Proceedings of the Federated Conference on
Computer Science and Information Systems pp. 485–490

ISBN 978-83-60810-22-4

On the implementation of stream ciphers based on a new family of algebraic graphs

Jakub Kotorowicz
Maria Curie-Sklodowska University
Institute of Mathematics,
pl. M. Curie-Sklodowskiej 5,
20-031 Lublin, Poland.
Email: jkotor@hektor.umcs.lublin.pl

Urszula Romańczuk*
Maria Curie-Sklodowska University
Institute of Mathematics,
pl. M. Curie-Sklodowskiej 5,
20-031 Lublin, Poland.
Email: urszula_romanczuk@yahoo.pl

Vasyl Ustimenko*
Maria Curie-Sklodowska University
Institute of Mathematics,
pl. M. Curie-Sklodowskiej 5,
20-031 Lublin, Poland.
Email: vasyl@hektor.umcs.lublin.pl

I. On the families of directed graphs of large girth

THE READER can find the missing theoretical definitions on directed graphs in [8]. Let Φ be an irreflexive binary relation over the set V, i.e., $\Phi \subset V \times V$ and for each v the pair (v, v) is not an element of Φ.

We say that u is the neighbour of v and write $v \to u$ if $(v, u) \in \Phi$. We use the term *balanced binary relation graph* for the graph Γ of an irreflexive binary relation ϕ over a finite set V such that for each $v \in V$ the sets $\{x|(x, v) \in \phi\}$ and $\{x|(v, x) \in \phi\}$ have the same cardinality. It is a directed graph without loops and multiple edges. We say that a balanced graph Γ is k-regular if for each vertex $v \in \Gamma$ the cardinality of $\{x|(v, x) \in \phi\}$ is k.

Let Γ be the graph of binary relation. The *path* 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 paths $a = x_0 \to x_1 \to \cdots \to x_s = b$, $s \geq 1$ 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 $0 < i < s$, $0 < j < t$. Without loss of generality we assume that $s \geq t$.

We refer to the number $\max(s, t)$ as the rank of $O_{s,t}$. It is greater than or equal to 2, because the graph does not contain multiple edges.

Notice that the graph of antireflexive binary relation 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, $i = 0, 1, \dots, s-1$, $s \geq 2$ are distinct vertices.

We will count directed cycles as commutative diagrams.

For the investigation of commutative diagrams we introduce the *girth indicator* gi, which is the minimal value for $\max(s, t)$ for parameters s, t of a commutative diagram $O_{s,t}$, $s + t \geq 3$. The minimum is taken over all pairs of vertices (a, b) in the digraph. Notice that two vertices v and u at distance is less than gi are connected by the unique path from u to v of length is less than gi.

We assume that the *girth* $g(\Gamma)$ of a directed graph Γ with the girth indicator $d+1$ is $2d+1$ if it contains a commutative diagram $O_{d+1,d}$. If there are no such diagrams we assume that $g(\Gamma)$ is $2d + 2$.

In case of a symmetric binary relation $\mathrm{gi} = d$ implies that the girth of the graph is $2d$ or $2d - 1$. It does not contain an even cycle $2d - 2$. In the general case $\mathrm{gi} = d$ implies that $g \geq d + 1$. So in the case of the family of graphs with unbounded girth indicator, the girth is also unbounded. We also have $\mathrm{gi} \geq g/2$.

In the case of symmetric irreflexive relations the above mentioned general definition of the girth agrees with the standard definition of the girth of a simple graph, i.e., the length of its minimal cycle.

We will use the term *the family of graphs of large girth* for the family of balanced directed regular graphs Γ_i of degree k_i and order v_i such that $\mathrm{gi}(\Gamma_i) \geq c \log_{k_i}(v_i)$, where c is a constant independent of i.

It follows from the definition that $g(\Gamma_i) \geq c \log_{k_i}(v_i)$ for an appropriate constant c. So, it agrees with the well known definition for the case of simple graphs.

The diameter of the strongly connected digraph [8] is the minimal length d of the shortest directed path $a = x_0 \to x_1 \to x_2 \to \cdots \to x_d = b$ between two vertices a and b. Recall that a graph is k-regular, if each vertex of G has exactly k edges. Let F be the infinite family of k_i regular graphs G_i of order v_i and diameter d_i. We say that F is a family of small world graphs if $d_i \leq C \log_{k_i}(v_i)$, $i = 1, \dots$ for some constant C independent of i. The reader can find the definition of small world simple graphs and related explicit constructions in [4]. For the studies of small world simple graphs without small cycles see [12], [16].

