UDC 519.1,514.128

U. Romańczuk-Polubiec, V. A. Ustimenko

On new key exchange multivariate protocols based on pseudorandom walks on incidence structures

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

A new key exchange protocol formulated in terms of multivariate cryptography and based on the elaboration of a common walk in the linguistic graph by correspondents is proposed. This algorithm is described in details in the case of a known family of graphs of large girth given by nonlinear equations over a finite field.

Linguistic graphs and their properties. The missing definitions of graph-theoretical concepts, which appear in this paper can be found in [1]. A *tactical configuration* introduced by E. H. Moore [2] is a rank two incidence structure I consisting of v_p points from the set P and v_l lines from the set L, where each point is incident to s lines, and each line is incident to r points. We denote the incidence graph of the incidence structure I by $\Gamma = \Gamma(P, L, I)$ and call Γ a *tc-graphs*, though we shall identify I with the simple graph Γ of this incidence relation, if no confusion can arise. We define the *biregular and bipartite graphs* as tc-graphs with bidegrees r, s. Clearly, the graph Γ has *order* $v = v_l + v_p$ (number of vertices) and *size* $e = rv_l = sv_p$ (number of edges). We also mean, as usual, that the *girth* $g(\Gamma)$ of the graph Γ is the length of the minimal cycle in the graph, and the *diameter* of the graph is the maximal distance between two vertices u and v in the graph, denoted by $\mathrm{diam}(\Gamma)$. The pair $\{\mathrm{x}, \mathrm{y}\}$, $\mathrm{x} \in P$, $\mathrm{y} \in L$ such that $\mathrm{x}I\mathrm{y}$ is called a *flag* of the incidence structure I.

Let $\mathbb{K}$ be a finite commutative ring. We refer to an incidence structure I with a point set $P_r = K^{\mathbb{N}}$ and a line set $L_s = K^{\mathbb{N}}$ as *infinite linguistic tc-graphs* $\mathrm{L}\Gamma(r, s, \mathbb{K})$, if the point $(\mathrm{x}) = (x_1, x_2, \ldots, x_r, x_{r+1}, x_{r+2}, \ldots) \in P_r$ is incident to the line $[\mathrm{y}] = [y_1, y_2, \ldots, y_s, y_{s+1}, y_{s+2} \ldots] \in L_s$ if and only if the following relations hold:

$$\begin{aligned}
&\xi_1 x_{r+1} + \zeta_1 y_{s+1} = f_1(x_1, x_2, \ldots, x_r, y_1, y_2, \ldots, y_s)\\
&\xi_2 x_{r+2} + \zeta_2 y_{s+2} = f_2(x_1, x_2, \ldots, x_r, x_{r+1}, y_1, y_2, \ldots, y_s, y_{s+1})\\
&\ldots\\
&\xi_i x_{r+i} + \zeta_i y_{s+i} = f_i(x_1, x_2, \ldots, x_{r+i-1}, y_1, y_2, \ldots, y_{s+i-1})\\
&\ldots
\end{aligned}$$

Here, ξ_j and ζ_j, $j = 1, 2, \ldots$ are nonzero divisors, and f_j, $j = 1, 2, \ldots$ are multivariate polynomials with coefficients from K. Brackets and parentheses allow us to distinguish points from lines (see [3, 4]).

For each positive integer $m \geqslant 2$, we obtain an incidence structure I_m with a point set $P_{r,m} = K^{r+m}$ and a line set $L_{s,m} = K^{s+m}$ as follows: $P_{r,m}$ and $L_{s,m}$ are obtained from P_r and L_s, respectively, by simply projecting each vector into its $r+m$ and $s+m$ initial coordinates with respect to the above order, respectively. The incidence I_m is then defined by imposing the first m incidence equations and ignoring all others. The incidence graph corresponding to the structure I_m is denoted by $\mathrm{L}\Gamma(r,s,m,\mathbb{K})$, and we call it the *linguistic incidence structure* or *linguistic graph.* Of course, $L\Gamma(r,s,m,\mathbb{K})$ is a $(|\mathbb{K}|^r,|\mathbb{K}|^s)$-biregular bipartite graph of order $2|\mathbb{K}|^{r+s+m}$.

For each positive integer $m \geqslant n \geqslant 1$, we consider the *standard graph homomorphism* ϕ_n^m of $\mathrm{L}\Gamma(r,s,m,\mathbb{K})$ onto $\mathrm{L}\Gamma(r,s,n,\mathbb{K})$ defined as a simple projection of each vector from $P_{r,m}$ and $L_{s,m}$ onto its $r+n$ and $s+n$ initial coordinates with respect to the above-mentioned order, respectively. Let $v \in \mathrm{L}\Gamma(r,s,m,\mathbb{K})$ and $v' \in \mathrm{L}\Gamma(r,s,n,\mathbb{K})$ be the vertices of the same type point or line. We refer the vertex v as a *lift* of v', when $v' = \phi_n^m(v)$.

Recall that, for simple graphs Γ_1 and Γ_2, a *graph homomorphism* ϕ of Γ_1 to Γ_2 is a mapping between these two graphs that respect their structure. More specifically, ϕ maps the adjacent vertices of Γ_1 to the adjacent vertices of Γ_2.

