UDC 519.1,514.128

V. A. Ustimenko

On walks of variable length in the Schubert incidence systems and multivariate flow ciphers

(Presented by Corresponding Member of the NAS of Ukraine O. M. Trofimchuk)

The flow cipher algorithm based on walks at the flag variety of a Schubert system over the finite commutative ring is proposed. The restriction of the incidence relation of the geometry of a finite simple Lie group of the normal type on the union of large Schubert cells of the maximal dimension is an example of the Schubert system. More general examples are connected with Kac–Moody groups. We introduce some applications of such ciphers based on periodic walks for the construction of multivariate private keys, security of which is connected with the discrete logarithm problem for cyclic subgroups of polynomial transformations of increasing order.

Schubert systems, definitions, and examples. 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 antireflexive binary relation on $V(G)$, i. e. $E(G)$ is a subset of $V(G) \times V(G)$, and write $v\, G\, u$ for the adjacent vertices u and v (or neighbors).

The *girth* of a graph G, denoted by $g = g(G)$, is the length of the shortest cycle in G.

We use a term *incidence structure* for a triple consisting of the set Γ, its partition $\Gamma = \Gamma_1 \bigcup \Gamma_2 \bigcup \cdots \bigcup \Gamma_n$, and a symmetric antireflexive binary relation I (incidence) on the set Γ such that xIy implies $\in \Gamma_i$, $y \in \Gamma_j$, and $i \neq j$.

We refer to the number n as the rank of an *incidence structure*. In the case $n = 2$, the triple is called an incidence structure, and $P = \Gamma_1$ and $L = \Gamma_2$ are called the set of points and the set of lines, respectively.

Let K be a finite commutative ring. Linguistic is called the incidence structure with the point set $\Gamma_1 = K^{s+m}$ and the line set $\Gamma_2 = K^{r+m}$ such that point (x) $= (x_1, x_2, \ldots, x_s, x_{s+1}, \ldots, x_{s+m})$ is incident to the line [y] $= [y_1, y_2, \ldots, y_r, y_{r+1}, y_{r+2}, \ldots, y_{m+r}]$ if and only if the relations

$$a_1 x_{s+1} + b_1 y_{r+1} = f_1(x_1, x_2, \ldots, x_s, y_1, y_2, \ldots, y_r),$$

$$a_2 x_{s+2} + b_2 y_{r+2} = f_2(x_1, x_2, \ldots, x_{s+1}, y_1, y_2, \ldots, y_{r+1}),$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$a_m x_{s+m} + b_m y_{r+m} = f1(x_1, x_2, \ldots, x_{s+m-1}, y_1, y_2, \ldots, y_{r+m-1})$$

hold, where a_j and b_j, $j = 1, 2, \ldots, m$, are not zero divisors, and f_j are multivariate polynomials with coefficients from K. Brackets and parentheses allow us to distinguish point from line (see [2]). The color $r(p)$ ($r([l])$) of point (p) (line $[l]$) is defined as the projection of an element p from the free module on its initial s (respectively, r) coordinates. As follows from the definition of linguistic incidence structure, there exists the unique neighbor with a chosen color for each vertex of the incidence graph.

Recall that a flag F of the incidence system $\Gamma = \Gamma_1 \bigcup \Gamma_2 \bigcup \cdots \bigcup \Gamma_m$ is the clique of a simple graph I. This means that x, y $\in F$ implies xIy.

Let $\Omega = \{1, 2, \ldots, t\}$ be a finite set. For each subset M in Ω and each commutative ring K, we consider the totality $K^M = \{f\colon M \to K\}$ of partial functions from Ω into K with support $\mathrm{supp}(f) = M$. It is convenient for us to write element $f \in K^M$ as a pair (M, f). Let M_1 and M_2 be nonempty sets of Ω. We denote, by $L(M_1, M_2, K)$, the linguistic graph with a point set K^{M_1} and a line set K^{M2} such that the incidence of the point (M_1, f_1) and the line (M_2, f_2) will be given by the following conditions:

$$m_i f_1(s_i) + l_i f_2(s_i)) = F_i(f_1(r_1), f_1(r_2), \ldots, f_1(r_{d_1}), f_2(p_1), f_2(p_2), \ldots, f_2(p_{d_2}), f_1(s_1),$$
$$f_1(s_2), \ldots, f_1(s_{i-1}), f_2(s_1), f_2(s_2), \ldots, f_2(s_{i-1})), \qquad i = 1, 2, \ldots, t.$$