II. On the K-theory of affine graphs with increasing girth indicator and its cryptographical motivations

We use the concepts of [19] here, where the reader can find additional examples of affine graphs over rings or fields.

Let K be a commutative ring. A *directed algebraic graph* ϕ over K consists of two things, such as the *vertex set* Q being a quasiprojective variety over K of nonzero dimension and the *edge set* being a quasiprojective variety ϕ in $Q \times Q$. We assume that ($x \phi y$ means $(x, y) \in \phi$).

* Research supported by a project "Human - The Best Investment".The project is co-funded from the sources of the European Union within the European Social Fund.

The graph ϕ is *balanced* if for each vertex $v \in Q$ the sets $\mathrm{Im}(v) = \{x \,|\, v\phi x\}$ and $\mathrm{Out}(v) = \{x \,|\, x\phi v\}$ are quasiprojective varieties over K of the same dimension.

The graph ϕ is *homogeneous* (or (r,s)-homogeneous) if for each vertex $v \in Q$ the sets $\mathrm{Im}(v) = \{x|v\phi x\}$ and $\mathrm{Out}(v) = \{x|x\phi v\}$ are quasiprojective varieties over F of fixed nonzero dimensions r and s, respectively.

In the case of *balanced homogeneous algebraic graphs* for which $r = s$ we will use the term r-homogeneous graph. Finally, a *regular algebraic graph* is a balanced homogeneous algebraic graph over the ring K if each pair of vertices v_1 and v_2 is a pair of isomorphic algebraic varieties.

Let $\mathrm{Reg}(K)$ be the totality of regular elements (or nonzero divisors) of K, i.e., nonzero elements $x \in K$ such that for each nonzero $y \in K$ the product xy is different from 0. We assume that $\mathrm{Reg}(K)$ contains at least 3 elements. We assume here that K is finite, thus the vertex set and the edge set are finite and we get a usual finite directed graph.

We apply the term *affine graph* for the regular algebraic graph such that its vertex set is an affine variety in the Zarisski topology.

Let G be an r-regular affine graph with vertex set $V(G)$, such that $\mathrm{Out}v$, $v \in V(G)$ is isomorphic to the variety $R(K)$. Let the variety $E(G)$ be its arrow set (a binary relation in $V(G) \times V(G)$). We use the standard term *perfect algebraic colouring of edges* for the polynomial map ρ from $E(G)$ onto the set $R(K)$ (the set of colours) if for each vertex v different output arrows $e_1 \in \mathrm{Out}(v)$ and $e_2 \in \mathrm{Out}(v)$ have distinct colours $\rho(e_1)$ and $\rho(e_2)$ and the operator $N_\alpha(v)$ of taking the neighbour u of vertex v ($v \to u$) is a polynomial map of the variety $V(G)$ into itself.

We will use the term *rainbow-like colouring* in the case when the perfect algebraic colouring is a bijection. Let $\mathrm{dirg}(G)$ be a directed girth of the graph G, i.e., the minimal length of a directed cycle in the graph. Obviously $\mathrm{gi}(G) \leq \mathrm{dirg}(G)$.

Studies of infinite families of directed affine algebraic digraphs over commutative rings K of large girth with the rainbow-like colouring is a nice but difficult mathematical problem. Good news is that such families do exist. In the next section we consider an example of such a family for each commutative ring with more than 2 regular elements.

At the end of section we consider cryptographical motivations for studies of such families.

1) Let G be a finite group and $g \in G$. The discrete logarithm problem for G is about finding a solution for the equation $g^x = b$ where x is an unknown positive integer. If the order $|g| = n$ is known we can replace G with a cyclic group C_n. So we may assume that the order of g is sufficiently large to make the computation of n unfeasible. For many finite groups the discrete logarithm problem is NP complete.

Let K be a finite commutative ring and M be an affine variety over K. Then the Cremona group $C(M)$ of all polynomial automorphisms of the variety M can be large. For example, if K is a finite prime field F_p and $M = {F_p}^n$ then $C(M)$ is a symmetric group S_{p^n}.