Proposition 1. *Let $m \geqslant n \geqslant 1$. The map ϕ_n^m is a $|\mathbb{K}|^{m-n}$-to-1 surjective graph homomorphism from a graph $L\Gamma(r,s,m,\mathbb{K})$ to a graph $L\Gamma(r,s,n,\mathbb{K})$.*

From the fact that ϕ_n^m is a graph homomorphism, one can deduce that, for a fixed ring $\mathbb{K}$, the diameter and the girth of $\mathrm{L}\Gamma(r,s,n,\mathbb{K})$ are nondecreasing functions of n.

Proposition 2. *Let $m > n \geqslant 1$, and let $\mathbb{K}$ be any commutative ring. Then* $\mathrm{diam}(L\Gamma(r,s,m,\mathbb{K})) \geqslant \mathrm{diam}(L\Gamma(r,s,n,\mathbb{K})$, *and* $\mathrm{girth}(L\Gamma(r,s,m,\mathbb{K})) \geqslant \mathrm{girth}(L\Gamma(r,s,n,\mathbb{K}))$.

Let $M = \{m_1, m_2, \ldots, m_d\}$ be a subset of $\{1, 2, \ldots m\}$ (set of indices for the equations), $d \leqslant m$ with the standard order. Assume that the equations indexed by elements from M of the kind

$$\xi_{m_1}x_{m_1} + \zeta_{m_1}y_{m_1} = f_{m_1}(x_1, x_2, \ldots, x_r, y_1, y_2, \ldots, y_s)$$

$$\xi_{m_2}x_{m_2} + \zeta_{m_2}y_{m_2} = f_{m_2}(x_1, x_2, \ldots, x_r, x_{m_1}y_1, y_2, \ldots, y_s, y_{m_1})$$

$$\ldots$$

$$\xi_{m_d}x_{m_d} + \zeta_{m_d}y_{m_d} = f_{m_d}(x_1, \ldots, x_r, x_{m_1}, \ldots, x_{m_{d-1}}, y_1, \ldots, y_s, y_{m_1}, \ldots, y_{m_{d-1}})$$

define another linguistic incidence structure I_M. Then the natural projections

$$\phi_M^m \colon (\mathrm{x}) \to (x_1, x_2, \ldots, x_r, x_{m_1}, x_{m_2}, \ldots, x_{m_d}),$$

$$\phi_M^m \colon [\mathrm{y}] \to [y_1, y_2, \ldots, y_s, y_{m_1}, y_{m_2}, \ldots, y_{m_d}]$$

of free modules define the natural homomorphism $\phi = \phi_M^m$ of the incidence structure I_m onto I_M. We refer to $\rho = phi_{\varnothing}^m$ as a coloring homomorphism of $\mathrm{L}\Gamma(r,s,n,\mathbb{K})$ onto the complete bipartite graph $K_{a,b}$, $a = |\mathbb{K}^r|$, $b = |\mathbb{K}^s|$. For each line $[l]$ and colour $\mathrm{t} = [t_1, t_2, \ldots, t_r]$, there is a unique neighbor $(\mathrm{x}) \in P$ of the line with the given color $\rho(\mathrm{x}) = \mathrm{t}$. Similarly, $(p)]$ and color $\mathrm{d} = [d_1, d_2, \ldots, d_s]$, there is a unique neighbor $[\mathrm{y}] \in L$ of the point with the color $\rho([\mathrm{x}]) = \mathrm{d}$. We will use the same symbol ρ for the coloring of the linguistic graph I_M.

It is clear that, $for \phi = \phi_M^m$, the relations $\rho(\mathrm{x}) = \rho(\phi(\mathrm{x}))$ and $\rho(\mathrm{y}) = \rho(\phi(\mathrm{y}))$ hold. This means that ϕ_M^m is a color-preserving homomorphism of the incidence structure (bipartite graph) onto another one. We refer to ϕ_M^m as a *symplectic homomorphism* and graph $\mathrm{L}\Gamma(r,s,M,\mathbb{K}) = \phi_M^m(\mathrm{L}\Gamma(r,s,m,\mathbb{K}))$ as a *symplectic quotient of the linguistic incidence structure I_m*. In the case of linguistic graphs defined by the infinite number of equations, we may consider the cases of symplectic quotients defined by the infinite subset M.

Proposition 3. *Let $m \geqslant d \geqslant 1$, and let $M = \{m_1, m_2, \ldots, m_d\}$ be a subset of $\{1, 2, \ldots, m\}$. The map ϕ_M^m is a $|\mathbb{K}|^{m-d}$-to-1 surjective graph homomorphism from a graph $L\Gamma(r,s,m,\mathbb{K})$ to a graph $L\Gamma(r,s,M,\mathbb{K})$.*

The color $\rho(\mathrm{x}) = \rho((\mathrm{x}))$ ($\rho(\mathrm{y}) = \rho([\mathrm{y}])$) of the point (x) (line [y]) is defined as the projection of an element (x) ([y]) from a free module on its initial r (relatively s) coordinates. We note that there exists the unique neighbor of a chosen color in a linguistic incidence structure (finite or infinite) for each vertex of the incidence graph. We can generalize this fact as follows:

Proposition 4. *Let v be a vertex in $L\Gamma(r, s, m, \mathbb{K})$, let u be a vertex in $L\Gamma(r, s, n, \mathbb{K})$ ($L\Gamma(r, s, M, \mathbb{K})$), and let $\{\phi_n^m(v), u'\}$ be a flag of the incidence structure I_n (I_M, respectively). Then there exists the unique vertex $u \in L\Gamma(r, s, m, \mathbb{K})$ such that $\phi_n^m(u) = u'$ and $\{u, v\}$ is a flag of the incidence structure I_m.*

