|$ vertices of different colours. In case of pair (G, μ) we shall refer to G as *parallelotopic graph* with the local projection μ (see [32, 33] and further references).

It is obvious that parallelotopic graphs are k-regular with $k = |C|$. If C' is a subset of C, then induced subgraph $G^{C'}$ of G which consists of all vertices with colours from C' is also a parallelotopic graph. It is clear that connected component of the parallelotopic graph is also a parallelotopic graph.

The *arc* of the graph G is a sequence of vertices $v_1, \dots, v_k$ such that $v_i I v_{i+1}$ for $i = 1, \dots, k-1$ and $v_i \neq v_{i+2}$ for $i = 1, \dots, k-2$. If $v_1, \dots, v_k$ is an arc of the parallelotopic graph (G, μ) then $\mu(v_i) \neq \mu(v_{i+2})$ for $i = 1, \dots, k-2$.

For the examples see [32, 34, 35].

Let $+$ be the latin square defined on the set of colours C. Let us assume $\rho(u, v) = \mu(u) - \mu(v)$. The operator $N_c(u)$ of taking the neighbour of the color is invertible, ${N_c}^{-1} = N_{-c}$, where $-c$ is the opposite for c element in the latin square. It means that ρ is invertible raibow-like colouring.

We shall consider some examples of graphs with parallelotopic colouring in the Sections 8 and 9.

6. The algorithm.

6.1. General symmetric algorithm. Let us consider the encryption algorithm corresponding to the graph Γ with the chosen invertible rainbow-like colouring of edges.

Let $\rho(u, v)$ be the colour of arrow $u \to v$, C is the totality of colours and $N_c(u)$ is the operator of taking the neighbour of u with the colour c.

The password be the string of colours $(c_1, c_2, \dots, c_s)$ and the encryption procedure is the composition $N_{c_1} \times N_{c_2} \dots N_{c_s}$ of bijective maps $N_{c_i} : V(\Gamma) \to V(\Gamma)$. So if the plaintext $v \in V(\Gamma)$ is given, then the encryption procedure corresponds to the following chain in the graph: $x_0 = v \to x_1 = N_{c_1}(x_0) \to x_2 = N_{c_2}(x_1) \to \cdots \to x_s = N_{c_s}(x_{s-1}) = u$. The vertex u is the ciphertext.

Let $N'_{c'}(N_c(v)) = v$ for each $v \in V(\Gamma)$. The decryption procedure corresponds to the composition of maps $N'_{c'_s}$, $N'_{c'_{s-1}}$, $\dots, N'_{c'_1}$. The above scheme gives a symmetric encryption algorithm with flexible length of the password (key). Let $A(\Gamma, \rho, s)$ be the above encryption scheme. The following statement is immediate corollary from definitions.

Lemma 2. *Let Γ be the invertible rainbow-like graph of girth g and $A(\Gamma, \rho, s)$ be the above encryption scheme for $s <$ (gi). Then different passwords produce distinct ciphertexts, plaintext and corresponding ciphertext are different.*

6.2. Symbolic computation and public keys. Let K be the commutative ring. Recall that graph Γ be the algebraic graph over K if the set of vertices $V(\Gamma)$ and the neighbourhood of each vertex u are algebraic quasiprojective varieties over the ring K (see [2]).

In the case of *symbolic invertible rainbow-like graph* (Γ, ρ, ρ'), the vertex set $V(\Gamma)$ and the neighbourhoods of each vertex are open algebraic varieties in Zarissky topology as well as the colour set C, maps $N(c, v) = N_c(u)$ and $N'(c, v) = N'_c(u)$ are polynomial maps from $C \times V(\Gamma)$ onto $V(\Gamma)$.

In the case of symbolic rainbow-like graph the encryption as above with the key $(t_1, t_2, \ldots, t_k)$ given by some polynomial map from $C^k \times V(\Gamma) \to V(\Gamma)$. We can treat t_i, $i = 1, \ldots, k$ as symbolic variables.

The specializations $t_i = \alpha_i \in K$ gives the public key map $P : V(\Gamma) \to V(\Gamma)$. Like in the known example of polynomial encryption proposed by Imai and Matsumoto we can combine P with two affine transformations T_1 and T_2 and work with the public map $Q = T_1 P T_2$.

Let us use the characters Alice and Bob from books on Cryptography [15, 16] or [28], where Bob is public user and Alice is a key holder. So she knows the string $t_1, \ldots, , t_s$, the graph and affine transformations T_1 and T_2. She can decrypt via consecutive applications of ${T_2}^{-1}$, $N'_{t'_k}$, $N'_{t'_k-1}, \ldots N'_{t_1}$ and ${T_1}^{-1}$.

The public user Bob has the encryption map Q only. He can encrypt, but the decryption is hard task because (1) Q is the polynomial map of degree ≥ 2 from many variables. (2) Even in the case when Bob knows T_1, T_2 and the graph Γ. The problem of finding the pass between the plaintext vertex and the ciphertext vertex has complexity $n \ln n$, where $n = |V(\Gamma)|$. So Bob is not able decrypt if the plainspace is large enough.

7. Generalised polygons and rainbow-like graphs. E. Moore [26] used term *tactical configuration* of order (s, t) for biregular bipartite simple graphs with bidegrees $s + 1$ and $r + 1$. It is an incidence stucture with the point set P, line set L and symmetric incidence relation I. Its size can be computed as $|P|(s + 1)$ or $|L|(t + 1)$.