Let us consider the family of affine graphs $G_i(K)$, $i = 1, 2, \ldots$ with the rainbow-like algebraic colouring of edges such that $V(G_i(K)) = V_i(K)$, where K is a commutative ring, and the colour sets are algebraic varieties $R_i(K)$. Let us choose a constant k. The operator $N_\alpha(v)$ of taking the neighbour of a vertex v corresponding to the output arrow of colour α are elements of $C_i = C(V_i(K))$. We can choose a relatively small number k to generate $h = h_i = N_{\alpha_1} N_{\alpha_2} \ldots N_{\alpha_k}$ in each group C_i, $i = 1, 2, \ldots$

Let us assume that the family of graphs $G_i(K)$ is the family of graphs of increasing girth. It means that the girth indicator $\mathrm{gi}_i = \mathrm{gi}(G_i(K))$ and the parameter $\mathrm{dirg}_i = \mathrm{dirg}(G_i(K))$ are growing with the growth of i. Notice that $|h_i|$ is bounded below by dirg_i/k. So there is a j such that for $i \geq j$ the computation of $|h_i|$ is impossible. In fact, the fastest grow of girth indicator will be in the case of a family of large girth. Finally we can take the base $g = T^{-1} h_j T$ where T is a chosen element of C_j to hide the graph up to conjugation. We may use some package of symbolic computations to express the polynomial map g via the list of polynomials in many unknowns. For example, if $V_j(K)$ is a free module K^n then we can write g in a public mode fashion

$x_1 \to g_1(x_1, x_2, \ldots, x_n)$, $x_2 \to g_2(x_1, x_2, \ldots, x_n)$, $\ldots$, $x_n \to g_n(x_1, x_2, \ldots, x_n)$.

The symbolic map g can be used for the Diffie - Hellman *key exchange protocol* (see [4] for the details). Let Alice and Bob be correspondents. Alice computes the symbolic map g and send it to Bob via an open channel. So the variety and the map are known for the adversary (Cezar).

Let Alice and Bob choose natural numbers n_A and n_B, respectively.

Bob computes g^{n_B} and sends it to Alice, who computes $(g^{n_B})^{n_A}$, while Alice computes g^{n_A} and sends it to Bob, who is getting $(g^{n_A})^{n_B}$. The common information is $g^{n_A n_B}$ given in "public mode fashion".

Bob can be just a public user (no information on the way in which the map g was created) , so he and Cezar make computations much slower than Alice who has the decomposition $g = T^{-1} N_{\alpha_1} N_{\alpha_2} \ldots N_{\alpha_k} T$.

We may modify slightly the Diffie - Hellman protocol using the action of the group on the variety. Alice chooses a rather short password $\alpha_1, \alpha_2, \ldots, \alpha_k$, computes the public rules for the encryption map g and sends them to Bob via an open channel together with some vertex $v \in V_j(K)$. Then Alice and Bob choose natural numbers n_A and n_B, respectively.

Bob computes $v_B = g^{n_B}(v)$ and sends it openly to Alice, who computes $(g^{n_A})(v_B)$, while Alice computes $v_A = g^{n_A}(v)$ and sends it to Bob, who receives $(g^{n_B})(v_A)$.

The common information is the vertex $g^{n_A \times n_B}(v)$.

In both cases Cezar has to solve one of the equations $E^{n_B}(u_A) = z$ or $E^{n_A}(u_B) = w$ for unknowns n_B or n_A, where z and w are known points of the variety.

2) We can construct the *public key* map in the following manner:

The key holder (Alice) chooses the variety $V_j(K)$ and the sequence $\alpha_1, \alpha_2, \ldots, \alpha_t$ of length $t = t(j)$ to determine the

encryption map g as above. Let $\dim(V_j(K)) = n = n(j)$ and each element of the variety be determined by independent parameters $x_1, x_2, \ldots, x_n$. Alice presents the map in the form of public rules, such as

$x_1 \to f_1(x_1, x_2, \ldots, x_n)$, $x_2 \to f_2(x_1, x_2, \ldots, x_n)$, $\ldots$, $x_n \to f_n(x_1, x_2, \ldots, x_n)$.

We can assume (at least theoretically) that the public rule depending on parameter j is applicable to the encryption of a potentially infinite text (the parameter t is a linear function on j now).

For the computation she may use the Gröbner base technique or alternative methods, special packages for the symbolic computation (popular "Mathematica" or "Maple", package "Galois" for "Java" as well special fast symbolic software). So Alice can use the decomposition of the encryption map into T^{-1}, maps of kind N_α and T to encrypt fast. For the decryption she can use the inverse graph $G_j(K)^{-1}$ for which $VG_j(K)^{-1} = VG_j(K)$ and vertices w_1 and w_2 are connected by an arrow if and only if w_2 and w_1 are connected by an arrow in $G_j(K)$. Let us assume that colours of $w_1 \to w_2$ in $G_j(K)^{-1}$ and $w_2 \to w_1$ in $G_j(K)$ are of the same colour. Let $N'_\alpha(x)$ be the operator taking the neighbour of vertex x in $G_j(K)^{-1}$ of colour α. Then Alice can decrypt applying sequentially $T, N'_{\alpha_t}, N'_{\alpha_{t-1}}, \ldots, N'_{\alpha_1}$ and T^{-1} to the ciphertext. So the decryption and the encryption for Alice take the same time. She can use a numerical program to implement her symmetric algorithm.