For a subgraph H of $\mathrm{L}\Gamma(r, s, m, \mathbb{K})$, we define $\phi_n^m(H)$ and $\phi_M^m(H)$ to be subgraphs of $\mathrm{L}\Gamma(r, s, n, \mathbb{K})$ and $\mathrm{L}\Gamma(r, s, M, \mathbb{K})$, respectively. The following proposition allows us to extend the notation of the *graph lift to a tree.*

Proposition 5. *Let T' be a tree in $L\Gamma(r, s, n, \mathbb{K})$ ($L\Gamma(r, s, M, \mathbb{K})$), and let v' be the a fixed vertex in T'. Then, for each lift v of v' from $L\Gamma(r, s, m, \mathbb{K})$, there exists the unique tree T in $L\Gamma(r, s, m, \mathbb{K})$ such that the vertex $v \in T$ and $\phi_n^m(T) = T'$ ($\phi_n^m(T) = T'$, respectively). Moreover, the $|\mathbb{K}|^{m-n}$ ($|\mathbb{K}|^{m-d}$) trees in $L\Gamma(r, s, m, \mathbb{K})$, which are preimages of T', are pairwise disjoint vertices.*

We note that the set of lifts of T' does not depend on the chosen vertex $v \in T'$, so the above proposition could be stated as "Each tree in $\mathrm{L}\Gamma(r, s, n, \mathbb{K})$ and $\mathrm{L}\Gamma(r, s, M, \mathbb{K})$ lifts to $|\mathbb{K}|^{m-n}$ and $|\mathbb{K}|^{m-d}$ trees in $\mathrm{L}\Gamma(r, s, m, \mathbb{K})$ and $\mathrm{L}\Gamma(r, s, M, \mathbb{K})$, respectively, which are pairwise disjoint vertices". *Note also* that, in particular, it is true for *paths lift to paths* for these graphs.

Proposition 6. *Let C be a component of $L\Gamma(r, s, m, \mathbb{K})$, $m \geqslant n \geqslant 1$, and let $L\Gamma(r, s, M, \mathbb{K})$ be a symplectic quotient. Then $\phi_n^m(C)$ and $\phi_M^m(C)$ are components of $L\Gamma(r, s, m, \mathbb{K})$ and $L\Gamma(r, s, M, \mathbb{K})$, respectively.*

We introduce adjacency relation ${}^{\mathcal{F}}I_m$ on the set of flags $\mathcal{F}(V_m)$ of the incidence structure I_m with a vertex set $V_m = P_{r,m} \cup L_{s,m}$ over a commutative ring K as a *flag relation* (or *flag linguistic graph*): the intersection of two distinct flags is a nonempty set (singleton). All vertices forming two flags $F_1 = \{(x_1), [y_1]\}$ and $F_2 = \{(x_2), [y_2]\}$ could be located at the same connected component of I_m, or all of them are from distinct connected components of I_m. Assume that the system of equations $G_1(\mathrm{x}) = g_1$, $G_2(\mathrm{x}) = g_2$, $\ldots$, $G_t(\mathrm{x}) = g_t$, where $g_i \in K$ are some constants, defines the *connectivity invariants* specified for points $(\mathrm{x}) \in P$ in the linguistic incidence structure I. For elements $(\mathrm{x}_1), (\mathrm{x}_2) \in P$ from the same connectivity component in the graph I_m, the following relations hold: $G_i(\mathrm{x}_1) = G_i(\mathrm{x}_2)$, $i = 1, 2, \ldots, t$. The existence of i such that $G_i(\mathrm{x}_1) \neq G_i(\mathrm{x}_2)$ implies that (x_1) and (x_2) are points from different connected components of the graph I_m.

As a consequence of Proposition 1, ϕ_n^m induce a map on flags of the incidence structure I_m, $\widetilde{\phi}_n^m \colon {}^{\mathcal{F}}I_m \to {}^{\mathcal{F}}I_n$ defined by $\widetilde{\phi}_n^m \colon \{u, v\} \mapsto \{\phi_n^m(u), \phi_n^m(v)\}$. Similarity, as a consequence of Proposition 3, ϕ_M^m induce a map on flags of the incidence structure I_m, $\widetilde{\phi}_M^m \colon {}^{\mathcal{F}}I_m \to {}^{\mathcal{F}}I_M$ defined by $\widetilde{\phi}_M^m \colon \{u, v\} \mapsto \{\phi_M^m(u), \phi_M^m(v)\}$. It is clear that an edge of $\mathrm{L}\Gamma(r, s, m, \mathbb{K})$ corresponds to some flag in ${}^{\mathcal{F}}I_m$. So, we have the following proposition that can be stated as *edges lift to edges.*

Proposition 7. *The maps $\widetilde{\phi}_n^m$ and $\widetilde{\phi}_M^m$ are $|\mathbb{K}|^{m-n}$-to-1 and $|\mathbb{K}|^{m-d}$-to-1 surjections, respectively. Moreover, q^{m-n} and q^{m-d} of $L\Gamma(r, s, m, \mathbb{K})$, which are preimages of a fixed edge of $L\Gamma(r, s, n, \mathbb{K})$ and $L\Gamma(r, s, M, \mathbb{K})$, are pairwise disjoint vertices, respectively.*

