On implemented graph based generator of cryptographically strong pseudorandom sequences of multivariate nature

Vasyl Ustimenko
0000-0002-2138-2357
Royal Holloway University of London, Institute of Telecommunications and Global Information Space, Kyiv, Ukraine
Vasyl.Ustymenko@rhul.ac.uk

Tymoteusz Chojecki
0000-0002-3294-2794
Uniwerystet Marii Curie-Skłodowskiej, Polska
Email:
Tymoteusz.chojecki@umcs.pl

***Abstract*— Classical Multivariate Cryptography (MP) is searching for special families of functions of kind $^nF=T_1F_TT_2$ on the vector space $V=(F_q)^n$ where F is a quadratic or cubical polynomial map of the space to itself, T_1 and T_2 are affine transformations and T is the piece of information such that the knowledge of the triple T_1, T_2, T allows the computation of reimage x of given $^nF(x)$ in polynomial time $O(n^\alpha)$. Traditionally F is given by the list of coefficients $C(^nF)$ of its monomial terms ordered lexicographically. We consider the Inverse Problem of MP of finding T_1, T_2, T for F given in its standard form. The solution of inverse problem is harder than finding the procedure to compute the reimage of ^nF in time $O(n^\alpha)$. For general quadratic or cubic maps ^nF this is *NP* hard problem. In the case of special family some arguments on its inclusion to class *NP* has to be given.**

Key words: secure pseudorandom sequences, Multivariate Cryptography, Stream Ciphers, public Keys.

I. Introduction

Assume that the triples $^nT_1$, $^nT_2$, ^nT will be constructed from some seed S of elements from F_q. The question whether or not increasing tuples of kind $C(^nF)$ form a cryptographically strong sequences of pseudorandom field elements can be addressed.

We used algebraic constructions of Extremal Graph Theory to present sequences $C(^nF)$ where the complexity of the inverse problem is justified by the complexity of finding the shortest path between two vertices of bipartite graph of order $2q^n$. In all suggested constructions the field F_q can be replaced by arbitrary commutative ring with unity.

1. On the inverse problem of Multivariate Cryptography.

Task of generation of cryptographically strong pseudorandom sequence of elements of finite field F_q is a traditional problem of applied cryptography. We can replace F_q for general commutative ring K with unity, infinite cases $K=Z$, $K=R$ or $K=F_2[x]$ are especially important.

Some practical applications are observed in [1] books (chapters 16, 17), [2] and [3], papers [4]-[9] selected for demonstration of different approaches for the constructions of pseudorandom sequences. Noteworthy that there are possibilities of construction genuinely random sequences with usage of quantum computers or other natural randomness sources (see [10], [11], [12]).

The task is about generation of potentially infinite sequence $a(n)=(a_1, a_2, \ldots, a_{f(n)})$ of field characters which depends from the secret seed. We assume that $f(n)$ is increasing function on the set N of natural number in natural variable n. Requirements of pseudo randomness practically means that sequences $a(n)$ satisfy several special tests which confirm that the behavior of sequence is ''similar'' to behavior of genuine random sequence. Nowadays the term cryptographically strong means that the knowledge of $a(n)$ for some value of n does not allow adversary to recover the seed and reconstruct the computation of $a(x)$ for arbitrary x. It means that adversarial task is at least as hard as one as known *NP*-hard problem intractable even with usage of Quantum Computer.