Bob can encrypt with the public rule but for a decryption he needs to invert the map. Let us consider the case $t_j = kl$, where k is a small number and the sequence $\alpha_1, \alpha_2, \ldots, \alpha_{t_j}$ has the period k, and the transformation $h = T^{-1}N_{\alpha_1}N_{\alpha_2}\ldots N_{\alpha_k}T$ is known for Bob in the form of public key mode. In such a case a problem to find the inverse for g is equivalent to a discrete logarithm problem with the base h in the related Cremona group of all polynomial bijective transformations.

Of course for further cryptanalysis we need to study the information on possible divisors of the order of the base of the related discrete logarithm problem, alternative methods to break the encryption. In the next section the family of digraphs $RE_n(K)$ will be described.

3) We may study the security of the private key algorithm used by Alice in the algorithm of the previous paragraph but with a parameter t bounded by the girth indicator of graph $G_j(K)$. In this case different keys produce distinct ciphertexts from the chosen plaintext. We prove that if the adversary has no access to plaintexts then he can break the encryption via the brute-force search via all keys from the key space. The encryption map has no fixed points.

III. On the Family of Affine Digraph of Increasing Girth over Commutative Rings

E. Moore used the term *tactical configuration* of order (s, t) for biregular bipartite simple graphs with bidegrees $s+1$ and $r+1$. It corresponds to the incidence structure with the point set P, the line set L and the 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 tactical configuration with partition sets P (point set) and L (line set) and an incidence relation I. We define the following irreflexive binary relation ϕ on the set F:

Let (P, L, I) be the incidence structure corresponding to regular tactical configuration of order t.

Let $F_1 = \{(l, p) | l \in L, p \in P, lIp\}$ and $F_2 = \{[l, p] | l \in L, p \in P, lIp\}$ be two copies of the totality of flags for (P, L, I). Brackets and parentheses allow us to distinguish elements from F_1 and F_2. Let $DF(I)$ be the directed graph (double directed flag graph) on the disjoint union of F_1 with F_2 defined by the following rules:

$(l_1, p_1) \to [l_2, p_2]$ if and only if $p_1 = p_2$ and $l_1 \neq l_2$,

$[l_2, p_2] \to (l_1, p_1)$ if and only if $l_1 = l_2$ and $p_1 \neq p_2$.

Below we consider the family of graphs $A(k, K)$, where $k > 5$ is a positive integer and K is a commutative ring. Such graphs are disconnected and their connected components were investigated in [17] (for the case when K is a finite field F_q see [7]).

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 [20] for the case of a general commutative ring K:

$$\begin{aligned} (p) &= (p_{0,1}, p_{1,1}, p_{1,2}, p_{2,2}, p_{2,3}, \ldots, p_{i,i}, p_{i,i+1}, \ldots), \\ [l] &= [l_{1,0}, l_{1,1}, l_{1,2}, l_{2,2}, l_{2,3}, \ldots, l_{i,i}, l_{i,i+1}, \ldots]. \end{aligned}$$

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

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

$$\begin{aligned} l_{i,i} - p_{i,i} &= l_{1,0}p_{i-1,i} \\ l_{i,i+1} - p_{i,i+1} &= l_{i,i}p_{0,1} \end{aligned}$$

This incidence structure (P, L, I) we denote as $A(K)$. We identify it with the bipartite *incidence graph* of (P, L, I), which has the vertex set $P \cup L$ and the 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 $A(k, K)$.

For each positive integer $k \geq 2$ we consider the *standard* graph homomorphism ϕ_k of (P_k, L_k, I_k) onto $(P_{k-1}, L_{k-1}, I_{k-1})$ defined on L_k by simply projection of each vector from P_k and L_k onto its $k-1$ initial coordinates with respect to the above order.

Let $DA_n(K)$ ($DA(K)$) be the double directed graph of the bipartite graph $A(n,K)$ ($A(K)$, respectively). Remember, that we have the arc e of kind $(l^1, p^1) \to [l^2, p^2]$ if and only if $p^1 = p^2$ and $l^1 \neq l^2$. Let us assume that the colour $\rho(e)$ of the arc e is $l^1_{1,0} - l^2_{1,0}$.