Here, elements of $M_1 - M_1 \bigcap M_2$ and $M_2 - M_1 \bigcap M_2$ are defined by lists $\{r_1, r_2, \ldots, r_{d_1}\}$ and $\{p_1, p_2, \ldots, p_{d_2}\}$, and elements of $M_1 \bigcap M_2$ are listed as s_1, $s_2, \ldots, s_t$. The color $r(v)$ of the vertex $v = (M_i, f_i)$, $i = 1, 2$, in the graph $L(M_1, M_2, K)$ is defined as the restriction of f_i onto $M_i - M_1 \bigcap M_2$. A linguistic incidence system $L(M_t, \Omega, K)$, $t \in J$, is defined for the family of subsets M_t, $t \in \Omega$, of Ω and the commutative ring K as a disjoint union of K^{M_t}, $t \in J$, together with the incidence relation I such that its restriction I_{ij} on $K^{M_i} \bigcup K^{M_j}$, where $i, j \in J$ are defined by a linguistic graph $L(M_1, M_2, K)$. We call the Schubert system a linguistic incidence structure $L(M_t, \Omega, K)$, $t \in J$, with a nonempty set of maximal flags of rank $|J|$ such that, for each order $i_1, i_2, \ldots, i_s$ on J, each maximal flag is uniquely defined by its representative of $K^{M_{i_1}}$, its neighbor of kind (M_{i_2}, f_{i_2}) is uniquely defined by $f_{i_2}|M_{i_2} - M_{i_1}$, a flag element of kind (M_{i_3}, f_{i_3}) is uniquely defined by the projection $f_{i_3}|Mi_3 - M_{i_1} \bigcap M_{i_2}$, and a representative of $K^{M_{i_s}}$ is uniquely defined by the projection of f_{i_s} onto $K_{i_s} - M_{i_1} \bigcap M_{i_2} \bigcap \cdots \bigcap M_{i_{s-1}}$.

As follows from the definition of Schubert systems, the sets $D_i = M_i - M_1 \bigcap M_2 \cdots M_{i-1} \bigcap \bigcap M_{i+1} \bigcap M_{i+2} \cdots M_s$ are nonempty. For each flag of kind (M_1, f_1), $(M_2, f_2), \ldots, (M_{i-1}, f_{i-1})$, (M_{i+1}, f_{i+1}), $(M_{i+2}, f_{i+2}) \ldots, (M_s, f_s)$, its completion to the maximal flag by adding (M_i, f_i) is uniquely defined by the projection of f_i onto D_i. A natural example of the Schubert system can be obtained via the restriction of the incidence relation of the geometry $\Gamma(G) = \Gamma_1 \bigcup \Gamma_2 \bigcup \cdots \bigcup \Gamma_n$ of a simple Lie group G of the normal type onto a disjoint union of large Schubert cells of maximal degree in each Γ_i, $i = 1, 2, \ldots, n$.

More general examples correspond to Kac–Moody groups. Let L be a Kac–Moody algebra defined by the Cartan matrix A over the field of complex numbers C. The algebra L can be written in the form $L^- + L_0 + L^+$, where L_0 is a Cartan subalgebra, and L^+ is a direct sum of root subspaces corresponding to positive real and imaginary roots r in the chosen Chevalley basis. Let $a_1, a_2, \ldots, a_n$ be the list of fundamental roots, then dual elements a_1^*, $a_2^*, \ldots, a_n^*$ form a basis in L_0. Let us denote, by L_Z, a Lie groupoid of all vectors in L with integer coordinates in the chosen basis. Let K be a commutative ring. Then the tensor product of L_Z and K is a Lie groupoid L_K over K. Let Γ_i be the totality of elements in K of kind $a_i{}^* + x$, where x is an element of the direct sum S_i of root subspaces L_r, where r is a positive root, and $a_i^*(r)$ is different from zero. We define an incidence system $S\Gamma(A, K)$, which is a disjoint union of Γ_i such that x from Γ_i and y from Γ_j are incident if and only if $[\mathrm{x}, \mathrm{y}] = 0$. As was shown in [3] (see also [4]) in the case of a finite-dimensional algebra L over the field K of characteristic zero (or "sufficiently large" characteristic), the incidence system $S\Gamma(A, K)$ is isomorphic to the Schubert system of the geometry of a simple group G, which is an adjoint group for the Lie algebra L. If $\det(A) = 0$, then the incidence system $S\Gamma(A, K)$ is a variety of infinite dimension (see [4]). In

the case of $K = F_q$, $S\Gamma(A, K)$ can be approximated by a finite Schubert system obtained by the change of the space L by a direct sum of root spaces L_r, where the positive root r satisfies the condition $r < r_0$ for certain r_0 and the chosen lexicographical order on roots (see [4, 5]). In a similar way, the Schubert system of the geometry of a simple Lie group of the twisted type can be embedded into the corresponding Lie algebra [6].

Let Γ, I be an incidence graph in the Schubert incidence system over a commutative ring K. Geometry elements forming two flags $F_1 = \{(M_1, f_1), (M_2, f_2), \ldots, (M_s, f_s)\}$ and $F_2 = \{(M_1^+, f_1^+), (M_2^+, f_2^+, \ldots, (M_s^+, f_s^+)\}$ may be located at the same connected component of I, or the representatives of F_1 and F_2 are from distinct connected components. Assume that the system of equations $G_1(\mathrm{x}) = a_1$, $G_2(\mathrm{x}) = a_2, \ldots, G_k(\mathrm{x}) = a_k$, where $a_i \in K$ are some constants, defines the connectivity invariants. For elements $\mathrm{x}, \mathrm{y} \in \Gamma_1$ from the same connectivity component, the relation $G_i(\mathrm{x}) = G_i(\mathrm{y})$, $i = 1, 2, \ldots, k$, holds.