Family of linguistic graphs $D(k, K)$ We consider the family of graphs $D(k, K)$, where $k > 2$ is a positive integer, and K is a commutative ring. Such graphs have been considered in [5] in the case $K = \mathbb{F}_q$ (see [6] for the description of connected components). Let P_D and L_D be two copies of Cartesian power $K^{\mathbb{N}}$, where K is the commutative ring, and $\mathbb{N}$ is the set of positive integers. Elements of P_D will be called *points*, and those of L_D *lines.*

To distinguish points from lines, we use parentheses and brackets. If $x \in K^{\mathbb{N}}$, then $(x) \in P_D$ and $[x] \in L_D$. It will be also advantageous to adopt the notation for the coordinates of points and lines introduced in [13] in the case of a 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 a finite number of components is different from zero.

We now define a linguistic incidence structure (P_D, L_D, I_D) defined by an infinite system of equations 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 coordinates hold:

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

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

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

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

(these four relations are defined for $i \geqslant 1$, $p'_{1,1} = p_{1,1}$, $l'_{1,1} = l_{1,1}$). The incidence structure (P_D, L_D, I_D) is denoted by $D(K)$. Now, we will say about the *incidence graph* of (P_D, L_D, I_D), which has the vertex set $P_D \bigcup L_D$ and the edge set consisting of all pairs $\{(p), [l]\}$, for which $(p)I[l]$.

For each positive integer $k \geqslant 2$, we obtain a quotient $(P_{D,k}, L_{D,k}, I_{D,k})$ as follows. First, $P_{D,k}$ and $L_{D,k}$ are obtained from P_D and L_D, respectively, by simply projecting each vector into its k initial coordinates. The incidence $I_{D,k}$ is then defined by imposing $k-1$ first incidence relations and ignoring all others. The incidence graph corresponding to the structure $(P_{D,k}, L_{D,k}, I_{D,k})$ is denoted by $D(k, K)$.

To facilitate the notation in the future results on "*connectivity invariants*", it will be convenient for us to define $p_{-1,0} = l_{0,-1} = p_{1,0} = l_{0,1} = 0$, $p_{0,0} = l_{0,0} = -1$, $p'_{0,0} = l'_{0,0} = -1$, $p'_{1,1} = p_{1,1}$, $l'_{1,1} = l_{1,1}$) and to assume that our equations are defined for $i \geqslant 0$. Note that, for $i = 0$, four above-written conditions are satisfied by every point and line. Moreover, for $i = 1$, the first two equations coincide and give $l_{1,1} - p_{1,1} = l_{1,0}p_{0,1}$.

Let $k \geqslant 6$, $t = [(k+2)/4]$, 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 line). For every r, $2 \leqslant r \leqslant t$, let

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

and $a(u) = (a_2, a_3, \ldots, a_t)$. Similarly, we assume that $a(u) = (a_2, a_3, \ldots, a_t, \ldots)$ for the vertex u of the infinite graph $D(K)$.

Proposition 8. *Let u and v be vertices from the same component of $D(k, K)$. Then $a(u) = a(v)$. Moreover, for any $t-1$ field elements $x_i \in F_q$, $2 \leqslant t \leqslant [(k+2)/4]$, there exists a vertex v of $D(k, K)$, for which $a(v) = (x_2, \ldots, x_t) = (x)$.*

We refer to the first coordinate $x_{1,0} = \rho(\mathrm{x})$ of a point x and the first coordinate $y_{1,0} = \rho(\mathrm{y})$ of a line y as the color of the vertex (point or line). The following property holds for the graph: there exists the unique neighbor $N_t(v)$ of a given vertex v of a given color $t \in K$.

A flag of the incidence system $D(n,K)$ (or $D(K)$) is an unordered pair $\{(\mathrm{x}),[\mathrm{y}]\}$ such that $(\mathrm{x})I[\mathrm{y}]$. Obviously, the totality of flags $FD(n,K)$ $(FD(K))$ of the bipartite flag $D(n,K)$ $(D(K)$, respectively) is isomorphic to the variety K^{n+1}. So, the flag $\{(\mathrm{x}),[\mathrm{y}]\}$ is defined by the tuple $(x_{10}, x_{11}, \ldots, y_{01})$. Note that $N_{y_1}(\{\mathrm{x}\}) = [\mathrm{y}]$.

We consider an operator $N_{P,\alpha}(\{(\mathrm{x}),[\mathrm{y}]\})$, $\alpha \in K$ mapping a flag $\{(\mathrm{x}),[\mathrm{y}]\}$ of the incidence structure $D(n,K)$ (or $D(K)$) into its image $\{(\mathrm{x}'),[\mathrm{y}]\}$, where $(\mathrm{x}') = N_{\rho(\mathrm{y})+\alpha}([\mathrm{y}])$. Similarly, an operator $N_{L,\alpha}(\{(\mathrm{x}),[\mathrm{y}]\})$ maps $\{(\mathrm{x}),[\mathrm{y}]\}$ into $\{(\mathrm{x}), N_{\rho(\mathrm{x})+\alpha}(\mathrm{x})\}$).