Let $F = \{(p, l) | p \in P, l \in L, pIl\}$ be the totality of flags for the incidence structure (P, L, I). We define the following irreflexive binary relation ϕ on the set F:

$((l_1, p_1), (l_2, p_2)) \in \phi$ if and only if $p_1 I l_2$, $p_1 \neq p_2$ and $l_1 \neq l_2$. Let $F(I)$ be the binary relation graph corresponding to ϕ. We refer to it as *directed flag graph* of I.

Lemma 3. *Let (P, L, I) be a tactical configuration of girth $g \geq 2k$. Then the girth indicator of $F(I)$ is $> k$.*

Parallelotopic tactical configuration (P, L, I) is an incidence structure with colouring functions $\mu_p : P \to C_p$ and $\mu_l : L \to C_l$ such that for each point $p \in P$ (line $l \in L$) there is the unique neighbour $n_c(p) \in L$ ($n_c(l) \in P$ of colour c from C_l (C_p, respectively).

Some encryption schemes connected with the parallelotopic tactical configurations of high girth had been introduced in [34].

Let (P, L, I) be the parallelotopic tactical configuration with the colouring functions $\mu_p : L \to C_p$ and $\mu_l :\to C_l$ and $+_p$, $+_l$ are latin squares on C_p and C_l, respectively.

The directed flag graph $F(I)$ admit the following invertible rainbow-like colouring ρ of edges: the value of $\rho(f_1, f_2)$ for $f_1 = (l_1, p_1)$ with $\mu_l(l_1) = c_1$, $\mu_p(p_1) = d_1$ and $f_2 = (l_2, p_2)$ with $\mu_l(l_2) = c_2$, $\mu_p(p_2) = d_2$ such that $f_1 I f_2$ is the pair $(c_2 - c_1, d_2 - d_1)$ from the set of colours $(C_l - \{0\}) \times (C_l - \{0\}$.

Generalised m-gons $GP_m(r, s)$ of order (r, s) were defined by J. Tits in 1959 (see [8, 5] and further references) as tactical configurations of order (s, t) of girth $2m$ and diameter m.

According to well known Feit–Higman theorem a finite generalised m-gon of order (s, t) has $m \in \{3, 4, 6, 8, 12\}$ unless $s = t = 1$.

The known examples of generalised m-gons of bidegrees ≥ 3 and $m \in \{3, 4, 6, 8\}$ include rank 2 incidence graphs of finite simple groups of Lie type (see [4]). The regular incidence stuctures are for $m = 3$ (groups $A_2(q)$), $m = 4$ (groups $B_2(q)$) and $m = 6$ (group $G_2(q)$). In all cases $s = t = q$, where q is prime power.

The biregular but not regular generalised m-gons have parameters $s = q^\alpha$, $t = q^\beta$, where q is a prime power. The list is below: $s = q$, $t = q^2$, q is arbitrary large prime power for $m = 4$; $s = q^2$, $t = q^3$, where $q = 3^{2k+1}$, $k > 1$ for $m = 6$; $s = q$, $t = q^2$, $q = 2^{2k+1}$ for $m = 8$.

Lemma 4. *Let (P, L, I) be the generalised $2k$-gon of order (r, s). Then*

$$|P| = \sum_{t=0,k-1} (r^t s^t + r^{t+1} s^t), \qquad |L| = \sum_{t=0,k-1} (s^t r^t + s^{t+1} r^s).$$

Lemma 5. *Let (P, L, I) be regular generalised m-gon of degree $q + 1$. Then $|P| = |L| = 1 + q + \cdots + q^{m-1}$.*

Let (P, L, I) be a regular tactical configuration of order (t, t). The *double configuration I'* is the incidence graph of the following incidence structure (P', L', I') : $P' = F(I) = \{(p, l) | p \in P, l \in L, pIl\}$, $L' = P \cup L$, $f = (p, l)Ix$,

$x \in L'$ if $p = x$ or $l = x$. It is clear that the order of tactical configuration I' is $(1, t)$. If (P, L, I) is a regular generalised m-gon, then (P', L', I') is a generalised $2m$-gon.

Let (P, L, I) be the generalised m-gon associated with the rank 2 finite simple group G of Lie type. It is an edge transitive tactical configuration of order (s, t), $s > 1$, $t > 1$.

Let B the Borel subgroup of G , S_p and S_l are largest orbits of B on P and L, respectively. Then *Schubert graph* $S(G)$ (affine part of generalised m-gon, see [34]) is the induced graph of I on the vertex set $S_p \cup S_l$.

Proposition 6. *The directed flag graph of the Schubert graph $S(G)$ or the directed flag graph of double configuration of the regular Schubert graph admit the symbolic rainbow-like colourings.*

Proof. Let U be the unipotent subgroup of the standard Borel subgroup for G, U_1 and U_2 are root subgroups corresponding to simple roots. The partition sets of $S(G)$ can be identified with the totalities of left cosets $P = (U : U_1)$ and $L = (U : U_2)$. Two cosets from gU_1 and hU_2 are incident if and only if their intersection is not the empty set. Let $U' = [U_1, U_2]$ be the mutual commutant of U_1 and U_2. Then the group U admits the factorisation U_1U_2U', i.e., each element u in U can be presented uniquely in the form u_1u_2u', where $u_i \in U_i$, $i = 1, 2$ and $u' \in U'$. Groups U_2U' and U_1U' act regularly on $U : U_1$ and $U; U_2$, respectively. So we can identify the element u_iu', $i = 1, 2$ with the corresponding left coset. We can consider the parallelotopic colouring $\mu(u_iu') = u_i$, $i = 1, 2$ and consider the standard rainbow-like colouring of the directed flag graph for $S(G)$ corresponding to μ.