We assume that two correspondents Alice and Bob use some protocol for secure elaboration of the ''seed'' which is the tuple $S=(s(1), s(2), \ldots, s(d))$ of *nonzero* symbols from finite field F_q of characters 2. They would like to construct a secure renovations of this seed in a form of potentially infinite sequences $^mR_Y(S)=R(S)$ and $^nH_Z(S)=H(S)$ of nonzero field elements of polynomial length $f(Y, m)$ and $g(Z, n)$ where n and m are potentially infinite natural numbers. The parameters n and m as well as pieces of information Y and Z are known publicly. In the case of finite commutative rings correspondents will use string $H(S)$ as the password of one time pad to encrypt plaintext P from $(F_q)^{g(Z,n)}$. So, the ciphertext will be $P+H(S)$. The tuple $R(S)$ will be used as a new seed for the next round of the procedure. Correspondents agree on new

This research is partially supported by British Academy Fellowship for Researchers at Risk 2022 and by UMCS program UMCS Mini-Grants.

numbers n^* and m^* and information pieces Y^* and Z^* and compute ${}^{m^*}R_{Y^*}(R(S))={}^*R$ and ${}^{n^*}H_{Z^*}(R(S))={}^*H$. They will keep $^*R$ safely as the seed for the next session and use $^*H$ for the encryption.

Assume that adversary got the password $H(S)$. He/she knows Z and n and can try to restore the seed S and break the communication process.

We use Multivariate Cryptography techniques for the implementation of this scheme and making seed restoration an *NP* -hard problem.

We generalize the above scheme via simple change of F_q for arbitrary commutative ring K *with unity.*

We assume that multivariate map F is given in its standard form of kind

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

where f_i are polynomials from $K[x_1, x_2, \dots, x_n]$ given in their standard forms which are lists of monomial terms ordered according to the lexicographic order. Let $c(F)$ be the list of non-zero coefficients of lexicographically ordered monomial terms. Practically we will use quadratic or cubic multivariate maps.

For the nonlinear map F of bounded degree given in its standard form we define *trapdoor accelerator* $F={}^1TG_D{}^2T$ as the triple ${}^1T$, ${}^2T$, G_D of transformations of K^n where ${}^iT$, $i=1, 2$ are elements of $AGL_n(K)$, $G=G_D$ is nonlinear map on K^n and D is the piece of information which allow us to compute the reimage for nonlinear G in time $O(n^2)$ (see [20]). In this paper we assume that D is given as a tuple of characters $(d(1), d(2), \dots, d(m))$ in the alphabet K.

We consider the INVERSE PROBLEM for the construction of trapdoor accelerator of multivariate rule, i. e. with given standard form of F find a trapdoors ${}^1TG_D{}^2T$ for F.

Obviously, this problem is harder than finding the reimage computation method for values of F. It is harder than finding reimage computation procedure with the complexity $O(n^2)$.

We suggest the following general scheme. Let ${}^nF_r$ *be a family of nonlinear maps in* n-variables which has trapdoor accelerator of kind $G_{D(n)}$ where $D(n)=({}^nd(1), {}^nd(2), \dots, {}^nd(r))$,such that $r=m(n)$. Affine maps are identities.

Correspondents have initial seed $(s(1), s(2), \dots, s(d))$. One of them selects parameters n and $r=m(n)$ and forms *multivariate frame* $Y(n, r)$ which consists on the tuple $h=(i_1, i_2, \dots, i_r)$ of elements from $M=\{1, 2, \dots, d\}$, tuples $b(k)=({}^kb_1, {}^kb_2, \dots, {}^kb_n)$ from M^n and matrices $M(k)=({}^kz(i,j))$, $i, j \in \{1, 2, \dots n\}$, $k=1,2$ with entries ${}^kz(i,j)$ from M.

and send his/her partner via open channel. They compute specialised matrices ${}^kM=(s({}^kz(i,j)))$ and tuples ${}^kb==(s({}^kb_1), s({}^kb_2), \dots, s({}^kb_n))$.

They form affine maps ${}^1T(x)={}^1Mx+{}^1b$ and ${}^2T={}^2Mx+{}^2b$, $k=1,2$.

Each correspondent computes standard form of ${}^1T\ {}^nF_r\ {}^2T=G(Y(n,r))=G$ *and write down the list* $C(G(Y(n, r))$ *of coefficients of monomial terms. They can treat* $C(G)$ *as password* $H(S)$ *for one time pad and use other multivariate frame* $Y(m^*, r^*)$ *as new seed* $R(S)$.