The existence of i such that $G_i(\mathrm{x}) = G_i(\mathrm{y})$ implies that x and y are vertices from different connected components of graph I.

On the flag varieties and walks on them. Finite geometries and the metric spaces connected with them are traditionally used in coding theory. Some cryptographical applications of finite geometries were proposed in [7]. The idea to use walks in a Schubert system for the generation of nonlinear bijective maps of vector spaces was proposed in [8]. The present article is devoted to generalizations of cryptographical algorithms based on a Schubert automaton proposed in [9].

Let us consider the set ΓF of maximal flags of a Schubert system. We define the spectrum $\mathrm{spec}(F)$ of a flag $F = \{(M_1, f_1), (M_2, f_2), \ldots, (M_s, f_s)\}$ as a sequence of colors $t_i = f_i|M_i - -(M_1 \bigcup M_2 \bigcup \cdots \bigcup M_{i-1} \bigcup M_{i+1} \bigcup \cdots \bigcup M_s)$ of its elements (M_i, f_i). We introduce the adjacency relation R on the set ΓF as the following relation (or graph): the intersection of two flags is a flag of rank $s - 1$. We refer to maximal flags satisfying relation R as adjacency flags.

If $F_1 R F_2$ for flags $F_1 = \{(M_1, f_1), (M_2, f_2), \ldots, (M_s, f_s)\}$ and $F_2 = \{(M_1^+, f_1^+), (M_2^+, f_2^+), \ldots, (M_s^+, f_s^+)\}$, then there exists the index i such that colors t_i and t_i^+ are distinct, and the functions f_i and f_i^+ differ by their values on $M_i - M_1 \bigcup M_2 \bigcup \cdots \bigcup M_{i-1} \bigcup M_{i+1} \bigcup \cdots \bigcup M_s$. As follows from the definition of Schubert systems, the operator $N^i{}_{t^+}(F)$, which maps a flag F with spectrum $(t_1, t_2, \ldots, t_{i-1}, t_i, t_{i+1}, \ldots, t_s)$ into the adjacent flag F^+ of color $(t_1, t_2, \ldots, t_{i-1}, t_i^+, t_{i+1}, \ldots, t_s)$, is well defined. Obviously, the equality $t_i = t_i^+$ implies that $N_t^i(F) = F$. We define the color of the edge of graph R between vertices F and F^+ as number i. The composition $N_{t_1}^{i_1} N_{t_2}^{i_2} \cdots N_{t_k}^{i_k}$ for different colors $\{i_1, i_2, \ldots, i_k\}$ computed for flag F corresponds to walk F, $F_1 = N_{t_1}^{i_1}(F)$, $F_2 = N_{t_2}^{i_2}(F_1), \ldots, F_k = N_{t_k}^{i_k}(F_{k-1})$ in graph R. Note that edges $F R F_1$, $F_1 R F_2, \ldots$, $F_{k-1} R F_k$ are colored in distinct colors. As follows from the definition of a Schubert system, the varieties of maximal flags ΓF and the color spaces $S_i = K^{M_i - M_1 \cup M_2 \cup \cdots \cup M_{i-1} \cup M_{i+1} \cup \cdots \cup M_s}$ are free modules over the commutative ring K.

Let Q be a subring K such that K is a free module over Q of dimension d. Then ΓF and S_i are affine spaces over Q of dimensions v and v_i, respectively. It is clear that d is a divisor of these integers. Polynomial functions $G_i \colon Q^v \to Q^d$ map the affine variety of flags $\Gamma F(Q)$ over the commutative ring Q into spaces A_i of dimension d. We refer to the direct sum $S(A)$ of spaces $S_i(A_i)$ as the spectral space (space of invariants) of the variety $\Gamma F(Q)$. With the maximal flag F, we associate its trace $\mathrm{sp}(F) = (t_1, t_2, \ldots, t_s, G_1(F), G_2(F), \ldots, G_t(F))$, where $(t_1, t_2, \ldots, t_s)$ is the spectrum corresponding to the vector $\mathrm{x}(F) = (x_1, x_2, \ldots, x_l)$, $l = v_1 + v_2 + \cdots + v_s$ from S and $(G_1(F), G_2(F), \ldots, G_t(F))$ is an element from the space of invariants, which could be given