Let α_1, $\alpha_2, \ldots, \alpha_k$ and $\beta_1, \beta_2, \ldots, \beta_k$ be chosen to be the random sequences of elements from the commutative ring K. The composition $E = N_{P,\alpha_1}N_{L,\beta_1}N_{P,\alpha_2}N_{L,\beta_2}\ldots N_{P,\alpha_k}N_{L,\beta_k}$ transforms flag $\{(\mathrm{x}),[\mathrm{y}]\}$ into a new flag $\{(\mathrm{x}'),[\mathrm{y}']\}$. The process of computation of $E(\{(\mathrm{x}),[\mathrm{y}]\} = \{(\mathrm{x}'),[\mathrm{y}']\}$ corresponds to a random walk in the expander graph $D(n,K)$ with the original vertex (x) and the final point (x$'$).

Symbolic keys and pseudorandom walks on flag space. Let $V_{s,r,m} = P_{s,m} \cup L_{r,m}$, $I_m = I_m(K)$, $m = 2,3,\ldots$ be a family of linguistic incidence structures with the point set $P_{s,m} = K^{s+m}$ and the line set $L_{s,m} = K^{r+m}$, where the parameters s and r are constants, and K is a fixed commutative ring. The sets of colors for points and lines are K^s and K^r, respectively. We assume that the subset $M = \{i_1, i_2, \ldots, i_d\}$, $d = d(m) \leqslant m$ defines the symplectic quotient I_M for each linguistic structure $I_m = I_m(K)$. Let G_1, G_2, $\ldots$, G_t be the connectivity invariants of the incidence structures I_m.

Let ${}^{\mathcal{F}}I_m$ be the flag relation, and let $\mathcal{F}(V_{s,r,m}) = \mathcal{F}(V_m(K))$ be a variety of flags for the incidence structure I_m. The information on the flag $\{(x),[y]\}$ can be given by the pair $(x) \in$ $\in K^{s+m}$, $\rho(y) \in K^r$ or, alternatively, by the pair $[y] \in K^{r+m}$ and $\rho(x) \in K^s$. So, $\mathcal{F}(V_{s,r,m})$ is isomorphic to K^{m+r+s}.

Let $N_{P,a}$, $a \in K^s$ be the *operator of change of the point of a flag* $F = \{(x),[y]\}$ defined by the rule $N_{P,a}(\{(\mathrm{x}),[\mathrm{y}]\}) = \{(\mathrm{x}'),[\mathrm{y}]\}$, where $(\mathrm{x}')I_m[\mathrm{y}]$ and $\rho(\mathrm{x}') = a$. Similarly, let $N_{L,a}$, $a \in K^s$ be the *operator of change of the line of a flag* $F = \{(x),[y]\}$ specified by the rule $N_{L,b}(\{(\mathrm{x}),[\mathrm{y}]\}) = \{(\mathrm{x}),[\mathrm{y}']\}$, where $[\mathrm{y}']I_m(\mathrm{x})$ and $\rho(\mathrm{y}') = b$. It is clear that the application of a composition of N_{P,a_1}, N_{L,b_1}, N_{P,a_2}, N_{L,b_2}, $\ldots$, N_{P,a_k}, N_{L,b_k} to the flag F corresponds to a walk in our linguistic graph with the starting point (p) or a walk in the graph ${}^{\mathcal{F}}I_m$ with the starting vertex $\{(x),[y]\}$.

Let $F = \{(\mathrm{x}),[\mathrm{y}]\}$ be a general flag of our linguistic structure I_m, i. e., $(\mathrm{x}) = (x_1, x_2, \ldots, x_r,$ $x_{r+1}, x_{r+2}, \ldots, x_{r+m})$, $[\mathrm{y}] = [y_1, y_2, \ldots, y_s, y_{s+1}, y_{s+2}\ldots, y_{s+m}]$ are incident. We assume that x_1, x_2, $\ldots$, x_r, y_1, y_2, $\ldots$, y_s, x_{s+1}, x_{s+2}, $\ldots$, x_{s+m} are the list of independent variables, which give us the entire information on a flag F of the incidence structure I_m. We assume that the connectivity invariants G_1, G_2, $\ldots$, G_t are written in terms of the coordinates of the point (x). We refer to a tuple $\mathrm{Tr}(F) = \langle x_1, x_2, \ldots, x_r, y_1, y_2, \ldots, y_s, G_1(\mathrm{x}), G_2(\mathrm{x}), \ldots, G_t(\mathrm{x})\rangle$ as the *trace of a flag* $F = \{(\mathrm{x}),[\mathrm{y}]\}$, i. e., $\mathrm{Tr}(F) = \langle \rho(\mathrm{x}), \rho(\mathrm{y}), G_1(\mathrm{x}), G_2(\mathrm{x}), \ldots, G_t(\mathrm{x})\rangle$.

We introduce a parameter n by the equality $n = (r+s+t)$. Let D_1, $D_2, \ldots, D_h$, D_{h+1} and E_1, $E_2, \ldots, E_h$ be two lists of elements, where D_i, $E_j \in K[z_1, z_2, \ldots, z_n]$, $i = 1, 2, \ldots, h+1$, $j = 1, 2, \ldots, h$. We refer to concatenation of both lists (writing the second list after the first one) as a *symbolic key*.