In the case of double flag graph $DS(G)$ of regular $S(G)$ we have isomorphic subgroups U_1 and U_2. The directed flag graph $F(DS(G))$for $DS(G)$ is the bipartite graph, its partition sets can be identified with two copies U_p and U_l of group U. Let $u_p \in U_p$ and $u_l \in U_l$. We have $u_p \to u_l$ if $u_l = u_pu_1$ for some element $u_1 \in U_1$ and $u_l \to u_p$ if $u_p = u_lu_2$ for some $u_2 \in U_2$. Notice, that U_1 is isomorphic to U_2 and u_1 and u_2 serve as colours for rainbow-like colouring of the graph.

If group G defined over F_q, then the vertex set of the above graphs are open algebraic variety over F_q and in each case the operator of taking neighbour of chosen colour is a polynomial map over F_q. So the colourings as above are symbolic rainbow-like colourings. □

Proposition 7. *Let (P, L, I) be the finite generalised polygon associated with the group G of Lie type of rank* 2.

(i) Then its directed flag graph admit an invertible rainbow-like colouring

(ii) If (P, LI) is a regular tactical configuration, then its directed flag graph of the double graph admit an invertible rainbow-like colouring.

Proof. We can assume that $P = (G : P_1)$ and $L = (G : P_2)$, where P_1 and P_2 are standard maximal parabolic subgroups. Vertices $l \in L$ and $p \in P$ of generalised polygon form the vertex of the directed flag graph $DF(G)$ if cosets p and l have non empty intersection. It is clear, that the vertices of the flag graph can be identified with the cosets by standard Borel subgroup $B = P_1 \cup P_2$.

Let α be the vertex, then the stabiliser G_α of α in G is isomorphic to B. The neighbours of α form the orbit of order $|U_1| \times |U_2|$. The action of unipotent subgroup of G_α is similar to regular action of $U_1 \times U_2$. So we can use the elements of this group as colours for the rainbow-like colouring. So we proved the point (i).

If (P, L, I) be the regular tactical configuration, the directed flag of double configurations is a bipartite graph. Its partition sets can be identified with two copies of manifold $(G : B)$. The unipotent subgroup of stabilizer G_α of vertex α acts on the neighbourhood as regular action of U_1 or U_2. So elements of this group can be used as colours of arrows of the directed flag graph. □

Remark 1. Directed flag graphs of generalised polygons do not admit a symbolic rainbow-like colouring, because their vertex-sets are closed projective varieties. So the operators of taking the neighbour along the edge of chosen colour are not a polynomial maps.

Remark 2. The invertible rainbow-like colouring can be defined on the directed flag graphs of any generalised polygon in terms of distance on the graph. In particular, it can be done for any projective plane (regular generalised triangle).

8. The incidence structures defined over commutative rings.

We define the family of graphs $D(k, K)$, where $k > 2$ is positive integer and K is a commutative ring, such graphs have been considered in [14] for the case $K = F_q$ (some examples are in [17]).

Let P and L be two copies of Cartesian power K^N, where K is the commutative ring and N is the set of positive integer numbers. Elements of P will be called *points* and those of L *lines*.

To distinguish points from lines we use parentheses and brackets: If $x \in V$, then $(x) \in P$ and $[x] \in L$. It will also be advantageous to adopt the notation for co-ordinates of points and lines introduced in [18] for the case of general commutative ring K:

$$(p) = (p_{0,1}, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, p'_{2,2}, p_{2,3}, \ldots, p_{i,i}, p'_{i,i}, p_{i,i+1}, p_{i+1,i}, \ldots),$$

$$[l] = [l_{1,0}, l_{1,1}, l_{1,2}, l_{2,1}, l_{2,2}, l'_{2,2}, l_{2,3}, \ldots, l_{i,i}, l'_{i,i}, l_{i,i+1}, l_{i+1,i}, \ldots].$$

The elements of P and L can be thought as infinite ordered tuples of elements from K, such that only finite number of components are different from zero.

We now define an incidence structure (P, L, I) as follows. We say the point (p) is incident with the line $[l]$, and we write $(p)I[l]$, if the following relations between their co-ordinates hold:

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

(This four relations are defined for $i \geq 1$, $p'_{1,1} = p_{1,1}$, $l'_{1,1} = l_{1,1}$). This incidence structure (P, L, I) we denote as $D(K)$. We identify it with the bipartite *incidence graph* of (P, L, I), which has the vertex set $P \cup L$ and edge set consisting of all pairs $\{(p), [l]\}$ for which $(p)I[l]$.

For each positive integer $k \geq 2$ we obtain an incidence structure (P_k, L_k, I_k) as follows. First, P_k and L_k are obtained from P and L, respectively, by simply projecting each vector onto its k initial coordinates with respect to the above order. The incidence I_k is then defined by imposing the first $k-1$ incidence equations and ignoring all others. The incidence graph corresponding to the structure (P_k, L_k, I_k) is denoted by $D(k, K)$.