also by the vector $y(F) = (y_1, y_2, \dots, y_m)$, $m = td$. Let $f_i = f(x_1, x_2, \dots, x_l, y_1, y_2, \dots, y_m)$ be a polynomial (or birational) map from $S + A$ into S_i defined over the commutative ring, Q. Let Z be an abstract flag from the totality $\Gamma F(Q)$ with the spectrum $z_1, z_2, \dots, z_l$ and invariants $G_1(Z), G_2(Z), \dots, G_m(Z)$. A specialization $f_i(Z) = f_i(Z_1, Z_2, \dots, Z_l, G_1(Z), G_2(Z), \dots, G_m(Z))$ associates the tuple $f_i(Z)$ from S_i with given Z. We define the symbolic code of a walk as the string $f_{i_1}, f_{i_2}, \dots, f_{i_t}$ of such maps, where the sequence $i_1, i_2, \dots, i_t$ is such that i_s differs from i_{s+1} for each s, and t is determined by a certain function $t = T(x_1, x_2, \dots, x_l, y_1, y_2, \dots, y_m)$, which maps $S + A$ into the set Z^+ of positive integers. Let F be a flag from $\Gamma F(Q)$. First, we compute its spectrum and the set of invariants $G_1(F), G_2(F), \dots, G_t(F)$ and get the tuple $(x_1, x_2, \dots, x_l, y_1, y_2, \dots, y_m)$ (extended spectrum of the flag) from the module $S + A$. Then we compute $t = t(F)$ and $f_{i_1}(F)$, $f_{i_2}(F), \dots, f_{i_t}(F)$ for our flag F. It allows us to compute $N = N_{t_1}^{i_1} N_{t_2}^{i_2} \cdots N_{t_t}^{i_m}(F)$, where $t_{i_s} = f_{i_s}(F)$. So we get the element $F^+ = N(F)$, which is the last vertex of the computed walk in graph R. This means that the symbolic code $f_{i_1}, f_{i_2}, \dots, f_{i_t}$ of length $t = T(x_1, x_2, \dots, x_l, y_1, y_2, \dots, y_m)$ determines the map $N = N(f_{i_1}, f_{i_2}, \dots, f_{i_t})$ of $\Gamma F(Q)$ into itself. Under certain conditions, the reimage of flag F^+ under the above-described map can be computed. Obviously, the flags F^+ and F are from the same connected component of graph R. So, for the extended spectra $(x_1^+, x_2^+, \dots, x_l^+, y_1^+, y_2^+, \dots, y_m^+)$ and $(x_1, x_2, \dots, x_l, y_1, y_2, \dots, y_m)$, the following equalities hold: $y_1^+ = y_1$, $y_2^+ = y_2, \dots, y_m^+ = y_m$. The tuple $(x_1^+, x_2^+, \dots, x_l'^+)$ is uniquely determined by the symbolic code and the spectrum of flag F. For each i, we consider the function of kind f_{i_r}, $i_r = i$, which appears in the symbolic code on the last position. If such a function really exists, we denote it by f_i^*; if not, we assume $f_i^* = x_i$. We refer to the set $f_1^*, f_2^*, \dots, f_l^*$ as the boundary of a symbolic code. For each function f_{i_k} of the symbolic code, we denote the previous function with the index i_k by $f_{i_k}^+$, if such a function exists. If not, we assume that $f_{i_k}^+ = x_{i_k}$. It is clear that $x_i^+ = {f^*}_i(x_1, x_2, \dots, x_l)$ for each i. Let us assume now that the map g from S into itself shifting x_i into x_i^+ is a bijection. Then flag F^+ can be used for the computation of the spectrum $g^{-1}(x_1, x_2, \dots, x_l)$ and the set of invariants y_j of F. We can compute the length $t = T(x_1, x_2, \dots, x_l, y_1, y_2, \dots, y_m)$ and the reverse walk F^+, $F_{i_t} = N_{f_{i_t}^+}^{i_t}(F^+)$, $F_{i_{t-1}} = N_{f_{i_t-1}^+}^{i_t-1}(F_{i_t-1}), \dots, F = N_{f_1^+}^{i_1}(F_1)$. Note that $\mathrm{sp}(F'^+) = (x_1^+, x_2^+, \dots, x_s^+)$, where the coordinate x_i^+ equals x_i plus the sum of all f_j for j equal to i. The simplest example of invertible functions can be obtained in the case where all functions f_i^* are linear functionals of the kind $x_1 H^{i1}(F) + x_2 H^{i2}(F) + \cdots + x_l H^{il}(F) + H^0$, where H^0 and H^{is} depend only on y_1, $y_2, \dots, y_m$, and the matrix $H^{ij}(F)$, $j \in \{i_1, i_2, \dots, i_l\}$, $i = 1, 2, \dots, l$, is invertible.

General algorithm of encryption. Let us consider the following private key encryption algorithm. Let $\Gamma F_n(K)$ be a sequence of varieties of maximal flags of Schubert systems $\Gamma_n(K)$ of rank n over finite commutative rings K of increasing order. The parameter $d = d(n)$ will stand for the dimension of the variety of maximal flags in $\Gamma F_n(K)$. Let us assume that Q is a subring of K such that a commutative ring K is isomorphic to a free module Q^m over Q. Let $\Gamma F_n(Q)$ be a set of maximal flags as a variety of dimension dm over Q. Correspondents Alice and Bob consider the variety $\Gamma F_n(K)$ as a plainspace $\Gamma F_n(K)$. A subring Q will be treated as a part of the common key. Similarly to the case of the Imai–Matsumoto multivariate cryptosystem, the key contains two bijective affine transformations L_1 and L_2 of the variety $\Gamma F_{dm}(Q)$. So, the plaintext can be identified with the string $\mathrm{x} = (p_1, p_2, \dots, p_{dm})$ written as a row vector in the alphabet Q. The transformation $L_i \colon \mathrm{x} \to \mathrm{x}A_i + \mathrm{b}_i$, $i = 1, 2$, is given by the matrix A_i of size dm and the vector b_i. We assume that the orders of transformations T_i, $i = 1, 2$, increase with the parameter n. The "nonlinear part" of the key (symbolic code) is