We take the flag $F = \{(\mathrm{x}),[\mathrm{y}]\}$ specified by parameters of the kind x_1, x_2, $\ldots$, x_r, y_1, y_2, $\ldots$, y_s, x_{r+1}, $\ldots$, x_{r+m} with trace $\mathrm{Tr}(F) = \langle x_1, x_2, \ldots, x_r, y_1, y_2, \ldots, y_r, G_1(\mathrm{x}), G_2(\mathrm{x}), \ldots, G_t(\mathrm{x})\rangle$. We concatenate all these tuples with preservation of the order and form a string of parameters β_1, $\beta_2, \ldots, \beta_n$ from Q. After that, we compute specializations of the coordinates $d_i = D_i(\mathrm{Tr}(F))$, where $i = 1, 2, \dots, h$, $h+1$ and $e_j = E_j(\mathrm{Tr}(F))$, where $j = 1, 2, \dots, h$ of our symbolic key. For the chosen ring K, this allows us to treat coordinates of the string d_1, $d_2, \dots, d_h$, d_{h+1} as elements of K^r and coordinates of e_1, $e_2, \dots, e_h$ as a string from K^s. The string $(d_1, d_2, \dots, d_h, d_{h+1}, e_1, e_2, \dots, e_h)$ is our *numerical key.*

Finally, we compute the decomposition N of operators N_{P,d_1}, F_{L,e_1}, N_{P,d_2}, N_{L,e_2}, $\dots$, N_{P,d_h}, N_{L,e_h}, $N_{P,e_{d+1}}$. The application of N to the flag F corresponds to a walk in the graph ${}^{\mathcal{F}}I_m$ with the starting point F and the final point $N(F)$.

Note that the colors of the point and the line forming $\check{F} = N(F) = \{\check{(\mathrm{x})}, [\check{\mathrm{y}}]\}$ are $d_{h+1} \in K^s$ and $e_h \in K^r$, respectively. Under certain conditions, we may restore the trace of a flag F from the given F'. We have $G_i(\mathrm{x}) = G_i(\check{\mathrm{x}})$, because both flags are from the same connected component. Additionally,

$$\begin{aligned}
&(\check{x}_1, \check{x}_2, \dots, \check{x}_r) = D_{h+1}(x_1, \dots, x_r, y_1, \dots, y_s, G_1(\check{\mathrm{x}}), \dots, G_t(\check{\mathrm{x}})), \\
&(\check{y}_1, \check{y}_2, \dots, \check{y}_r) = E_h(x_1, \dots, x_s, y_1, \dots, y_s, G_1(\check{\mathrm{x}}), \dots, G_t(\check{\mathrm{x}})).
\end{aligned} \tag{1}$$

We may choose functions D_{h+1} and E_h such that the above-written system of equations has the unique solution independently of the values of $G_i(\mathrm{x}')$, $i = 1, 2, \dots, t$. Obviously, the first choice is a system of equations linear in the variables x_1, x_2, $\dots$, x_r, y_1, y_2, $\dots$, y_s. Then we can reconstruct our walk in the reverse order corresponding to the composition of $N_{P,e_{h-1}}$, $N_{L,d_{h-1}}$, $N_{P,e_{h-2}}$, $\dots$, N_{L,e_1}, N_{P,d_1}.

Multivariate transformations based on symbolic keys. The above-mentioned map defined by a symbolic key has multivariate nature. The plainspace is the totality of tuples $(x_1, x_2, \dots, x_s, y_1, y_2, \dots, y_r, x_{s+r+1}, x_{s+r+2}, \dots, x_{s+r+m})$. For each function $D_i(z_1, z_2, \dots, z_{s+r+t})$, we consider a specialization of the variables $z_1 = x_1$, $z_2 = x_2$, $\dots$, $z_s = x_s$, $z_{s+1} = y_1$, $z_{s+2} = y_2, \dots, z_{s+r} = y_r$, $z_{s+r+1} = G_1(\mathrm{x})$, $z_{s+r+2} = G_2(\mathrm{x}), \dots, z_{s+r+t} = G_t(\mathrm{x})$. In such a way, we construct the function D'_i depending on the general tuple $(x_1, \dots, x_s, y_1, \dots, y_r, x_{r+1}, \dots, x_{r+m})$ of the plainspace. Similarly, we apply the same specialization to each E_i and get the transformation E'_i. The transformations N_{P,D'_i} and N_{L,E'_j} are multivariate bijections on K^{r+s+m}. The formal composition of N_{P,D'_1}, N_{L,E'_1}, N_{P,D'_2}, N_{L,E'_2}, $\dots$, N_{P,D'_h}, N_{L,E'_h}, and $N_{P,D'_{h+1}}$ is a symbolic presentation of the map N.

Algoritm 1. The algorithm of generation of an irreversible multivariate transformation with the side door to the secret numeric key.

1. Choose the most preferable singular linear transformation $T_1 \colon W \to W$ such that $T_1|_{W_1}$ is invertible and $T_1|_{W_2}$ is not invertible, where $W_1 = K^{r+d}$ and $W_2 = K^{m-d}$.

2. Take the tuple $z = (z_1, z_2, \dots, z_k) \in W$ and compute $w = T_1(z)$.

3. Choose the flag symplectic quotient ${}^{\mathcal{F}}I_M$ of a flag linguistic graph ${}^{\mathcal{F}}I_m$ corresponding to $M = \{m_1, m_2, \dots, m_d\}$ with natural order of elements and the incidence structure I_M with a point set $P_{r,M} = K^{\mathbb{N}}$ and a line set $L_{s,M} = K^{\mathbb{N}}$, where a point (x) and a line $[\mathrm{y}]$ are of the kinds $(\mathrm{x}) = (x_1, x_2, \dots, x_r, x_{m_1}, x_{m_2}, \dots, m_d)$ and $[\mathrm{y}] = [y_1, y_2, \dots, y_s, y_{m_1}, y_{m_2}, \dots, m_d]$, respectively.

