ALBANIAN JOURNAL OF MATHEMATICS
Volume 8, Number 1, Pages 37–45
ISSN: 1930-1235; (**2014**)

ON STREAM CIPHER BASED ON FAMILY OF GRAPHS $\widetilde{D(n,q)}$ OF INCREASING GIRTH

Monika Polak
University of Maria Curie Sklodowska
Lublin, Poland
Email: monika.katarzyna.polak@gmail.com

Vasyl Ustimenko
University of Maria Curie Sklodowska
Lublin, Poland
Email: vasyl@hektor.umcs.lublin.pl

Abstract. In this short paper we present symmetric encryption algorithm based on family of bipartite graphs $\widetilde{D(n,q)}$. It is a fast stream cipher with computation speed $O(n)$ for the key of fixed length. If the key is linear function from n the efficiency is $O(n^2)$. Encryption map has a multivariate nature, so the security level can be evaluated via degrees and other parameters of corresponding multivariate polynomials. We show that the degree of graph based encryption maps are growing with the growth of the dimension of the plain space. Therefore this algorithm is resistant to linearization attacks.

1. Introduction

Multivariate polynomials are just polynomials in several variables. In this article we are interested in polynomials over finite fields. Though multivariate polynomial cryptography is a potential candidate for post quantum cryptography, schemes based on it are mostly used for digital signature purpose only; see [1] for further details. Multivariate cryptography is proposed as a tool for public key cryptography, but only few encryption schemes were developed untill now, see for example [2].

In this paper we explore the possibility of using multivariate polynomial systems for symmetric encryption. Main security assumption of presented symmetric scheme is backed by the NP-hardness of the problem to solve nonlinear system of equations over a finite field. There are many different algorithms where graphs are used. Graph based algorithms are used, in particular, in cryptography, coding theory, car navigation systems, sociology, mobile robotics and even in computer games. Families of graphs can be used to create multivariate polynomials for cryptographic schemes. Graphs were first used in cryptography by Ustimenko in [3, 4]. There are other examples of crypto-systems based on graphs $D(n,q)$, which were introduced

2000 *Mathematics Subject Classification.* 05C90 and 94C15 and 94A60 .
Key words and phrases. data security and stream cipher and graph based algorithm and multivariate transformations.

©2014 albanian-j-math.com

in [5]. Multivariate maps used in this algorithms were investigated in [6–8]. A. Wróblewska proved that maps related to $D(n,q)$ are cubical; see [7]. Computer simulations of multivariate maps based on graph $D(n,K)$ are designed in [9, 10].

2. Families of graphs

For our purposes we are interested only in simple graphs. *Simple graph* is a undirected graph containing no graph loops or multiple edges. By $\Gamma(V,E)$ we denote graph where V is a set of vertices and E is a set of edges. We say that graph is *connected* if for arbitrary pair of vertices $v_1, v_2 \in V$ there is a path from v_1 to v_2. The *girth* of a connected, simple graph is a length of the shortest cycle in a graph. Graph $\Gamma(V = V_1 \cup V_2, E)$ is *bipartite* if set of vertices can be divided into two sets V_1 and V_2 ($V_1 \cap V_2 = \emptyset$) such that every edge connects a vertex in V_1 to one in V_2.

We refer to bipartite graph $\Gamma(V_1 \cup V_2, E)$ as *regular* one if every vertex from V_1 and V_2 has the same constant degree. Mentioned definitions and more facts from Simple Graphs Theory can be find in [11].

The following interpretation of family of graphs $D(n,q)$ can be find in [5]. Let $\mathbb{F}_q$ be a finite field. Firstly, let us recall the definition of graph $D(q)$ corresponding to infinite incidence structure (P,L,I), where P is collection of points and L is collection of lines. By I we denote the incidence relation for this graph. Let us to use the notions for points and lines introduced in [5]:

$$(p) = (p_{1,0}, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, p'_{2,2}, p_{2,3}, ..., p_{i,i}, p'_{i,i}, p_{i,i+1}, p_{i+1,1}...),$$
$$[l] = [l_{0,1}, l_{1,1}, l_{1,2}, l_{2,1}, l_{2,2}, l'_{2,2}, l_{2,3}, ..., l_{i,i}, l'_{i,i}, l_{i,i+1}, l_{i+1,1}...].$$

Two types of brackets allow us to distinguish points and lines. Points and lines are elements of two copies of the vector space over $\mathbb{F}_q$. In an infinite incidence structure (P,L,I) the point (p) is incident with the line $[l]$, and we write $(p)I[l]$, if the following relations between their coordinates hold:

$$\begin{cases} l_{1,1} - p_{1,1} = l_{0,1}p_{1,0} \\ l_{1,2} - p_{1,2} = l_{1,1}p_{1,0} \\ l_{2,1} - p_{2,1} = l_{0,1}p_{1,1} \\ l_{i,i} - p_{i,i} = l_{0,1}p_{i-1,i}, \\ l'_{i,i} - p'_{i,i} = l_{i,i-1}p_{1,0} \\ l_{i,i+1} - p_{i,i+1} = l_{i,i-1}p_{1,0} \\ l_{i+1,i} - p_{i+1,i} = l_{0,1}p'_{i,i} \end{cases} \tag{1}$$

where $i \geq 2$.