a "potentially infinite" sequence of pairs (i_s, f_{i_s}), where $f_{i_s} = f(x_1, x_2, \ldots, x_l, y_1, y_2, \ldots, y_m)$, $s = 1, 2, \ldots, N$, is a polynomial (or birational) map from $S + A$ into S_i defined as above. We assume that the boundary of the symbolic key $\{f_1^*, f_2^*, \ldots, f_l^*\}$ is fixed, and the expansion of this key can be achieved by writing, from the left, a new set of initial elements. Additional requirements are inequalities $i_s \neq i_{s+1}$, which hold for each s. The key contains also three time functions $h_i = t_i(x_1, x_2, \ldots, x_l, y_1, y_2, \ldots, y_m)$, $i = 0, 1, 2$, which are certain maps from $S + A$ into the set of positive integers Z^+. At the beginning, Alice applies the affine transformation L_1 to the plaintext x and gets the flag $F = L_1(\mathrm{x})$ written as a string over the alphabet K. Then she computes the length $h = h_0(F)$ of the nonlinear part of the symbolic key, as well as the values $f_{i_1}(F)$, $f_{i_2}(F), \ldots, f_{i_h}(F)$ of functions from the symbolic key for the obtained flag F. The next step for Alice is the computation of $N = N_{t_1}^{i_1} N_{t_2}^{i_2} \cdots N_{t_h}^{i_h}(F)$, where $t_{i_s} = f_{i_s}(F)$, and she gets the last flag of computed walks $F^+ = N(F)$. The flag $L_2(F^+) = Y$ is sent to Bob via an open channel. We shall assume that the input and output data for our encryption algorithm are given in the form of tuples over the commutative ring K. The length of the sequence (i_s, f_{i_s}) is chosen in a special way, so the reimage of flag F^+ for the map N is always computable (or computable in the case of "almost all" flags). Bob gets Y and computes flag ${L_2}^{-1}(Y) = F^+$, which belongs to the connected component of graph R containing F. He computes numerically the invariants $G_1(F^+)$, $G_2(F^+), \ldots, G_t(F^+)$ and uses the boundary $\{f_1^*, f_2^*, \ldots, f_l^*\}$ for the computation of the spectrum of F. He computes the reverse walk in the graph R for finding its initial vertex F. Finally, Bob computes ${L_1}^{-1}(F)$ and writes this tuple in the form of a string over the alphabet K. At the end of the communication session, the correspondents may change affine maps L_1 and L_2 for their powers ${L_i}^{T_i}$, $i = 1, 2$.

An example of effectively computable enciphering map. Obviously, an arbitrary linguistic graph is a Schubert structure. Let K be a finite commutative ring. Let us consider the infinite bipartite graph $D(K)$ with the point set $\Gamma_1 = P$ consisting of elements $\mathrm{x} = (x_1, x_2, x_3, x_3^-, \ldots, x_n, x_n^-, \ldots)$ and the line set $\Gamma_2 = L$ consisting of lines $\mathrm{y} = [y_1, y_2, y_3, y_3^-, \ldots, y_n, y_n^-, \ldots]$ with the incidence relation I : xIy, x $\in P$, and y $\in L$ if and only if the following two sets of relations hold:

(1) $x_2 - y_2 = y_1 x_1$, $x_3 - y_3 = x_1 y_2$, $x_4 - y_4 = y_1 x_3$, $x_5 - y_5 = x_1 y_4$, $\ldots$, $x_n - y_n = x_1 y_{n-1}$ for odd n and $x_n - y_n = y_1 x_{n-1}$ for even n.

(2) $x_3^- - y_3^- = y_1 x_2$, $x_4^- - y_4^- = x_1 y_3^-$, $x_5^- - y_5^- = y_1 x_4^-$, $\ldots$, $x_n^- - y_n^- = y_1 x_{n-1}^-$ for odd n and $x_n^- - y_n^- = x_1 y_{n-1}^-$ for even values of parameter n. Let us consider also the bipartite graph $D(n, K)$ defined on the set of points $P_n = K^n$ and lines $L_n = K^n$ in the following way: vectors x_n and y_n from P_n and L_n, are identified with the projections of the infinite tuples x $\in P$ and y $\in L$ into their n initial coordinates, x_n and y_n are connected by an edge if and only if the first $n-1$ relations from the definition of incidence of x and y hold. In the case $K = F_q$, the family of graphs $D(n, K) = D(n, q)$ together with special induced subgraphs was defined in [10]. In that paper, some extremal properties of these graphs were investigated. For the general commutative rings, the simplest properties of $D(n, K)$ and $CD(n, K)$ were considered in [11].

The most general connectivity properties of graphs $CD(n, K)$ were obtained in [12]. The discrete dynamical systems corresponding to these families of graphs were studied in [13]. If the characteristic of a commutative ring K equals 2, then the graph $CD(n, K)$ simply coincides with the connected component of $D(n, K)$. Note that all connected components of $D(n, K)$ are isomorphic. The partition sets P_n and L_n of the graph $CD(n, q)$ can be identified with K^t, where $t = [3/4n] + 1$ for $n = 0, 2, 3 \pmod 4$ and $t = [3/4n] + 2$ for $n = 1 \pmod 4$.