4. Treat the tuple $w \in W$ as a flag F_1 in the linguistic graph ${}^{\mathcal{F}}I_m$ of the kind

$$F_1 = (x_1, \dots, x_s, y_1, \dots, y_r, x_{r+1}, x_{r+2}, \dots, x_{m_1}, x_{m_1+1}, \dots, x_{m_2}, \dots, x_{m_d}, x_{r+m}).$$

5. Generate the symbolic key corresponding to the symbolic way in the flag linguistic graph ${}^{\mathcal{F}}I^{\pi}_m$, i. e., a list of polynomial functions $D_i(v_1, v_2, \dots, v_{r+s+t})$, $i = 1, 2, \dots, h+1$, $E_j(v_1, v_2, \dots, v_{r+s+t})$, $j = 1, 2, \dots, h$, and compute its specializations $D'_i(F_2)i = 1, 2, \dots, h+1$, $E'_j(F_2)j = 1, 2, \dots, h$ corresponding to the substitution $v_i = x_i$, $i = 1, 2, \dots, r$, $v_{r+j} = y_j$, $j = 1, 2, \dots, s$, $v_{r+s+e} = G_i(F_2)$, $e = 1, 2, \dots, t$.

6. Determine the multivariate transformation N corresponding to the chosen symbolic key, i. e.,

$$N = N_{P,D'_1} N_{L,E'_1} \cdots N_{P,D'_h} N_{L,E_h} N_{P,D'_{h+1}}.$$

7. Compute the flag $F_2 = N(F_1)$ of the graph ${}^{\mathcal{F}}I_m^{\pi}$ and treat it as a tuple $u \in W$.

8. Choose an invertible affine transformation $T_2\colon W \to W$ and compute $\mathrm{c} = T_2(u)$.

9. Using the symbolic computation, determine a multivariate transformation $H\colon W \to W$ as a composition of T_1, N, and T_2. It is clear that the transformation $H\colon W \to W$ is polynomial over K of the kind

$$z_1 \to h_1(z_1, z_2, \dots, z_k),$$

$$z_2 \to h_2(z_1, z_2, \dots, z_k),$$

$$\dots,$$

$$z_k \to h_k(z_1, z_2, \dots, z_k),$$

where

$$h_i \in K[z_1, z_2, \dots, z_k].$$

The general algorithms of the key exchange multivariate protocol based on pseudorandom walks on incidence structures. Key exchange algorithms are used to exchange cryptographic keys between two communicating users (in our case, Alice and Bob). The most popular key exchange protocol was proposed in [7]. A key exchange algorithm enables the communicating users, who do not know each other, to share a secret key over an unsecured communication channel. This secret numerical key can then be used to encrypt any subsequent communication between the two users, by using the encryption and decryption maps defined via a path in the graph. In this new algorithm, the secret key is a pseudorandom walk determined by a list of pseudorandom elements from the commutative ring.

Algoritm 2. The proposed key exchange between two users consists of the following steps:

I. Alice and Bob will determine together

I.1. The free module $W = K^k$ over a commutative ring K, where $k = r + s + m$.

I.2. A linguistic graph $\mathrm{L}\Gamma(r, s, m, \mathbb{K})$ corresponding to the incidence structure I_m.

I.3. The length of a pseudorandom path in the graph I_m of the kind $2h + 1$.

II. Alice should do the following steps:

II.1. Generate a multivariate transformation $H\colon W \to W$ using Algorithm

II.2. Use the symbolic computation and determine a deformed symbolic key $\widetilde{D}_i$, $\widetilde{E}_j \in$ $\in K[z_1, z_2, \dots, z_n]^l$, $i = 1, 2, \dots, h + 1$, $j = 1, 2, \dots, h$ as a composition of the selected transformation T_1 with the chosen symbolic key $\widetilde{D}_i$, $i = 1, 2, \dots, h + 1$, $\widetilde{E}_j$, $j = 1, 2, \dots, h$ used in Algorithm 1.

II.3. Send the determined transformation H and the deformed symbolic key $\widetilde{D}_i$, $i = 1, 2, \dots$, $h + 1$, $\widetilde{E}_j$, $j = 1, 2, \dots, h$ to Bob.

III. Next, Bob should do the following steps:

III.1. Choose a random tuple $\mathrm{v} = (v_1, v_2, \dots, v_k)$, where $v_i \in K$, $i = 1, 2, \dots, k$, compute $\mathrm{w} = H(\mathrm{v})$ and send w to Alice.

III.2. Determine the secret numerical key d_1, $d_2, \ldots, d_{h+1}$, e_1, $e_2, \ldots, e_h$ in the standard way, by using the deformed symbolic key, i. e., $d_1 = \widetilde{D}_1(v)$, …, $h+1 = \widetilde{D}_{h+1}$, $e_1 = \widetilde{E}_{1,}(v)$, …, $y_r = v_r$, $e_h = \widetilde{E}_{h,}(v)$.