The set of vertices of infinite incidence structure (P,L,I) is $V = P \cup L$ and the set of edges E consisting of all pairs $\{(p),[l]\}$ for which $(p)I[l]$. Bipartite graphs $D(n,q)$ have partition sets P_n (collection of points) and L_n (collection of lines) isomorphic to vector space $\mathbb{F}_q^n$, where $n \in \mathbb{N}_+$. For each positive integer $n > 2$ the finite incidence structures (P_n, L_n, I_n) can be obtained in a following way. P_n and L_n are obtained from P and L, respectively, by projecting each vector onto its n initial coordinates with respect to the natural order. The incidence relations I_n are then defined by imposing the first $n-1$ incidence equations and ignoring all others. The graphs corresponding to the finite incidence structures (P_n, L_n, I_n) are denoted by $D(n,q)$.

 ©2014 albanian-j-math.com

The family of graphs $\widetilde{D(n,q)}$ was firstly introduced in [5] as a tool in construction of family of graphs $D(n,q)$. The applications of this family of graphs weren't contemplated before. In the construction of the family of graphs graphs $\widetilde{D(q)}$ Cartan matrix

$$\begin{pmatrix} 2 & -2 \\ -2 & 2 \end{pmatrix}$$

and Lie algebra are used. Lie algebra is a vector space over finite field with the bilinear product satisfying certain properties (see [12]). Let us to use the analogical notions for points and lines in graph $\widetilde{D(q)}$:

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

In infinite incidence structure $(\widetilde{P, L, I})$ the point (p) is incident with the line $[l]$, and we write $(p)I[l]$, if the following relations between their coordinates hold:

$$(2) \qquad \begin{cases} l_{1,1} - p_{1,1} = l_{0,1}p_{1,0} \\ l_{1,2} - p_{1,2} = l_{0,1}p_{1,1} \\ l_{2,1} - p_{2,1} = l_{1,1}p_{1,0} \\ l_{i,i} - p_{i,i} = l_{0,1}p_{i,i-1} + l_{i-1,i}p_{1,0} \\ l_{i,i+1} - p_{i,i+1} = l_{0,1}p_{i,i} \\ l_{i+1,i} - p_{i+1,i} = l_{i,i}p_{1,0} \end{cases}$$

where $i \geq 2$.

The graphs $\widetilde{D(n,q)}$ corresponding to the finite incidence structures $(\widetilde{P_n, L_n}, I_n)$ can be obtained by the same way as for graphs $D(n,q)$.

Graphs from families $D(n,q)$ and $\widetilde{D(n,q)}$ are bipartite, q-regular, sparse and without short cycles. The girth in graphs from described families increasing with growing n. In fact $D(n,q)$ is a family of graphs of large girth and there is a conjecture that $\widetilde{D(n,q)}$ is another family of graphs of large girth.

3. Algorithm

The family of graphs $\widetilde{D(n,q)}$ can be use as a tool for symmetric encryption. Firstly let $v = (v_1, v_2, v_3, v_4, \ldots, v_n) \in \widetilde{D(n,q)}$ (or $v = [v_1, v_2, v_3, v_4, \ldots, v_n] \in \widetilde{D(n,q)}$) and $N_t(v)$ be the operator of taking neighbor of vertex v where first coordinate is $v_1 + t$:

$$\begin{aligned}N_t(v_1, v_2, v_3, v_4, v_5) &\to [v_1 + t, *, *, *, *],\\ N_t[v_1, v_2, v_3, v_4, v_5] &\to (v_1 + t, *, *, *, *).\end{aligned}$$

The remaining coordinates can be determined uniquely using relations in Eq. (2). We can construct multivariate map F in a following way:

$N_{t_1}(\overline{x})$ is given by:

$$\begin{bmatrix} x_1+t_1 \\ x_2+x_1(x_1+t_1) \\ x_3+x_2(x_1+t_1) \\ x_4+x_1x_2+x_1^2(x_1+t_1) \\ x_5+x_1x_3+(x_1x_2+x_4)(x_1+t_1) \\ x_6+x_5(x_1+t_1) \\ x_7+x_1x_5+x_1^2x_3+(x_1^2x_2+x_1x_4)(x_1+t_1) \\ \vdots \\ x_{3i+5}+x_1x_{3i+3}+(x_1x_{3i+2}+x_{3i+4})(x_1+t_1) \\ x_{3i+6}+x_{3i+5}(x_1+t_1) \\ x_{3i+7}+x_1x_{3i+5}+x_1^2x_{3i+3}+(x_1^2x_{3i+2}+x_1x_{3i+4})(x_1+t_1) \\ \vdots \\ {}_1f_n(x_1,x_2,\ldots,x_n) \end{bmatrix} = \begin{bmatrix} {}_{t_1}x_1 \\ {}_{t_1}x_2 \\ {}_{t_1}x_3 \\ {}_{t_1}x_4 \\ {}_{t_1}x_5 \\ {}_{t_1}x_6 \\ {}_{t_1}x_7 \\ \vdots \\ {}_{t_1}x_{3i+5} \\ {}_{t_1}x_{3i+6} \\ {}_{t_1}x_{3i+7} \\ \vdots \\ {}_{t_1}x_n \end{bmatrix}$$

We have $N_{t_2}[\overline{{}_{t_1}x}]$ given by:

$$\begin{pmatrix} {}_{t_1}x_1+t_2 \\ x_2-(t_1+t_2)_{t_1}x_1 \\ x_3+(t_1+t_2)_{t_1}x_1^2 \\ x_4-(t_1+t_2)_{t_1}x_2 \\ x_5+({}_{t_1}x_1^2x_1-x_3)(t_1+t_2) \\ x_6-({}_{t_1}x_1^2x_1-x_3)_{t_1}x_1(t_1+t_2) \\ x_7-(t_1+t_2)_{t_1}x_5 \\ \vdots \\ x_{3i+5}+({}_{t_1}x_1{}^2x_{3i+1}+x_{1t_1}x_{1t_1}x_{3i}-x_{3i+3})(t_1+t_2) \\ x_{3i+6}-({}_{t_1}x_1{}^2x_{3i+1}+x_{1t_1}x_{1t_1}x_{3i}-x_{3i+3})_{t_1}x_1(t_1+t_2) \\ x_{3i+7}-(t_1+t_2)_{t_1}x_{3i+5} \\ \vdots \\ {}_2f_n(x_1,x_2,\ldots,x_n) \end{pmatrix} = \begin{pmatrix} {}_{t_2}x_1 \\ {}_{t_2}x_2 \\ {}_{t_2}x_3 \\ {}_{t_2}x_4 \\ {}_{t_2}x_5 \\ {}_{t_2}x_6 \\ {}_{t_2}x_7 \\ \vdots \\ {}_{t_2}x_{3i+5} \\ {}_{t_2}x_{3i+6} \\ {}_{t_2}x_{3i+7} \\ \vdots \\ {}_{t_2}x_n \end{pmatrix}$$

$N_{t_3}(\overline{{}_{t_2}x})$ is given by:

$$\begin{bmatrix} {}_{t_2}x_1+t_3 \\ {}_{t_1}x_2+(t_2+t_3)_{t_2}x_1 \\ {}_{t_1}x_3+(t_2+t_3)_{t_2}x_2 \\ {}_{t_1}x_4+(t_2+t_3)_{t_2}x_1^2 \\ {}_{t_1}x_5+(t_2+t_3)({}_{t_1}x_4-{}_{t_1}x_{1_{t_2}}x_1^2) \\ {}_{t_1}x_6+(t_2+t_3)_{t_2}x_5 \\ {}_{t_1}x_7+({}_{t_1}x_4-{}_{t_1}x_{1_{t_2}}x_1^2)(t_2+t_3)_{t_2}x_1 \\ \vdots \\ {}_{t_1}x_{3i+5}+(t_2+t_3)({}_{t_1}x_{3i+4}-{}_{t_2}x_{1t_2}x_{3i+1t_1}x_1-{}_{t_1}x_{3i_{t_2}}x_2^2) \\ {}_{t_1}x_{3i+6}+(t_2+t_3)_{t_2}x_{3i+5} \\ {}_{t_1}x_{3i+7}+(t_2+t_3)({}_{t_1}x_{3i+4}-{}_{t_2}x_{1t_2}x_{3i+1t_1}x_1-{}_{t_1}x_{3it_2}x_1{}^2)_{t_2}x_1 \\ \vdots \\ {}_3f_n(x_1,x_2,\ldots,x_n) \end{bmatrix} = \begin{bmatrix} {}_{t_3}x_1 \\ {}_{t_3}x_2 \\ {}_{t_3}x_3 \\ {}_{t_3}x_4 \\ {}_{t_3}x_5 \\ {}_{t_3}x_6 \\ {}_{t_3}x_7 \\ \vdots \\ {}_{t_3}x_{3i+5} \\ {}_{t_3}x_{3i+6} \\ {}_{t_3}x_{3i+7} \\ \vdots \\ {}_{t_3}x_n \end{bmatrix}$$