It is known that there exist m quadratic invariants a_1, $a_2, \ldots, a_m$ where $m = [1/4n] - e$ with $e = -1$ for $n = 0, 2, 3 \pmod 4$ and $e = 0$ in the remaining case such that, for two points (or lines) x and y of the graph $D(n, q)$ from the same connected component, the equalities $a_1(\mathrm{x}) = a_1(\mathrm{y})$ and $a_2(\mathrm{x}) = a_2(\mathrm{y}), \ldots, a_m(\mathrm{x}) = a_m(\mathrm{y})$ hold. The inequality $a_i(\mathrm{x}) \neq a_i(\mathrm{y})$ for some i implies that x and y are vertices from distinct connected components.

In the case of characteristic 2, the above-written conditions uniquely define the partition into connected components. Colors of point $(\mathrm{x}) = (x_1, x_2, \ldots, x_n)$ and line $[\mathrm{y}] = [y_1, y_2, \ldots, y_n]$ are just the first coordinates x_1 and y_1 of these tuples. The flag (x), [y], (x)I[y] of this linguistic graph is uniquely determined by coordinates of point $(x_1, x_2, \ldots, x_n)$ and color y_1 of line [y].

Let us assume that the commutative ring K is a free module Q^r over another ring Q, and the multiplication of K is a quadratic map of $K \times K$ into K over Q. The natural example is the Kronecker extension of the ring Q, i. e. $K = Q[x]/g(x)$, where $g(x) \in Q[x]$ is some polynomial.

Let us consider the above-described algorithm in the case of a symbolic key $x_1 + d_1$, $y_1 + {} + d_1^+, \ldots, x_l + d_l$, $y_1 + d_l'^+$ of even variative length $2l$, $l = T(\mathrm{x}, y_1)$ (in the case of odd length $2l+1$, one can use the symbolic key $(x_1 + d_1, y_1 + d_1^+, \ldots, x_l + d_l, y_1 + d_l^+, x_l + d_{l+1})$), where the function T is obtained from the map $f(z_1, z_2, \ldots, z_r, z_{r+1}, z_{r+2}, \ldots, z_{2r}, z_{2r+1}, z_{2r+2}, \ldots, z_{r(m+2)})$ from the set $Q^{r(m+2)}$ into Z^+ by the specialization $(z_1, z_2, \ldots, z_{r(m+2)}) = (x_1^+, x_2^+, \ldots, x_r^+, y_1^+, y_2^+, \ldots, y_r'^+, a_{11}, a_{12}, \ldots, a_{1r}, a_{21}, a_{22}, \ldots, a_{2r}, \ldots, a_{m1}, a_{m2}, \ldots, a_{mr})$, where $(x_1^+, x_2^+, \ldots, x_r^+)$ and $(y_1^+, y_2^+, \ldots, y_r^+)$ are coordinates of the flag xIy written in the chosen base of $K = Q^r$, and $(a_{i1}, a_{i2}, \ldots, a_{ir})$, $i = 1, 2, \ldots, m$, are the coordinates of the invariant values $a_1(\mathrm{x}), a_2(\mathrm{x}), \ldots, a_m(\mathrm{x})$ of the point x from the flag. Let the flag from K^{n+1} be defined by the vector v of the free module $Q^{r(n+1)}$. Let L_1 and L_2 be two invertible affine transformations of the plainspace $Q^{r(n+1)}$. We assume that they are a part of the key of our symmetric algorithm. For simplification, we assume that the length of a symbolic key is an odd number.

Let us denote, by N, the composition of maps $N_{x_1+d_1}$, $N_{y_1+d_1^+}$, $N_{x_2+d_2}$, $N_{y_2+d_2^+}, \ldots, N_{x_l+d_l}$, $N_{y_1+d_l^+}$. The encryption consists of the following steps:

(a) application of the affine map L_1 to the plainspace v, the resulting vector $L_1(\mathrm{v})$ from $Q^{r(n+1)}$ have to be written as a vector u from the free module over the extension K of Q.

(b) the computation of the vector $\mathrm{w} = N(\mathrm{u})$ and its presentation by the vector w^+ in the chosen base of $Q^{r(n+1)}$.

(c) computation of the vector $\mathrm{z} = L_2(\mathrm{w}^+)$. The deciphering is the reverse process. The correspondent (Bob) receives the ciphertext z in the form of a vector from $Q^{r(n+1)}$. He computes ${L_2}^{-1}$ and writes this vector as a element w from K^{n+1}. Then Bob defines $\mathrm{u} = N^{-1}(\mathrm{w})$ and writes the result in the form of a vector u^+ with coordinates from Q. For the determination of the plainspace v, he writes $L_1^{-1}(\mathrm{u}^+)$ in the form of an element from K^{n+1}.