To facilitate notation in future results, it will be convenient for us to define $p_{-1,0} = l_{0,-1} = p_{1,0} = l_{0,1} = 0$, $p_{0,0} = l_{0,0} = -1$, $p'_{0,0} = l'_{0,0} = -1$, and to assume that (6) are defined for $i \geq 0$.

Notice that for $i = 0$, the four conditions (1) are satisfied by every point and line, and, for $i = 1$, the first two equations coincide and give $l_{1,1} - p_{1,1} = l_{1,0}p_{0,1}$.

The incidence relation motivated by the linear interpretation of Lie geometries in terms their Lie algebras [31] (see [33]). Let us define the "root subgroups" U_α, where the "root" α belongs to the root system Root $= \{(1,0), (0,1), (1,1), (1,2), (2,1), (2,2), (2,2)' \ldots, (i,i), (i,i)', (i,i+1), (i+1,i) \ldots\}$. The "root system above" contains all real and imaginary roots of the Kac-Moody Lie Algebra $\tilde{A}_1$ with the symmetric Cartan matrix. We just doubling imaginary roots (i,i) by introducing $(i,i)'$.

Remark. For $K = F_q$ the following statement had been formulated in [20].

Let $k \geq 6$, $t = [(k+2)/4]$, and let $u = (u_\alpha, u_{11}, \ldots, u_{tt}, u'_{tt}, u_{t,t+1}, u_{t+1,t}, \ldots)$ be a vertex of $\mathrm{D}(k,K)$ ($\alpha \in \{(1,0),(0,1)\}$, it does not matter whether u is a point or a line). For every r, $2 \leq r \leq t$, let

$$a_r = a_r(u) = \sum_{i=0,r} (u_{ii}u'_{r-i,r-i} - u_{i,i+1}u_{r-i,r-i-1}),$$

and $a = a(u) = (a_2, a_3, \cdots, a_t)$.

Proposition 8. *(i) The classes of equivalence relation $\tau = \{(u,v) | a(u) = a(v)\}$ are connected components of graph $D(n,K)$, where $n \geq 2$ and K be the ring with unity of odd characteristic.*

(ii) For any $t-1$ ring elements $x_i \in K$), $2 \leq t \geq [(k+2)/4]$, there exists a vertex v of $\mathrm{D}(k,K)$ *for which*

$a(v) = (x_2, \ldots, x_t) = (x)$.

(3i) The equivalence class C for the equivalence relation τ on the set $K^n \cup K^n$ is isomorphic to the affine variety $K^t \cup K^t$, $t = [4/3n]+1$ for $n = 0,2,3$ mod 4*, $t = [4/3n]+2$ for $n = 1$* mod 4.

Remark. Let K be the general commutative ring and C be the equivalence class on τ on the vertex set $\mathrm{D}(K)$ ($\mathrm{D}(n,K)$, then the induced subgraph, with the vertex set C is the union of several connected components of $\mathrm{D}(K)$ ($\mathrm{D}(n,K)$).

Without loss of generality we may assume that for the vertex v of $C(n,K)$ satisfying $a_2(v) = 0, \ldots a_t(v) = 0$. We can find the values of components $v'_{i,i)}$ from this system of equations and eliminate them. Thus we can identify P and L with elements of K^t, where $t = [3/4n]+1$ for $n = 0,2,3$ mod 4, and $t = [3/4n]+2$ for $n = 1$ mod 4.

We shall use notation $C(t,K)$ ($C(K)$) for the induced subgraph of $D(n,K)$ with the vertex set C.

Remark. If $K = F_q$, q is odd, then the graph $C(t,k)$ coincides with the connected component $CD(n,q)$ of the graph $D(n,q)$ (see [17]), graph $C(F_q)$ is a q-regular tree. In other cases the question on the connectivity of $C(t,K)$ is open. It is clear that $g(C(t,F_q))$ is $\geq 2[2t/3]+4$.

Proposition 9. *Projective limit of graphs $D(n,K)$ (graphs $C(t,K)$, $CD(n,K)$) with respect to standard morphisms of $D(n+1,K)$ onto $D(n,K)$ (their restrictions on induced subgraphs) equals to $D(K)$ $(C(K)$.*

If K is an integrity domain, then $D(K)$ and $CD(K)$ are forests. Let C be the connected component, i.e tree.

It is well known that a continuous bijection of the interval $[a,b]$ has a fixed point. In case of open variety K^n, where K is commutative ring situation is different. For each pair (K,n), $n \geq 3$ and each $t \in K - \{0\}$ we shall construct a linguistic dynamical system, i.e family $F = F_n(K) = \{f_t\}$ of invertible nonlinear polynomial maps $f_t : K^n \to K^n$ without fixed points ($f_t(x) \neq x$ for each $x \in K^n$), such that ${f_t}^{-1} = f_{-t}$ and $t_1 \neq t_2$ implies $f_{t_1}(x) \neq f_{t_2}(x)$ for each x.

For each sting $\mathrm{a} = (a_1, \dots a_s)$ we consider the composition $G_{\mathrm{a}} = f_{a_1} \times f_{a_2} \times \dots f_{a_s}$ of transformations f_{a_i}, $i = 1, \dots, s$.