 ©2014 albanian-j-math.com

$N_{t_4}\,[\overline{{}_{t_3}x}]$ is

$$\begin{pmatrix} {}_{t_3}x_1 + t_4 \\ {}_{t_2}x_2 - (t_3+t_4)_{t_3}x_1 \\ {}_{t_2}x_3 + (t_3+t_4)_{t_3}x_1^2 \\ {}_{t_2}x_4 - (t_3+t_4)_{t_3}x_2 \\ {}_{t_2}x_5 + ({}_{t_3}x_1^2{}_{t_2}x_1 - {}_{t_2}x_3)(t_3+t_4) \\ {}_{t_2}x_6 - ({}_{t_3}x_1^2{}_{t_2}x_1 - {}_{t_2}x_3)_{t_3}x_1(t_3+t_4) \\ {}_{t_2}x_7 - (t_3+t_4)_{t_3}x_5 \\ \vdots \\ {}_{t_2}x_{3i+5} + ({}_{t_3}x_1^2{}_{t_2}x_{3i+1} + {}_{t_3}x_1{}_{t_2}x_1{}_{t_3}x_{3i} - {}_{t_2}x_{3i+3})(t_3+t_4) \\ {}_{t_2}x_{3i+6} - ({}_{t_3}x_1^2{}_{t_2}x_{3i+1} + {}_{t_3}x_1{}_{t_2}x_1{}_{t_3}x_{3i} - {}_{t_2}x_{3i+3})_{t_3}x_1(t_3+t_4) \\ {}_{t_2}x_{3i+7} - (t_3+t_4)_{t_3}x_{3i+5} \\ \vdots \\ {}_4f_n(x_1,x_2,\ldots,x_n) \end{pmatrix} = \begin{pmatrix} {}_{t_4}x_1 \\ {}_{t_4}x_2 \\ {}_{t_4}x_3 \\ {}_{t_4}x_4 \\ {}_{t_4}x_5 \\ {}_{t_4}x_6 \\ {}_{t_4}x_7 \\ \vdots \\ {}_{t_4}x_{3i+5} \\ {}_{t_4}x_{3i+6} \\ {}_{t_4}x_{3i+7} \\ \vdots \\ {}_{t_4}x_n \end{pmatrix}$$

and $N_{t_5}\,(\overline{{}_{t_4}x})$

$$\begin{bmatrix} {}_{t_4}x_1 + t_5 \\ {}_{t_3}x_2 + (t_4+t_5)_{t_4}x_1 \\ {}_{t_3}x_3 + (t_4+t_5)_{t_4}x_2 \\ {}_{t_3}x_4 + (t_4+t_5)_{t_4}x_1^2 \\ {}_{t_3}x_5 + (t_4+t_5)({}_{t_3}x_4 - {}_{t_3}x_1{}_{t_4}x_1^2) \\ {}_{t_3}x_6 + (t_4+t_5)_{t_4}x_5 \\ {}_{t_3}x_7 + ({}_{t_3}x_4 - {}_{t_3}x_1{}_{t_4}x_1^2)(t_4+t_5)_{t_4}x_1 \\ \vdots \\ {}_{t_3}x_{3i+5} + (t_4+t_5)({}_{t_3}x_{3i+4} - {}_{t_4}x_1{}_{t_4}x_{3i+1}{}_{t_3}x_1 - {}_{t_3}x_{3i}{}_{t_4}x_1^2) \\ {}_{t_3}x_{3i+6} + (t_4+t_5)_{t_4}x_{3i+5} \\ {}_{t_3}x_{3i+7} + (t_4+t_5)({}_{t_3}x_{3i+4} - {}_{t_4}x_1{}_{t_4}x_{3i+1}{}_{t_3}x_1 - {}_{t_3}x_{3i}{}_{t_4}x_1^2)_{t_4}x_1 \\ \vdots \\ {}_5f_n(x_1,x_2,\ldots,x_n) \end{bmatrix} = \begin{bmatrix} {}_{t_5}x_1 \\ {}_{t_5}x_2 \\ {}_{t_5}x_3 \\ {}_{t_5}x_4 \\ {}_{t_5}x_5 \\ {}_{t_5}x_6 \\ {}_{t_5}x_7 \\ \vdots \\ {}_{t_5}x_{3i+5} \\ {}_{t_5}x_{3i+6} \\ {}_{t_5}x_{3i+7} \\ \vdots \\ {}_{t_5}x_n \end{bmatrix}$$