On the properties of an encryption map It turns out that, independently of the choice of sequences d_1, $d_2, \ldots, d_l$ and d_1^+, $d_2^+, \ldots, d_l^+$, the transformation N is a polynomial map of kind $(x_1, x_2, \ldots, x_n) \to (f_1(x_1, x_2, \ldots, x_{n+1}), f_2(x_1, x_2, \ldots, x_{n+1}), \ldots, f_n(x_1, x_2, \ldots, x_{n+1}))$, where all polynomials $f_i(x_1, x_2, \ldots, x_{n+1})$, $i = 1, 2, \ldots, n$, $n+1$, are cubic (see [15] and references therein). This means that both the encryption map $E = L_1 N L_2$ and the inverse map $E^{-1} = {} = L_1^{-1} N^{-1} L_2^{-1}$, together with the inverse map $E' = L_2' N' L_1'$ are cubic transformations. Recall that E^{-1} corresponds to d_1, $d_2, \ldots, d_l$ and d_1', $d_2', \ldots, d_l'$ written in the inverse order.

Let us assume that a fixed key is in multiple use, and the adversary has an access to some plaintext and can obtain a rather large set of pairs of the plaintext-ciphertext kind. In this case,

the fact that the degree of the polynomial inverse map is bounded by 3 makes the linearization attacks feasible. In fact, the key can be computed in a polynomial time. The above-written condition is not a realistic one. So, the cubic encryption map was used for the protection of real communication networks for various rings.

First, the algorithms were used in the case of prime finite fields (e. g., Z_{127}). Then the arithmetical rings Z_{2^n}, $n = 7, 8, 16, 32$, and the Galois fields F_{2^n} for $n = 7, 8, 16, 32$, were used. The attractive side of the encryption algorithm is its speed (complexity $O(nl)$), resistance against attacks without access to plaintexts. In the case of $l \leqslant [n/2] + 2$ and $K = F_q$, the different sequences d_i ($d_i \neq d_{i+1}$), d_i^+, ($d_i^+ \neq d_{i+1}^+$, $i = 1, 2, \ldots, l$) give different ciphertexts. The generalizations of this fact to the case of arbitrary commutative rings are given in [13]. Computer simulations (see surveys [14], [15] and references therein) in the case of a special choice of affine transformations demonstrate that the encryption function has strong mixing properties. It satisfies the well-known Madryga's requirements: change of one character in the plaintext or in the key leads to a change of the vast majority characters of the ciphertext if the alphabet K is used.

The enciphering algorithm with the key of variative length described in the example given above allows one to increase the level of resistance of an encryption against attacks with an access to some plaintexts without essential change of the robustness and the mixing quality.

The dependence of the length function l on a plainspace makes classical linearization attacks impossible.

Let us show that the complexity of the known difficult discrete logarithm problem can serve as a security argument for the algorithm. Assume that the sequences d_i and d_i^+, $i = 1, 2, \ldots, l$, are periodic. This means that there exists r such that $l = r_j$, $d_{i+r}^+ = d_i^+$, $d_{i+r} = d_i$. Additionally, we assume that $L_1 = L^{2^{-1}}$ and the parameter r is constant. Let $G = L_1 N^+ L_2$, where the map $N^+ = N_{x_1+d_1} N_{y_1+d_1^+} N_{x_2+d_2} N_{y_2+d_2^+} \cdots N x_r + d_l$, $N y_r + d_r^+ L_2$ is computed with the use of some computer algebra program. The resulting polynomial transformation G will be written as $(x_1, x_2, \ldots, x_n) \to (g_1(x_1, x_2, \ldots, x_{n+1}), g_2(x_1, x_2, \ldots, x_{n+1}), \ldots, g_n(x_1, x_2, \ldots, x_{n+1}))$, where each polynomial $g_i(x_1, x_2, \ldots, x_{n+1})$, $i = 1, 2, \ldots, n+1$, is a cubic expression given by a list of monomials in lexicographical order. So, the value of G at the given point will be computed in the time bounded by $O(n^4)$. Note that the order of a map G coincides with the order of N^+. As follows from the above-written facts, each power of the map G in the symmetric group $S(K^n)$ is a cubic map or the identity. Let M be a multiplicative subset of the commutative ring K. This means that M is closed under multiplication and does not contain zero. If all $d_i + d_{i+1}$, $d_i^+ + d_{i+1}^+$, $i = 1, 2, \ldots, l$, and $d_1 + d_l$, $d_1^+ + d_l^+$ are elements of M, then the order of the transformation G tends to infinity with the growth of the parameter n. The increase of the map order is going on with the increase of the characteristic of the ground ring (see [13] and references therein).

Recall that, in our case, the correspondents use the periodic map $G = G_r$, and the length function l is a function of the plainspace, which can generally has any value. We assume that the adversary can get many pairs (p, c), where p is a plaintext, and c is a corresponding ciphertext.

Additionally, we assume that the basic polynomial G is known to the adversary. The natural attack on the key can be conducted via the investigation of the equation $G^z(p) = c$ with the known tuples p and c and the unknown positive integer z. So, we get the discrete logarithm problem

for the cyclic subgroup generated by G. We have to solve the equation $G^z = H$, where H is some function transforming p into c. The opponent could not solve this problem in the case of a sufficiently large number of variables, because the order of G is increasing, but the degree of the right-hand side is still cubic. The investigation of iterations of G brings no additional data for the investigation of the discrete logarithm problem. The adversary can determine G^{-1} by computing many pairs of kind $(v, G(v))$ and by conducting a linearization attack. The computation of the unknown functions $l = l(x)$, $j(x) = l(x)/r$, and $G^{-j}(x)$ is related to the above-mentioned discrete logarithm problem with the base G. Note that the function $j(x)$ can be very sophisticated, for instant, defined as a specialization of the known Matijasevich polynomial.