We shall refer to a string $\mathrm{a} = (a_1, \dots, a_s)$ with regular elements (not zero divisors) $a_i + a_{i+1}$, $i = 1, \dots, s-1$ as regular string of length s. Let $R_s = R_s(K)$ be the totality of all regular string of length s.

The rank $r = r(F)$, $r \geq 1$ of linguistic dynamical system F is the maximal number s such that for each $\mathrm{a} \in R_s$ the condition $G_{\mathrm{a}}(x) = G_{\mathrm{b}}(x)$, $b \in K - \{0\}^l$, $l \leq s$ implies $\mathrm{a} = \mathrm{b}$. Let us consider simple graph $\Gamma = \Gamma(F)$ of the dynamical system F with the vertex set $V = K^n$ such that $u \in V$ and $v \in V$ are connected by edge if and only $f_t(u) = v$ for some $t \in K$.

The property $r(F) \geq s$ means that for each vertex x and $\mathrm{a} \in R_s$ vertices x and $G_{\mathrm{a}}(x)$ are connected by the unique pass of length $\leq s$.

Recall that the girth $g = g(\Gamma)$ of the simple graph Γ is the length of its smallest cycle.

Property $r(F) \geq s$ implies that in case of integral domain K the girth g of the graph $\Gamma(F)$ is $> 2s$.

In [41] the family of dynamical systems $L_n(K)$, $n \neq 0 (\mathrm{mod})\ 3$ is even number ≥ 2 of rank $r \geq 1/3n$ had been constructed explicitly.

We consider the definition of *arithmetical dynamical system* $F = \{f_\alpha | \alpha \in Q\}$ simply via consideration of quasiprojective manyfold M of K^n instead of K^n and requirement $f_\alpha - 1 \in F$ instead of ${f_\alpha}^{-1} = f_{-\alpha}$, Q is just a subset of K. Major justification of *arithmetical graphs* related to such dynamical systems is that they are examples of *graphs with memory*, because we can not only consider such a graph as finite automaton where states v and $f_\alpha(v)$ are connected by the arrow with the label α, but each state v is a string of characters from the alphabet K.

Theorem 10. *Let $N_x(\mathrm{v})$ be the operator of taking the neighbour of the vertex $\mathrm{v} = (v_1, v_2, \dots, v_s)$ of the colour $v_1 + x$ in the graph $D(n,K)$.*

Then this operator defines an arithmetical dynamic system $D_n(K)$ on $K^n \cup K^n$ of rank $d = [(n+5)/2] - 1$.

Operator N_x preserves connected components of $D(n, K)$ and blocks of equivalence relation τ.

Corollary 11. *Let $N'_x(v)$, $t \in K$ be the operator of taking the neighbour of the vertex* v *of the colour $v_1 + x$ in the parallelotopic graph $C(t, K)$, which is the restriction of operator $N_x(v)$ on the equivalence class C. Then it defines arithmetical dynamic system $C_t(K)$ on $K^t \cup K^t$ over $Q = K$ of rank $d = [2/3t] + 1$.*

Let us consider the directed flag graph $F(t, K)$ of the tactical configuration $C(t, K)$. We can consider the symbolic invertible rainbow-like colouring $\rho(f_1, f_2)$ of $F(t, K)$ defined on the colour set $K^* \times K^*$ by the following rule:

Let $f_1 = ([l^1], (p^1))$, $f_2 = ([l^2], (p^2))$ form the arrow in $F(t, K)$. So, $[l_2]I(p_1)$. We assume that $\rho(f_1, f_2) = (l^1_{1,0} - l^2_{1,0}, p^1_{0,1} - l^2_{0,1})$.

If K is finite, then the cardinality of the colour set is $(|K| - 1)^2$. Let Reg$K$be the totality of regular elements, i.e., not zero divisors. Let us delete all arrows with colour (x, y), where one of the elements x and y is not a zero divisor. New graph $RF(t, K)$ is a symbolic rainbow-like graph over the set of colours $(\mathrm{RegK})^2$

The following statement follows immediately from the above corollary.

Theorem 12. *The girth indicator* gi *of the symbolic rainbow-like graph $RF(t, K)$ is $\geq 2/3t$.*

Proof. Let $N_\alpha(v)$ be the operator of taking the neighbour of vertex v with the colour $\mu(v) + \alpha$. Let $\alpha_1, \alpha_2, \ldots, \alpha_d$, $d = 2s + 1$ be regular string of arithmetical dynamical system related to the graph of odd length. Let $[x]$ be the line in the graph $C(t, K)$. Then $[x], N_{\alpha_1}(x)$ be the vertex f_1 of the directed flag graph for $C(t, K)$. We can obtain each vertex of $F(t, K)$ (or $RF(t, K)$) by appropriate choice of $[x]$ and α_1. Elements of kind $(u = N_{\alpha_{2i}}(\ldots N_{\alpha_2})(N_{\alpha_1}([x]), N_{\alpha_{2i+1}}(u))$, $1 \leq i \leq s$ form the pass in the graph $RF(t, K)$, because the rainbow-like colours of the edges between each two consecutive flags are the regular elements. We can obtain any pass of $RF(K)$ by appropriate choice of starting line $[x]$ and regular string. The existence of $O_{s,k}$ commutative diagram, $s \geq k$ means that for two different regular strings $(\alpha_1, \ldots, \alpha_{2s+1})$ and $\beta_1, \ldots \beta_{2k+1}$ the images of $[x]$ under compositiona of $N_{\alpha_1}, \ldots N_{\alpha_{2s}}$ and $N_{\beta_1} \ldots N_{\beta_{2k}}$ are same. If $2s$ is than the rank d of dynamical system it is impossible. So $2s \geq d$ the girth indicator gi of dynamical system is $\geq 1/3t$. □

Corollary 13. *Let K be a finite such that $k = |\mathrm{Reg}K| \geq 2$. Then graphs*

$RF(t, K)$, $t = 1, 2, \ldots$ form the family of symbolic rainbow-like graphs of large girth of bounded degree.