Recall, that we have the arc e' of kind $[l^2, p^2] \to (l^1, p^1)$ if and only if $l^1 = l^2$ and $p^1 \neq p^2$. Let us assume that the colour $\rho(e')$ of arc e' is $p^1_{1,0} - p^2_{1,0}$. It is easy to see that ρ is a perfect algebraic colouring.

If K is finite, then the cardinality of the colour set is $(|K| - 1)$. Let $\mathrm{Reg}K$ be the totality of regular elements, i.e., not zero divisors. Let us delete all arrows with colour, which are zero divisors. We will obtain a new graph $RA_n(K)$ ($RA(K)$) with the induced colouring into colours from the alphabet $\mathrm{Reg}(K)$. The vertex set for the graph $DA_n(K)$ consists of two copies F_1 and F_2 of the edge set for $A(n,K)$.

If K is finite, then the cardinality of the colour set is $(|K| - 1)$. Let $\mathrm{Reg}K$ be the totality of regular elements, i.e., non-zero divisors. Let us delete all arrows with colour, which are zero divisors. We can show that a new infinite affine graph $A(K)$ does not contain cycles (see [9]). This means that the directed graph $RA(K)$ does not contain commutative diagrams and the digraphs $RA_n(K)$ form a family of digraphs with increasing girth indicator. In fact computer simulations support the following assertion.

CONJECTURE: Graphs $RA_n(K)$ form a family of digraphs of large girth.

IV. On the implementation of the stream cipher based on $RA_t(K)$

The set of vertices of the graph $RA_n(K)$ is a union of two copies of a free module K^{n+1}. So the Cremona group of the variety is the direct product of $C(K^{n+1})$ with itself, expanded by polarity π. In the simplest case of a finite field F_p, where p is a prime number, $C(F_p)$ is a symmetric group $S_{p^{n+1}}$. The Cremona group $C(K^{n+1})$ contains the group of all affine invertible transformations, i.e., transformation of kind $\mathrm{x} \to \mathrm{x}A + \mathrm{b}$, where $\mathrm{x} = (x_1, x_2, \ldots, x_{n+1}) \in C(K^{n+1})$, $\mathrm{b} = (b_1, b_2, \ldots, b_{n+1})$ is a chosen vector from $C(K^{n+1})$ and A is a matrix of a linear invertible transformation of K^{n+1}.

The graph $RA_n(K)$ is a bipartite directed graph. We assume that the plaintext K^{n+1} is a point $(p_1, p_2, \ldots, p_{n+1})$. We choose two affine transformations T_1 and T_2 as linear transformation of kind $p_1 \to p_1 + a_1p_2 + a_2p_3 + \cdots + a_np_{n+1}$. We will follow a general scheme, so Alice and Bob compute chosen T_1 and T_2, and choose a string $(\beta_1, \beta_2, \ldots, \beta_l)$ of colours for $RE_n(K)$, such that $\beta_i \neq -\beta_{i+1}$ for $i = 1, 2, \ldots, l-1$. They will use $N_l = N_{\beta_1} \times N_{\beta_2} \cdots \times N_{\beta_l}$. Recall that N_α, $\alpha \in \mathrm{Reg}(K)$ is the operator of taking the neighbour of the vertex v alongside the arrow with the colouur α in the graph $RA_n(K)$.

Alice and Bob keep chosen parameters T_1,$(\beta_1, \beta_2, \ldots, \beta_l)$ and T_2 secret and use the encryption map g which is the composition of T_1, N_l and T_2.

In the case of $RA_n(K)$ the degree of transformation N_l is 3, independent of the choice of length l like in the case of graphs $D(n,K)$ [9]. We can prove that for arbitrary key the encryption map is a cubical polynomial map of the free module K^{n+1} onto itself.

In our computer implementations we used T_1 and T_2 of kind $p_1 \to p_1 + a_1p_2 + a_2p_3 + \cdots + a_np_{n+1}$, where all a_i are not zero divisors.

V. On the comparison of private keys based on $A(n,K)$ and $D(n,K)$

In the paper [5] we have implemented the stream cipher based on graphs $D(n,K)$ with vertex set the union of two copies of the free module K^n. The time of execution of the encryption map and its mixing properties and comparison with other private keys (DES and RC4 are considered in [5] for cases of rings Z_2^8, Z_2^{16} and Z_2^{32}. The reader can find speedy evaluation for cases of rings Z_2^8, Z_2^{16} and Z_2^{32} in [16]. Recently, private keys based on $D(n, F_q)$, $q = 2^8$, $q = 2^{16}$ and $q = 2^{32}$ were implemented (see [13], where time evaluation is presented).