The author expresses his sincere gratitude to Professor Richard Weiss (Boston) for his constant support of the idea to use geometries over diagrams for the problems of informational defence and a stimulating lecture course at the University of Maria Curie Sklodowska in Lublin.

1. *Buekenhout F.* Handbook of incidence geometry. – Amsterdam: North-Holland, 1995. – 1399 p.
2. *Ustimenko V.* Maximality of affine group and hidden graph cryptosystems // J. Alg. Discr. Math. – 2005. – No 1. – P. 133–150.
3. *Ustimenko V.* Linear interpretations for flag geometries of Chevalley groups // Ukr. Mat. Zh. – 1990. – **42**, No 3. – P. 383–387.
4. *Ustimenko V.* On the varieties of parabolic subgroups, their generalisations and combinatorial applications // Acta Appl. Math. – 1998. – **52**. – P. 223–238.
5. *Ustimenko V.* Small Schubert cells as subsets in Lie algebras // Funct. Analysis and Appl. – 1991. – **25**, No 4. – P. 81–83.
6. *Ustimenko V.* Geometries of twisted groups of Lie type as objects of linear algebra // Questions of Group Theory and Homological Algebra. – Yaroslavl: Yaroslavl State Univ., 1990. – P. 33–56 (in Russian).
7. *Beutelspachera A.* Enciphered geometry. Some applications of geometry to cryptography // Ann. of Discr. Math. – 1988. – **37**. – P. 59–68.
8. *Ustimenko V.* Graphs with special arcs and cryptography // Acta Appl. Math. – 2002. – **74**, No 2. – P. 117–153.
9. *Ustimenko V.* Schubert cells in Lie geometries and key exchange via symbolic computations // Albanian J. of Math. – 2010. – **4**, No 4. – P. 135–145.
10. *Lazebnik F., Ustimenko V. A., Woldar A. J.* New series of dense graphs of high girth // Bull. (New Series) of AMS. – 1995. – **32**, No 1. – P. 73–79.
11. *Ustimenko V.* Coordinatisation of trees and their quotients // Voronoj's Impact on Modern Science. – Kiev: Institute of Mathematics of the NASU, 1998. – **2**. – P. 125–152.
12. *Ustimenko V.* Algebraic groups and small world graphs of high girth // Albanian J. of Math. – 2009. – **3**, No 1. – P. 25–33.
13. *Ustimenko V., Romanczuk U.* On dynamical systems of large girth or cycle indicator and their applications to multivariate cryptography // Artificial Intelligence, Evolutionary Computing and Metaheuristics. – Berlin: Springer, 2013. – P. 257–285.
14. *Ustimenko V.* On the cryptographical properties of extreme algebraic graphs // Algebraic Aspects of Digital Communications, edited by T. Shaska, E. Hasimaj. – Amsterdam: IOS Press, 2009. – P. 256–281.
15. *Ustimenko V.* On the extremal graph theory for directed graphs and its cryptographical applications // Advances in Coding Theory and Cryptography, edited by T. Shaska, W. C. Huffman, D. Joyner, V. Ustimenko. – Singapore: World Scientific, 2007. – **3**. – P. 181–200.

Institute of Telecommunications
and Global Information Space, the NAS of Ukraine, Kiev
University of Maria Curie Sklodowska, Poland

Received 02.09.2013

В. А. Устименко

О блужданиях переменной длины в системах инцидентности Шуберта и полиномиальном потоковом шифровании

Предложен алгоритм потокового шифрования, основанный на блужданиях на многообразиях флагов системы Шуберта, определенной над коммутативным кольцом. Примером системы Шуберта является ограничение отношений инцидентности геометрии простой группы Ли нормального типа на объединение больших клеток максимальной размерности. Более общие примеры соответствуют группам Каца–Муди. Приведен пример использования таких симметричних алгоритмов, определенных на периодических блужданиях, для создания публичного ключа, безопасность которого связана с проблемой дискретного логарифма для циклических подгрупп полиномиальных преобразований возрастающего порядка.

В. О. Устименко

Про блукання змінної довжини в системах інцидентності Шуберта та поліноміальному струменевому кодуванні

Запропоновано алгоритм струменевого кодування, що грунтується на блуканнях на многовидах прапорів системи Шуберта, визначеної над комутативним кільцем. Прикладом системи Шуберта є обмеження відношень інцидентності геометрії простої групи Лі нормального типу на об'єднання великих клітин максимального виміру. Більш загальні приклади пов'язані з групами Каца–Муді. Наводено приклад використання таких струменевих алгоритмів, визначених на періодичних блуканнях, для створення відкритого поліноміального ключа, безпека якого пов'язана з проблемою дискретного логарифма для циклічних підгруп поліноміальних перетворень зростаючого порядку.