In [36] the reader can find the implementation of the algorithm of Section 3 for the case of family $RF(n, F_q)$ on the base of "Mathematika" package. The generalisation of this algorithm the reader can find in [43].

Remark 1. The plainspace (or cipherspace) for graph based encryption corresponding to each graph in this section (or its connected component) has structure of free module $V = K^l$ over the commutative ring K. The affine transformation $x \to Ax+b$, where x is the column tuple from V, A is an invertible matrix and b is a fixed tuple, is sparse if the time of its execution is bounded by independent on size of the plainspace and keyspace constant. Let e be encryption transformation. If we apply $e' = \tau^{-1}e\tau$ (composition of τ^{-1}, e and τ, where τ is sparse affine transformation), then it is still fast, ciphertext is different from the plaintext, because of e and e' are conjugate permutations on the plainspace. case Notice, that e' can be given by effective explicit formula for computation (via maps of kind $\tau^{-1}N_\alpha\tau$). In fact e' has better security because the original family of graphs is hidden.

Remark 2. Let us consider the family of graphs $CD(n, q)$, where n is growing but odd q is fixed. Points and lines of the graph are tuples over F_q. The operator of "deleting" the last component of the tuple is colour preserving graph homomorphism from $CD(n, q)$ onto $CD(n-1, q)$. So we have a folder of parallelotopic graphs in sense of [34] and projective limit of $CD(n, q)$ is well defined. Graphs $(CD(n, q)$ are connected. It insure the following property of Turing encryption machine related to this family of graphs: Let T be the pert of the plaintext at the beginning (with respect to natural order of components) and T' be arbitrarily chosen text. If we consider the algorithm working with "potentially infinite" plaintext and password, then there is the password such that T will be transformed into T'.

This magic password is hard to find: one can think that say T is first unit of Koblitcz book [15] and T' is translation of T in Spanish (assume that and size of T and T' are the same, English and Spanish use the same Latin alphabet). So in this case the password will do translator's job.

This theoretical property demonstrate good mixing properties of related encryption. Notice that each block cipher (like DES, AES etc) is principally different from our graph based encryption. If we consider the text which is constant on each block, then the ciphertext will be also periodical on blocks.

By the modulo of conjecture on small world properties of the family (in case of bounded degree) the length of the magic password will be $O(l)$ where l is the length of the text T.

Remark 3. Remark 2 is applicable to each family F of connected components for every family of bounded degree from this section.

Remark 4. Family F as above defines stream cipher, in fact, the component y_i of the ciphertext depends only from the first i components. The implementations show that change of one character from the password leads to the change of more than 99 percents of ciphertext's characters. The change of i-th character of the plaintext tuple lead to change of more than 99 percent of ciphertext's components on the position j, $j \geq i$. This mixing properties are much better in comparison with the case of stream cipher $RC4$. Conjugation of graph based encryption with special sparse affine transformation τ allows get the encryption rule which will change 99 percent of the entire text with the change of one character from the plaintext.

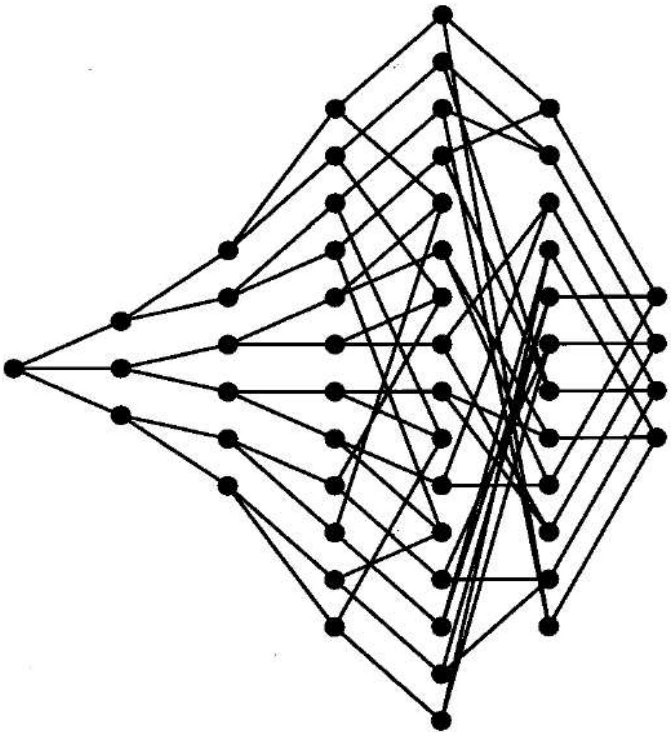
Remark 5. The speed of graph based algorithms based on family F compares well with the speed of very fast but not very secure stream cipher $RC4$. The tables of GRAPHICAL APPENDIX reflect execution time evaluation of 4 algorithms: $RC4$, GE1 (based on graphs $CD(n, 256)$, see [30]) and $GE2$ (based on $RF(t, Z_{2^{32}})$. Size of the key is given in bites (40, 48, ...), the size of the plaintext is given in MB's (7.6 and 55 MB's are chosen). All computations are conducted on the same computer (by an Intel Pentium 1.6 GHz processors workstation, ORACLE 9i DBMS Server), PL/SQL programming language has been used. Experiment demonstrates that such graph based encryption can be used for the encryption of large data (Geological Information Systems, other Oracle based data bases).