The mixing properties of $D(n, Z_2^m)$, $m = 8, 16, 32$ based encryption in combination with special affine transformations were investigated in [20]. If we change one character of the string $\alpha_1, \alpha_2, \ldots, \alpha_s$ (the graphical part of the key related to the pass of the graph) then at least 97 percent of characters of the ciphertext will be changed . If we change one character of the plaintext then again at least 97 percent of the characters of the ciphertext will be changed.

We present at the conference similar results of statistics for mixing properties of an $A(m, Z_q)$ based stream cipher.

We can see that graphs the $A(n,K)$ and $D(n,K)$ are given by equations which use $n-1$ additions (or subtractions) and multiplications. So algorithms based on these graphs or corresponding digraphs have the same speed evaluations.

Graphs $A(n, Z_m)$, $m > 2$ are connected but $D(n,K)$ are not. It means that if we fixed affine maps, then for each pair of vectors v_1 an v_2 from the plainspace there is a string $\alpha_1, \alpha_2, \ldots, \alpha_s$ such the corresponding $A(n, Z_m)$ based encryption map converts the plaintext v_1 into the ciphertext v_2. The reader can find some theoretical results on $A(n,K)$ in [17].

A. Evaluation of the order of encryption map

We assume that the product of our affine transformations is the identity. So the order of the encryption map is the same with $N = N_{\alpha_1} N_{\alpha_2} \ldots N_{\alpha_s}$. We assume that s is even and our string is obtained by repetition of the word α_1, α_2, where $\alpha_1 + \alpha_2 \in \mathrm{Reg}(K)$. So the security of our encryption is related to the discrete logarithm problem with base $b = N_{\alpha_1} N_{\alpha_2}$. It turns out that in cases of $K = Z_n$, $n > 2$ the order of b does not depend on the choice of α_1 and α_2.

B. Case of primes

We have run computer tests, to measure the length of the cycles generated by powers of b for graphs $A(n, K)$ with different n, and different K (cycles of permutation b acting on K^n). Table I shows these results for the first few prime numbers p ($K = Z_p$). Each test was repeated at least 20 times, every time with a random start point, and random (α_1, α_2) parameter.

TABLE I
CYCLE LENGHT FOR $K = Z_q$, WHERE q IS PRIME

$p \setminus n$	4	10	30	50	100	200	400	600	1000
3	9	27	81	81	243	243	729	729	2187
5	5	25	125	125	125	625	625	625	3125
7	7	49	49	343	343	343	2041	2041	2041
11	11	11	121	123	121	1331	1331	1331	1331

It is easy to see that the cycle length is always a power of the prime number p. Another property is that cycle length does not depend on starting point, nor parameters (α_1, α_2). This property does not hold for $p = 2$. In that case the cycle length is always a power of 2, but for the same n we have different results depending on start point x, and (α_1, α_2).

C. Case of composite numbers

TABLE II
CYCLE LENGTH FOR SOME COMPOSITE NUMBERS q

$q \setminus n$	4	10	30	50	100	200	400
4	16	32	64	128	256	512	1024
6	72	432	2592	5184	31104	62208	
8	32	64	128	256	512	1024	2048
9	27	81	243	243	729	729	2187
15	45	675	10125	10125	30375	151875	455625

TABLE III
CYCLE LENGTH FOR $q = 15$, CASE OF THE $A(n, Z_q)$

n_{MIN}	n_{MAX}	cycle length
4	4	45
5	8	225
9	24	675
25	26	3375
27	80	10125
81	120	30375
140	240	151875
260	620	455625
640	720	2278125
760		6834375

The comparison of cycles in cases $A(n, K)$ and $D(n, K)$ encryption demonstrates big advantage of $A(n, K)$. The typical example is below.

TABLE IV
CYCLE LENGTH FOR $q = 15$, CASE OF $D(n, Z_{15})$ ENCRYPTION

n_{MIN}	n_{MAX}	cycle length
4	7	45
8	17	225
18	53	675
54	65	3375
150	249	10125
250	299	30375
300	649	151875
650	1000	455625

VI. CONCLUSION, ON THE IMPORTANCE OF NUMERICAL ALGORITHM FOR EVALUATION OF SYMBOLIC CRYPTOGRAPHICAL TOOLS

As we mentioned above the private key algorithm based on graphs $A(n, K)$ turns out to be good stream cipher. It compares well with $D(n, K)$ based encryption.