IV. Finally, in order to restore the elements of the secret numerical key $d_1, d_2, \ldots,$ d_{h+1}**,** $e_1, e_2, \ldots, e_h$ **from the element** $\mathrm{w} \in W$**, Alice should do the following steps:**

IV.1. Use the invertible affine transformation T_2 to compute $T_2^{-1}(\mathrm{w}) = \mathrm{v}'$ and write it as a flag $F_2 = \{\check{\mathrm{x}}, \check{\mathrm{y}}\}$ from the graph ${}^{\mathcal{F}}I_m^{\pi}$.

IV.2. Compute $G_1(\check{\mathrm{x}})$, $G_2(\check{\mathrm{x}})$, …, $G_t(\check{\mathrm{x}})$ determined by equations (1) for the elements x_1, $x_2, \ldots, x_r$, y_1, $y_2, \ldots, y_s$ forming a flag $F_1 = \{\mathrm{x}, \mathrm{y}\}$.

IV.3. Use the symbolic key and these calculations to determine a secret numerical key as a list of pseudorandom elements d_1, d_2, …, d_h, d_{h+1}, e_1, e_2, …, e_h from K.

Conclusion. We can use our algorithm in the case of linguistic structures $D(m, K)$. The previous section gives the full description of data, which we need for the implementation of our key exchange protocol. The graphs $D(m, K)$ have been used for the construction of a stream cipher (see [9, 10, 11] and references therein). In this case, both algorithms (symmetric one and key exchange protocol) can be used together. It is known that the graphs $D(m, K)$ are good expanders (see [12, 13]). This means that the behavior of pseudorandom walks generated for their use in these algorithms is similar to the behavior of random walks on random graphs (see [8, 14, 15]).

1. *Biggs N. L.* Algebraic graph theory. – Cambridge: Cambridge Univ. Press, 1993. – 324 p.
2. *Moore E. H.* Tactical memoranda // Amer. J. Math. – 1886. – **18**. – P. 264–303.
3. *Ustimenko V.* Maximality of affine groups and hidden graph cryptosystems // J. Alg. Discr. Math. – 2005. – No 1. – P. 133–150.
4. *Ustimenko V.* On walks of variable length in Schubert incidence systems and multivariate flow systems // Dop. NAN Ukrainy. – 2014. – No 3. – P. 55–150.
5. *Lazebnik F., Ustimenko V. A., Woldar A. J.* A new series of dense graphs of high girth // Bull. Amer. Math. Soc. (New Series). – 1995. – **32**, No 1. – P. 73–79.
6. *Lazebnik F., Ustimenko V. A., Woldar A. J.* A characterization of the components of the graphs $D(k, q)$ // Discr. Math. – 1996. – **157**. – P. 271–283.
7. *Diffie M., Hellman M. E.* New directions in cryptography // IEEE Trans. Inform. Theory. – 1976. – **IT – 22**. – P. 644–654.
8. *Hoory S., Linial N., Wigderson A.* Expander graphs and their applications // Bull. Amer. Math. Soc. (New Series). – 2006. – **43**, No 4. – P. 439–561.
9. *Ustimenko V.* Coordinatisation of trees and their quotients // Voronoj's Impact on Modern Science. – Kiev: Institute of Mathematics, 1998. – Vol. 2. – P. 125–152.
10. *Ustimenko V.* CRYPTI: Graphs as tools for symmetric encryption // Lecture Notes in Computer Science, Proceedings of AAECC-14 Symposium on Applied Algebra, Algebraic Algorithms and Error Correction Codes. – Berlin: Springer, 2001. – P. 278–286.
11. *Kotorowicz J., Ustimenko V.* On the implementation of cryptoalgorithms based on algebraic graphs over some commutative rings // Condens. Matt. Phys. – 2008. – **11**, No 2. – P. 347–360.
12. *Ustimenko V.* Graphs with special arcs and cryptography // Acta Appl. Math. – 2002. – **74**. – P. 117–153.
13. *Ustimenko V.* On a group theoretical constructions of expanding graphs // J. Alg. Discr. Math. – 2003. – No 3. – P. 102–109.
14. *Lovász L.* Random walks on graphs: A survey // Bolyai Soc. Math. Studies. – 1993. – **2**. – P. 1–46.
15. *Romańczuk U., Ustimenko V.* On extremal graph theory. Explicit algebraic constructions of extremal graphs and corresponding Turing encryption machines // Artificial Intelligence, Evolutionary Computing and Metaheuristics. – Berlin: Springer, 2013. – P. 257–285.

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

Received 16.07.2014

У. Романчик-Полубець, В. О. Устименко

Про нові протоколи обміну ключами, що базуються на псевдовипадкових блуканнях в структурі інциденції

Запропоновано нові протоколи обміну ключами, що формулюються в термінах алгебраїчної криптографії від багатьох змінних та базуються на створенні кореспондентами спільного блукання в лінгвістичному графі. Алгоритм детально описано у випадку відомої родини графів великого обгорту, що задається нелінійними рівняннями над скінченним полем.

У. Романчик-Полубец, В. А. Устименко

О новых протоколах обмена ключами, основанных на псевдослучайных блужданиях в инцидентностной структуре

Предложены новые протоколы обмена ключами, сформулированные в терминах алгебраической криптографии от многих переменных и основанные на создании корреспондентами общего блуждания в лингвистическом графе. Алгоритм детально описан в случае известной семьи графов большого захвата, заданной нелинейными уравнениями над конечным полем.