and so on. Operator N_{t_k} works as follows:

$$\begin{aligned} {}_{t_{k-1}}x_1 &\longrightarrow {}_kf_1(x_1,x_2,\ldots,x_n), \\ {}_{t_{k-1}}x_2 &\longrightarrow {}_kf_2(x_1,x_2,\ldots,x_n), \\ {}_{t_{k-1}}x_3 &\longrightarrow {}_kf_3(x_1,x_2,\ldots,x_n), \\ {}_{t_{k-1}}x_4 &\longrightarrow {}_kf_4(x_1,x_2,\ldots,x_n), \\ {}_{t_{k-1}}x_5 &\longrightarrow {}_kf_5(x_1,x_2,\ldots,x_n), \\ {}_{t_{k-1}}x_6 &\longrightarrow {}_kf_6(x_1,x_2,\ldots,x_n), \\ {}_{t_{k-1}}x_7 &\longrightarrow {}_kf_7(x_1,x_2,\ldots,x_n), \\ &\vdots \\ {}_{t_{k-1}}x_n &\longrightarrow {}_kf_n(x_1,x_2,\ldots,x_n). \end{aligned}$$

If we calculate the next few vectors we see a regularity and so we can formulate general formulas for functions f_i which are depend from k. Let $l = 2,3,4,\ldots$ then:

$$N_{t_{2l+1}}({}_{2l}x_1,\,{}_{2l}x_2,\,{}_{2l}x_3,\ldots,{}_{2l}x_n) \longrightarrow$$

$$\begin{bmatrix} {}_{t_{2l}}x_1 + t_{2l+1} \\ {}_{t_{2l-1}}x_2 + (t_{2l} + t_{2l+1})t_{2l}x_1 \\ {}_{t_{2l-1}}x_3 + (t_{2l} + t_{2l+1})t_{2l}x_2 \\ {}_{t_{2l-1}}x_4 + (t_{2l} + t_{2l+1})t_{2l}x_1^2 \\ {}_{t_{2l-1}}x_5 + (t_{2l} + t_{2l+1})({}_{t_{2l-1}}x_4 - t_{2l-1}x_1 t_{2l}{x_1}^2) \\ {}_{t_{2l-1}}x_6 + (t_{2l} + t_{2l+1})t_{2l}x_5 \\ {}_{t_{2l-1}}x_7 + ({}_{t_{2l-1}}x_4 - t_{2l-1}x_1 {}_{t_{2l}}x_1^2)(t_{2l} + t_{2l+1})t_{2l}x_1 \\ \vdots \\ {}_{t_{2l-1}}x_{3i+5} + (t_{2l} + t_{2l+1})({}_{t_{2l-1}}x_{3i+4} - t_{2l}x_1 t_{2l}x_{3i+1} {}_{t_{2l-1}}x_1 - t_{2l-1}x_{3i} {}_{t_{2l}}x_1^2) \\ {}_{t_{2l-1}}x_{3i+6} + (t_{2l} + t_{2l+1})t_{2l}x_{3i+5} \\ {}_{t_{2l-1}}x_{3i+7} + (t_{2l} + t_{2l+1})({}_{t_{2l-1}}x_{3i+4} - t_{2l}x_1 {}_{t_{2l}}x_{3i+1} t_{2l-1}x_1 - t_{2l-1}x_{3i} {}_{t_{2l}}x_1^2)t_{2l}x_1 \\ \vdots \\ {}_{2l+1}f_n(x_1, x_2, \dots, x_n) \end{bmatrix} = [\overline{t_{2l+1}x}],$$

$$N_{t_{2l}}[{}_{2l-1}x_1, {}_{2l-1}x_2, {}_{2l-1}x_3, \dots, {}_{2l-1}x_n] \longrightarrow$$