In [12] graphs $CD(n, 127)$ had been used, the execution with key-size 48 of graph based algorithm were 20 time slower than $RC4$.

At the beginning of the GRAPHICAL APPENDIX the graph CD(3, 3) is depicted (graphs $CD(n, 256)$ are too dense for drawing).

9. Conclusion.

We can see that both known families of simple graphs of large girth of bounded but arbitrary large degree admit the rainbow-like colouring of edges: $X^{p,q}$ defined by G. Margulis are Cayley graphs, graphs $CD(n, q)$ are parallelotopic graphs. Notice, that in the case of $CD(n, q)$ and their modifications(graphs defined in [35] and generalisetions (directed graphs $RF_n(K)$ we have the algebraic graphs such that the operator of taking the neighbour of vertex along the edge of chosen colour is a bijective polynomial map on the vertex set. So, we have cases of symbolic rainbow-like graphs. It means that the general



RC4 pass / file	40	48
7.5	1	1
55	8	8

GE1 pass / file	40	48
7.5	2.23	2.68
55	15.7	18.8

GE2 pass / file	40	48	64	128	256
7.5	0.23	0.23	0.23	0.46	0.92
55	1.58	1.58	1.58	3.16	6.32

symmetric algorithm and the public-key algorithm as above can be implemented at the level of symbolic computations. We can use such an implementation on the mode of stream-ciphers.

Let us discuss the case of families of unbounded degree but bounded girth. We can see that directed graph of generalised polygon (or its affine part) over the finite field F_{p^m} admit the rainbow-like colouring of edges. We can treat the finite field F_{p^m} as a vector space over the prime field F_p. We can keep the parameter p fixed and work with unbounded m. Formally this way gives us the Turing machine for the encryption of “potentially infinite” text.

The generalised polygon and its affine part both are algebraic graphs, but there is an essential difference between them: the affine part admit the symbolic rainbow-like colouring, but the generalised polygon itself is not.

We can use affine parts of generalised polygons for the symmetric or public-key encryption processes, but not the generalised polygons. Notice if m is growing then the task of the construction of irreducible over F_p polynomial is getting harder. So we stop our computation at some large m. So we can use graph based encryption of generalised polygons (or their affine parts) as block ciphers but not a stream ciphers.

REFERENCES

[1] Bien F. Constructions of telephone networks by group representations. *Notices Amer. Mah. Soc.*, **36** (1989), 5–22.

[2] Biggs N. Algebraic Graph Theory, (2nd ed). Cambridge, University Press, 1993.

[3] Biggs N. L. Graphs with large girth. *Ars Combin.* **25C** (1988), 73–80.

[4] Biggs N. L., A. G. Boshier. Note on the Girth of Ramanujan Graphs. *J. Combin. Theory Ser. B* **49**, *2* (1990), 190–194.

[5] Carter R. Simple groups of Lie type. London, 1984.

[6] Bollobás B. Extremal Graph Theory. Academic Press, London, 1978.

[7] Bollobás B. Random Graphs. Academic Press, London, 1985.

[8] Brower A., A. Cohen, A. Nuemaier. Distance regular graphs. Springer, Berlin, 1989.

[9] Dijkstra E. A note on two problems in connection with graphs. *Numer. Math.* **1** (1959), 269-271.

[10] Erdös' P., H. Sachs. Reguläre Graphen gegebener Taillenweite mit minimaler Krotenzahl. *Wiss. Z. Martin-Luther-Univ. Halle-Wittenberg, Math.-Naturwiss. Reihe* **12** (1963), 251–258.

[11] Futorny V., V. Ustimenko. On Small World Semiplanes with Generalised Schubert Cells. *Acta Appl. Math.* **4** (2007), already available online.

[12] Govorov M., Y. Khmelevsky, V. Ustimenko, A. Khorev. Security for GIS N-tier Architecture. 11th International Symposium on Spatial Data Handling Fisher (Ed. Peter F.) Springer-Verlag., 71, 2005.

[13] Guinand P., J. Lodge. Tanner Type Codes Arising from Large Girth Graphs. In: Proceedings of the 1997 Canadian Workshop on Information Theory (CWIT'97), Toronto, Ontario, Canada, June 3-6, 1997, 5–7.

[14] Guinand P., J. Lodge. Graph Theoretic Construction of Generalized Product Codes. In: Proceedings of the 1997 IEEE International Symposium on Information Theory (ISIT '97), Ulm, Germany, June 29 – July 4, 1997, 111.

[15] Koblitz N. A Course in Number Theory and Cryptography, Second Edition. Springer, 1994, 237 p.