On another hand this algorithm is a private decryption tool for corresponding symbolic public key algorithms. Encryption map g with arbitrarily chosen password is a cubic polynomial map. All powers of g are cubic maps, so cyclic group generated by g can be used for the synbolic key exchange protocol. Studies of the properties of the stream cipher are crucial for the evaluation of the main parameters of symbolic algorithms because the speed of symbolic computations is much slower in comparison with our numerical algorithm.

Usually the order of nonlinear polynomial map g^k from Cremona group (composition of g with itself, corresponding to permutation π^k) is growing with the growth of k. The computation of the order t of "pseudorandom" g is a difficult task. Really, if t is known then the inverse map for g is g^{t-1}, but the best known algorithm of finding g^{-1} has complexity $d^{O(n)}$, where d is the degree of g. The efficient general algorithm of finding g^{-1} is known only in the case when degree of g is one, i. e. g is affine map $\mathrm{x}A + \mathrm{b}$, where x and b are row vectors from V and A is nonsingular square matrix. So there is a serious complexity gap between linearity and nonlinearity.

The discrete logarithm problem (dlp) for the cyclic group generated by "pseudorandom" polynomial map g, i. e. problem of finding solution for equation $g^x = b$ looks very hard. If x is known, then $g^{t-x} = b^{-1}$, but the computation of b^{-1} takes $d^{O(n)}$. So in the case of "pseudorandom" polynomial base g we can use the term *hidden symbolic* discrete logarithm problem, word *hidden* is used because the order t of cyclic group is unknown, *symbolic* is used because generation of polynomial maps g and b can be done via tools of symbolic computations (popular "Maple" or "Mathematica" operating on polyomial maps or special fast programs of Computer Algebra). Certainly the choice of the nonlinear base g for the dlp for $C(K^n)$ is an important heuristic problem. Obviously one needs to find g of very large order. If the degree of g^x is growing linearly with the growth of g: deg(g(x))= $ax + b$ then x can be obtained from the linear equation $ax + d = \deg(b(x))$. This fact is a motivation of the following concept.

The sequence of subgroups G_l of $C(K^l)$, $l \to \infty$ is a *family of stable groups* if degree of each g. $g \in G_l$ is bounded by constant c independent on l. The construction of large stable subgroups G_l with $c \geq 2$ of Cremona group is an interesting mathematical task.

There is an easy way to construct stable subgroups via conjugation of $AGL_l(K)$ (subgroup of all automorphisms of K^n of degree 1) with the nonlinear polynomial maps $f_l \in C(K^l)$. Let us refer to members of such families as pseudolinear groups. Degrees of f_l and ${f_l}^{-1}$ are at least 2. So in case of the use "pseudorandom" polynomials, f_i such that $\max(f_l, {f_l}^{-1})$ is bounded by constant, we obtain a stable family with $c \geq 4$. Let τ be a Singer cycle from $AGL_l(F_q)$ of order $q^n - 1$ ($K = F_q$), f_l and ${f_l}^{-1}$ are nonlinear maps. Then $g = {f_l}^{-1}\tau f_l$ looks as appropriate base for the hidden symbolic discrete logarithm problem. Certainly one may use other linear transformations of large order instead of Singer cycle.

So the case of families of stable degree with $c \in \{2, 3\}$ is the most interesting one.

The new family of large stable subgroups of $C(K^l)$ over general commutative ring K containing at least 3 regular elements (non zero divisors). with $c = 3$ is presented in our paper.

New transformations g_n of K^n also form stable subgroups with $c = 3$. Computer simulations demonstrate the faster growth of order in comparison with previously known family.

Remark. The map of kind $h = f_1 g_n f_2$, where $f_1, f_2 \in C(K^n)$ of bounded degree can be used as a public key algorithm with public rules $h_1 = h_1(x_1, x_2, \ldots, x_n)$, $h_2 = h_2(x_1, x_2, \ldots, x_n)$, $\ldots$, $h_n = h_1(x_1, x_2, \ldots, x_n)$.

Computer simulations show that even in the case of distinct affine transformations $f_1, {f_2}^{-1}$ the powers δ^k of cubic map $\delta = f_1 g(n) f_2$ have rather sophisticated degrees $t(n, k)$ which are growing with the growth of parameters n and k. In practice the computation of order for δ (or its inverse) are much harder in comparison with studies of order for conjugates of g_n. Notice that in the case of field F_p invertible affine transformations and $g(n)$ generate entire group S_{p^n} (Cremona group of the vector space ${F_p}^n$).