$$\begin{pmatrix} {}_{t_{2l-1}}x_1 + t_{2l} \\ {}_{t_{2l-2}}x_2 - (t_{2l-1} + t_{2l})t_{2l-1}x_1 \\ {}_{t_{2l-2}}x_3 + (t_{2l-1} + t_{2l})t_{2l-1}x_1^2 \\ {}_{t_{2l-2}}x_4 - (t_{2l-1} + t_{2l})t_{2l-1}x_2 \\ {}_{t_{2l-2}}x_5 + ({}_{t_{2l-1}}x_1^2 t_{2l-2}x_1 - t_{2l-2}x_3)(t_{2l-1} + t_{2l}) \\ {}_{t_{2l-2}}x_6 - ({}_{t_{2l-1}}x_1^2 t_{2l-2}x_1 - t_{2l-2}x_3)t_{2l-1}x_1(t_{2l-1} + t_{2l}) \\ {}_{t_{2l-2}}x_7 - (t_{2l-1} + t_{2l})t_{2l-1}x_5 \\ \vdots \\ {}_{t_{2l-2}}x_{3i+5} + ({}_{t_{2l-1}}x_1^2 x_{3i+1} + t_{2l-1}x_1 t_{2l-2}x_1 t_{2l-1}x_{3i} - t_{2l-2}x_{3i+3})(t_{2l-1} + t_{2l}) \\ {}_{t_{2l-2}}x_{3i+6} - ({}_{t_{2l-1}}x_1^2 x_{3i+1} + t_{2l-1}x_1 t_{2l-2}x_1 t_{2l-1}x_{3i} - t_{2l-2}x_{3i+3})t_{2l-1}x_1(t_{2l-1} + t_{2l}) \\ {}_{t_{2l-2}}x_{3i+7} - (t_{2l-1} + t_{2l})t_{2l-1}x_{3i+5} \\ \vdots \\ {}_{2l}f_n(x_1, x_2, \dots, x_n) \end{pmatrix} = (\overline{t_{2l}x}).$$

Denote the composition of $N_{t_1} \circ N_{t_2} \circ N_{t_3} \dots \circ N_{t_k}$ as $N_{t_1,t_2,\dots,t_k}$. It is easy to check that if $N_{t_1,t_2,\dots,t_k}(\bar{x}) = \bar{y}$ then $N_{-t_k,-t_{k-1},\dots,-t_1}(\bar{y}) = \bar{x}$.

The following

$$N_{t_1,t_2,\dots,t_k}(x_1, x_2, \dots x_n) \to ({}_k f_1, {}_k f_2, \dots, {}_k f_n),$$

is a polynomial transformation of $\mathbb{F}_q^n$ into itself such that

$$\begin{aligned} x_1 &\longrightarrow {}_k f_1(x_1, x_2, \dots, x_n), \\ x_2 &\longrightarrow {}_k f_2(x_1, x_2, \dots, x_n), \\ &\vdots \\ x_n &\longrightarrow {}_k f_n(x_1, x_2, \dots, x_n). \end{aligned}$$

Computations show that $\deg_k f_i$ is growing independent from the choice of string $t_1, t_2, \dots, t_k$.

If $\mathrm{char}\mathbb{F}_q \neq 2$ then graph $\widetilde{D(n,q)}$ is connected and there exist a path dependent of the choice of $t_1, t_2, \dots, t_k$ conducting one vertex (x) to another one (y).

Let S be a matrix containing degrees of polynomials ${}_k f_{i+1}$, for $i = 1, 2, \dots, n-1$, depending on the length of the password k. Position $s_{i,j}$ shows the degree of polynomial ${}_k f_{i+1}$ if the used password is of length j. The first 5 rows (for $n = 2, 3, 4, 5, 6$) for matrix S are completed as follows: $s_{1,l} = s_{2,l} = 2$, $s_{3,2l-1} = 3$, $s_{3,2l} = 2$, $s_{4,l} = 3$, $s_{5,2l} = 4$, $s_{5,2l+1} = 3$ and the first column corresponding to

 ©2014 albanian-j-math.com

TABLE 1. Table contains degree of polynomials ${}_kf_n$ for different length k of key parameter t

n \ k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	...
2	2	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	...
3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	...
4	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	...
5	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	...
6	2	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	...
7	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	...
8	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	...
9	2	5	4	5	4	5	4	5	4	5	4	5	4	5	4	5	4	5	4	5	...
10	4	3	5	4	5	4	5	4	5	4	5	4	5	4	5	4	5	4	5	4	...
11	3	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	...
12	2	5	4	6	5	6	5	6	5	6	5	6	5	6	5	6	5	6	5	6	...
13	4	3	6	5	6	5	6	5	6	5	6	5	6	5	6	5	6	5	6	5	...
14	3	4	5	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	...
15	2	5	4	7	6	7	6	7	6	7	6	7	6	7	6	7	6	7	6	7	...
16	4	3	6	5	7	6	7	6	7	6	7	6	7	6	7	6	7	6	7	6	...
17	3	4	5	6	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	...
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋱

$k = 1$ is completed according to the scheme: $s_{3l+1,1} = 3$, $s_{3l+2,2} = 2$, $s_{3l+3,3} = 4$, $l = 1, 2, 3 \ldots$. The the remaining positions in the matrix S can be completed recursively:

$$\begin{aligned}
s_{3l+3,2l} &= s_{3l+3-2,2l-1} = s_{3l+1,2l-1},\\
s_{3l+3,2l+1} &= s_{3l+3-2,2l+1} + 1 = s_{3l+1,2l+1} + 1,\\
s_{3l+4,2l} &= s_{3l+4-5,2l-1} + 2 = s_{3l-1,2l-1} + 2,\\
s_{3l+4,2l+1} &= s_{3l+4-4,2l+1-1} + 2 = s_{3l,2l} + 2,\\
s_{3l+5,2l} &= s_{3l+5-1,2l} + 1 = s_{3l+1,2l} + 1,\\
s_{3l+5,2l+1} &= s_{3l+5-1,2l+1-1} = s_{3l+4,2l},
\end{aligned}$$

where $l = 1, 2, 3, \ldots$.

Let L_1 and L_2 be sparse affine transformation of the vector space $\mathbb{F}_q^n$

$$\begin{aligned}
L_1 &= T_{A,b} : \bar{x} \longrightarrow \bar{x}A + b,\\
L_2 &= T_{C,d} : \bar{x} \longrightarrow \bar{x}C + d,
\end{aligned}$$

where $A = \left[a_{i,j}\right]$ and $C = \left[c_{i,j}\right]$ are $n \times n$ matrices with $a_{i,j}, c_{i,j} \in \mathbb{F}_q$, $|A| \neq 0$ and $|C| \neq 0$. It is clear that

$$\begin{aligned}
L_1^{-1} &= T_{A,b}^{-1} = T_{A^{-1},-bA^{-1}},\\
L_2^{-1} &= T_{C,d}^{-1} = T_{C^{-1},-dC^{-1}}.
\end{aligned}$$

Alice and Bob agree private encryption key $K_e = (L_1, L_2, \mathrm{t} = (t_1, t_2, \ldots, t_k), n)$, where $t_{i+1} \neq -t_i$ for $i = 1, \ldots, k-1$ and they must keep the key in secret. Messages are written using characters belonging to the alphabet $\mathbb{F}_q$. To encode they use the composition:

$$F = L_1 \circ N_{t_1,t_2,\ldots,t_{2s}} \circ L_2 = L_1 \circ N_{t_1} \circ N_{t_2} \circ N_{t_3} \ldots \circ N_{t_k} \circ L_2.$$

Alice and Bob can use their knowledge about quadruple (L_1, L_2, t,n) for the decryption. The decryption map is of the form:

$$L_2^{-1} \circ N_{-t_k,-t_{k-1},\ldots,-t_1} \circ L_1^{-1}.$$

©2014 albanian-j-math.com

Let $q = p^m$, where p is prime number. Cipher-text before transmitting should be rewritten in alphabet $\mathbb{F}_p$ to hide key parameter n.

Let $g(n,k)$ denote the degree of polynomial ${}_kf_n$. If k is fixed $\lim\limits_{n\to\infty} g(n,k) = k+3$ and if n is fixed then $\lim\limits_{k\to\infty} g(n,k) = \left\lfloor \frac{n}{3} \right\rfloor + 2$. We propose to use key parameter $t = (t_1, t_2, \ldots, t_k)$ of length $k = \alpha n + \beta$, $\alpha \in (0,1)$. This choice of k allows us to create multivariate map F of unbounded degree.

Theorem 3.1. *In password is of length $k = \alpha n + \beta \in \mathbb{N}$ then degree (maximal degree of monomial) of multivariate map F:*

$$\begin{aligned} x_1 &\longrightarrow {}_kf_1(x_1, x_2, \ldots, x_n), \\ x_2 &\longrightarrow {}_kf_2(x_1, x_2, \ldots, x_n), \\ &\vdots \\ x_n &\longrightarrow {}_kf_n(x_1, x_2, \ldots, x_n) \end{aligned}$$

and is unbounded:

$$\deg F_{\mathrm{t},n} = \deg F(L_1, L_2, \mathrm{t}, n, \mathbb{F}_q) = g(n,k)$$

and

$$\lim_{k\to\infty, n\to\infty} g(n,k) = \infty$$

Proof. The proof in a natural way follows from recursive equations (3) and mathematical induction. □