[16] Koblitz N. Algebraic aspects of Cryptography. InN Algorithms and Computations in Mathematics, vol. 3, Springer, 1998.

[17] Lazebnik F., V. A. Ustimenko. New Examples of graphs without small cycles and of large size. *European J. Combin.* **14** (1993) 445–460.

[18] Lazebnik F., V. A. Ustimenko. Explicit construction of graphs with an arbitrary large girth and of large size. *Discrete Appl. Math.* **60** (1995), 275–284.

[19] Lazebnik F., V. A. Ustimenko, A. J. Woldar. A New Series of Dense Graphs of High Girth. *Bull. Amer. Math. Soc. (N.S.)* **32**, *1* (1995), 73–79.

[20] Lazebnik F., V. A. Ustimenko, A. J. Woldar. A characterization of the components of graphs $D(k, q)$. *Discrete Math.* **157** (1996), 271–283.

[21] Lazebnik F., V. A. Ustimenko, A. Woldar. Polarities and $2k$-cycle-free graphs. *Discrete Math.* **197/198** (1999), 503–513.

[22] Lubotsky A., R. Philips, P. Sarnak. Ramanujan graphs. *J. Comb. Theory* **115**, *2* (1989), 62–89.

[23] Margulis G. A. Explicit construction of graphs without short cycles and low density codes. *Combinatorica* **2** (1982), 71–78.

[24] Margulis G. Explicit group-theoretical constructions of combinatorial schemes and their application to desighn of expanders and concentrators. *Probl. Peredachi Inf.* **24**, *1* (1988), 51–60; English translation: *Probl. Inf. Transm.* **24**, *1* (1988), 39-46.

[25] Margulis G. Arithmetic groups and graphs without short cycles. 6th Intern. Symp. on Information Theory, Tashkent, abstracts, vol. **1** (1984), 123–125 (in Russian).

[26] Moore E. H. Tactical Memoranda. *Amer. J. Math.* **18**, *4* (1896), 264-303.

[27] Ore R. Graph Theory. London, 1974.

[28] Seberry J., J. Pieprzyk. Cryptography: An Introducion to Computer Security. Prentice Hall, 1989, 379 p.

[29] Tanner R. Michiel. A recursive approach to low density codes. *IEEE Trans. Inform. Theory* **27**, *5* (1984), 533–547.

[30] Touzene A., V. Ustimenko. Graph Based Private Key Crypto System. *Internat. J. Computer Research*, Nova Science Publisher **13**, *4* (2006), 12 p.

[31] Ustimenko V. A. Linear interpretation of Chevalley group flag geometries. *Ukrainian Math. J.* **43**, *7,8* (1991), 1055–1060 (in Russian).

[32] Ustimenko V. A. Coordinatisation of regular tree and its quotients. In: Voronoi's impact on modern science (Eds P. Engel and H. Syta) book 2, National Acad. of Sci, Institute of Matematics, 1998, 228 p.

[33] Ustimenko V. A. On the varieties of parabolic subgroups, their generalizations and combinatorial applications. *Acta Appl. Math.* **52** (1998), 223–238.

[34] Ustimenko V. A. Graphs with Special Arcs and Cryptography. *Acta Appl. Math.* **74**, *2* (2002), 117–153.

[35] Ustimenko V. A. CRYPTIM: Graphs as tools for symmetric encryption. In: Lecture Notes in Comput. Sci., vol. **2227**, Springer, New York, 2001.

[36] Ustimenko V. A. Maximality of affine group and hidden graph cryptsystems. *J. Algebra and Discrete Math.* **10** (October 2004), 51–65.

[37] Ustimenko V. A., D. Sharma. CRYPTIM: system to encrypt text and image data. Proceedings of International ICSC Congress on Intelligent Systems 2000, Wollongong, 2001, 11 pp.

[38] Ustimenko V., A. Touzene. CRYPTALL: system to encrypt all types of data. *Nauk. Zap., Kyiv 23* (2004), 12–15.

[39] Khmelevsky Yu., V. A. Ustimenko. Practical aspects of the Informational Systems reengineering. The South Pacific Journal of Natural Science, vol. **21**, 2003, `www.usp.ac.fj(spjns)`.

[40] Ustimenko V., A. Woldar. Extremal properties of regular and affine generalised polygons as tactical configurations. *European J. Combin.* **24** (2003), 99–111.

[41] Ustimenko V. A. Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography. *J. Math. Sci.*, Springer **140**, *3* (2007), 412–434.

[42] Ustimenko V. On the extremal graph theory for directed graphs and its cryptographical applications. In: Advances in Coding Theory and Cryptography, Series on Codin Theory and Cryptology (Eds T. Shaska, W. C. Huffman, D. Joener, V. Ustimenko) vol. **3**, 2007, 181–200.

[43] Ustimenko V. A. Algebraic small world graphs of large girth and related groupd. Proceedings of the international conferences Infinite particle systems, Complex systems theory and its application, Kazimierz Dolny, Poland, 2005–2006 (to appear).

[44] Ustimenko V. A. On the extremal binary relation graphs of high girth. Proceedings of the international conferences Infinite particle systems, Complex systems theory and its application, Kazimierz Dolny, Poland, 2005–2006 (to appear).

University of Maria Curie-Sklodowska
Poland
e-mail: `vasyl@golem.umcs.lublin.pl`

Received October 23, 2006
Final Accepted June 27, 2007