So we do hope that our method of generation of public key maps produces good approximation of random maps of degree 3 of large order (see [22] for the results of symbolic computations).

REFERENCES

[1] F. Bien, *Constructions of telephone networks by group representations*, Notices Amer. Math. Soc. **3** (1989), 5–22.

[2] B. Bollobás, *Extremal graph theory*, Academic Press, London, 1978.

[3] M. Klisowski, V. A. Ustimenko *On the public keys based on the extremal graphs and digraphs*, International Multiconference on Computer Science and Informational Technology, October 2010, Wisla, Poland, CANA Proceedings, 12 pp.

[4] N. Koblitz, *Algebraic aspects of cryptography*, Algorithms and Computation in Mathematics, vol. 3, Springer, 1998.

[5] S. Kotorowicz and V. Ustimenko, *On the implementation of cryptoalgorithms based on algebraic graphs over some commutative rings*, Condens. Matter Phys. **11** (2008), no. 2(54), 347–360.

[6] S. Kotorowicz, V. Ustimenko, *On the comparison of mixing properties of stream ciphers based on graphs $D(n, q)$ and $A(n, q)$* (to appear)

[7] F. Lazebnik, V. A. Ustimenko, and A. J. Woldar, *A new series of dense graphs of high girth*, Bull. Amer. Math. Soc. (N.S.) **32** (1995), no. 1, 73–79.

[8] R. Ore, *Graph theory*, Wiley, London, 1971.

[9] U. Romańczuk, V. Ustymenko *On some cryptographical applications of new family of expanding graphs*, Presentation in Conference CECC'2011, Debrecen, Hungary

[10] T. Shaska and V. Ustimenko, *On some applications of graph theory to cryptography and turbocoding*, Albanian J. Math. **2** (2008), no. 3, 249–255, Proceedings of the NATO Advanced Studies Institute: "New challenges in digital communications".

[11] T. Shaska, V Ustimenko, *On the homogeneous algebraic graphs of large girth and their applications*, Linear Algebra Appl. **430** (2009), no. 7, 1826–1837, Special Issue in Honor of Thomas J. Laffey.

[12] M. Simonovits, *Extremal graph theory*, Selected Topics in Graph Theory 2 (L. W. Beineke and R. J. Wilson, eds.), no. 2, Academic Press, London, 1983, pp. 161–200.

[13] A. Touzene, V. Ustimenko, Marwa AlRaissi, Imene Boudeliouua,*Performance of Algebraic Graphs Based Stream-Ciphers Using Large Finite Fields* (to appear)

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

[15] V. Ustimenko, *On the extremal graph theory for directed graphs and its cryptographical applications*, Advances in Coding Theory and Cryptography (T. Shaska, D. W. C. Huffman, Joener, and V. Ustimenko, eds.), Series on Coding Theory and Cryptology, vol. 3, World Scientific, 2007, pp. 181–199.

[16] V. Ustimenko, *On the extremal regular directed graphs without commutative diagrams and their applications in coding theory and cryptography*, Albanian J. Math. **1** (2007), no. 4, Special issue on algebra and computational algebraic geometry.

[17] V. Ustimenko, *Algebraic groups and small world graphs of high girth*, Albanian J. Math. **3** (2009), no. 1, 25–33.

[18] V. Ustimenko, *On the cryptographical properties of extremal algebraic graphs*, Algebraic Aspects of Digital Communications (Tanush Shaska and Engjell Hasimaj, eds.), NATO Science for Peace and Security Series - D: Information and Communication Security, vol. 24, IOS Press, July 2009, pp. 256–281.

[19] V. A. Ustimenko, *Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography*, Journal of Mathematical Sciences, Springer, vol.140, N3 (2007) pp. 412-434.

[20] V. Ustimenko and J. Kotorowicz, *On the properties of stream ciphers based on extremal directed graphs*, Cryptography Research Perspective (Roland E. Chen, ed.), Nova Science Publishers, April 2009, pp. 125–141.

[21] A. Wróblewska, *On some applications of graph based public key*, Albanian J. Math. **2** (2008), no. 3, 229–234, Proceedings of the NATO Advanced Studies Institute: "New challenges in digital communications".

[22] M. Klisowski, U. Romanczuk, V, Ustimenko, *On the implementation of cubic public keys based on new family of algebraic graphs*, Annales UMCS Informatica Lublin - Polonia, Proceedings of the conference "Cryptography and Security Systems 2011, Nalenczow, September, 2011 (to appear).