For fixed L_1, L_2 and $2k \leq g(\widetilde{D(n,q)})$ different keys produce distinct cipher-text ($g(\widetilde{D(n,q)})$ is the girth of graph). The encoding complexity is $O(n^2)$. It is impractical to decrypt a message on the basis of the cipher-text and knowledge of the encryption/decryption algorithm. We do not need to keep the algorithm secret. To decrypt a message without knowledge of secret key we need to solve nonlinear system of equations over finite field (the maximum degree of this polynomials is keep in secret). According to Theorem 1 the degree of map F is unbounded if key parameter t is of length $k = \alpha n + \beta$. The $\deg F^{-1} = \deg F$ so Linearization Attacks on this symmetric-key algorithm are impossible. Solving such system of equation is a NP-hard problem in general.

Remark 3.2. *One can try Dijkstra's algorithm of finding the shortest pass between plaintext and cipher-text. Notice that its complexity is $O(v \log v)$, but here v is exponential q^n. Therefore we get worse complexity then even brute force search via the key space.*

References

[1] Ding J., Gower J. E., Schmidt D. S., *Multivariate Public Key Cryptosystems*, 260. Springer, Advances in Information Security, Vol. 25, (2006)

[2] Koichi Sakumoto, *Public-Key Identification Schemes Based on Multivariate Cubic Polynomials*, in Lecture Notes in Computer Science, Vol. 7293, pp 172–189 (2012)

[3] Ustimenko V., *Coordinatisation of Trees and their Quotients*, in the "Voronoj's Impact on Modern Science", Kiev, Institute of Mathematics, Vol. 2, pp 125–152 (1998)

[4] Ustimenko V., *CRYPTIM: Graphs as Tools for Symmetric Encryption*, Lecture Notes in Computer Science, Springer, Vol. 2227, pp 278–287 (2001)

[5] Lazebnik F., Ustimenko V. A. and Woldar A. J., *A New Series of Dense Graphs of High Girth*, Bull (New Series) of AMS, Vol.32, N1, pp 73–79 (1995)

 ©2014 albanian-j-math.com

[6] Ustimenko V. *Maximality of affine group and hidden graph cryptosystems*, J. Algebra Discrete Math., No. 1, pp 133–150 (2005)

[7] Wróblewska A., *On some properties of graph based public keys*, Albanian Journal of Mathematics, Vol. 2, No. 3, pp 229–234, NATO Advanced Studies Institute: "New challenges in digital communications" (2008)

[8] Ustimenko V., Wróblewska A., *On some algebraic aspects of data security in cloud computing*, Proceedings of International conference "Applications of Computer Algebra", Malaga, pp 144–147 (2013)

[9] Kotorowicz J., Ustimenko V., *On the implementation of cryptoalgorithms based on algebraic graphs over some commutative rings*, Condensed Matters Physics, Special Issue: Proceedings of the international conferences "Infinite particle systems, Complex systems theory and its application", Kazimerz Dolny, Poland, 2006, 11 (No. 2(54)), pp 347–360 (2008)

[10] Klisowski M., Ustimenko V., *On the Comparison of Cryptographical Properties of Two Different Families of Graphs with Large Cycle Indicator*, Mathematics in Computer Science, , Vol. 6, No. 2, pp 181–198 (2012)

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

[12] Bourbaki N., *Lie Groups and Lie Algebras*, Springer (1989)

[13] Shaska T., Ustimenko V., *On some applications of graph theory to cryptography and turbocoding*. Albanian J. Math., vol. 2, no. 3, pp. 249âĂŞ255. In: Proceedings of the NATO Advanced Studies Institute: New challenges in digital communications (2008)

[14] Koblitz N., *Algebraic Aspects of Cryptograph*, Springer (1998)

[15] Simonovitz M., *Extermal Graph Theory* , In "Selected Topics in Graph Theory", 2, edited by L. W. Beineke and R. J. Wilson, Academic Press, London, pp 161–200 (1983)

[16] Ustimenko V., *Some optimisation problems for graphs and multivariate cryptography* (in Russian), In Topics in Graph Theory: A tribute to A.A. and T. E. Zykova on the ocassion of A. A. Zykov birthday, pp 15–25, (2013), www.math.uiuc.edu/kostochka.

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

[18] Ustimenko V., *On the cryptographical properties of extreme algebraic graphs*, in Algebraic Aspects of Digital Communications, IOS Press (Lectures of Advanced NATO Institute, NATO Science for Peace and Security Series - D: Information and Communication Security, Vol. 24, p 296 (2009)

©2014 albanian-j-math.com