REMARK. It is possible to modify the definition of ${}^1M$ *and* ${}^2M$ *with the option of entries from* $MU\{1,0\}$.

II. On graph based trapdoor accelerators of Multivariate Cryptography.

We suggest the algorithm where trapdoor accelerator ${}^nF_r$ defined over commutative ring K is a cubical rule ${}^wF$ induced by the walk $w={}^rw$ of length r on algebraic incidence structure (bipartite graph) with point and line sets isomorphic to variety K^n.

The walk depends on the sequence of symbols $(s(1), s(2), \dots, s(r))$ in the alphabet K of length r on bipartite graph $\mathbb{\Gamma}_n(K)$ with partition sets and recovery of the walk between the plaintext tuple and the ciphertext gives the information about the seed. Noteworthy that Dijkstra algorithm is able to find the path between given vertices in time $O(v\ln(v))$ where v is the order of graph. In our case the order is $2q^n$. It means that the complexity of this algorithm is subexponential.

In the case of $K=F_q$ suggested algorithm graphs $\mathbb{\Gamma}_n(q)$ form one of the known families of graphs with increasing girth $D(n, q)$ and $A(n, q)$ (see [13], [14] and further references, [15] and further references). Recall that girth is the length of minimal cycle in a graph. If the distance r between vertexes is less than half of the girth, then the shortest path between them is unique. For the graphs from each family the projective limit is well defined and tends to q-regular forest. Connected components of these graphs are good *tree approximations.* It means that if n is sufficiently large then expected complexity is $q(q-1)^{r-1}$. We select r, $r \le n$ as unbounded linear function $l(n)$ in variable n. In fact it can be proven that a_i, $i=1, 2, \dots, f(n)$ are polynomial expressions in variables $s(1), s(2), \dots, s(r)$ of degree r. Let us construct the function ${}^nF$. The incidence structure $A(n, K)$ is defined $A(n, K)$ as bipartite graph with the point set $P=K^n$ and line set $L=K^n$ (two copies of a Cartesian power of K are used). We will use brackets and parenthesis to distinguish tuples from P and L. So $(p)=(p_1, p_2, \dots, p_n) \in P_n$ and $[l]=[l_1, l_2, \dots, l_n] \in L_n$. The incidence relation $I=A(n,K)$ (or corresponding bipartite graph I) is given by condition $p\ I\ l$ if and only if the equations of the following kind hold. $p_2 - l_2=l_1p_1$, $p_3 - l_3= p_1 l_2, p_4 - l_4 = l_1p_3$, $p_5 - l_5 = p_1 l_4$, … , $p_n - l_n = p_1 l_{n-1}$ for odd n and $p_n - l_n = l_1 p_{n-1}$ for even n. We can consider an infinite bipartite graph $A(K)$ with points $(p_1, p_2, \dots, p_n, \dots)$ and lines $[l_1, l_2, \dots, l_n, \dots]$. It is proven that each odd n girth indicator of $A(n, K)$ is at least $[n/2]$.

Another incidence structure $I= D(n, K)$ is defined below. Let us use the same notations for points and lines as in previous case of graphs $A(n, K)$.

Points and lines of $D(n, K)$ also are elements of two copies of the affine space over K. Point $(p)=(p_1, p_2, \dots, p_n)$ is incident with the line $[l]=[l_1, l_2, \dots, l_n]$ if the following relations between their coordinates hold: $p_2 - l_2=l_1p_1$, $p_3 - l_3=$

$p_1 l_2, p_4 - l_4 = l_1 p_3, \ldots, l_i - p_i = p_1 l_{i-2}$ if i congruent to *2* or *3* modulo *4*, $l_i - p_i = l_1 p_{i-2}$ if i congruent to *1* or *0* modulo *4*. Incidence structures $D(n, F_q)$, $q>2$

form a family of large girth (see [13 LUW]), for each pair n , $n \geq 2$, q, $q>2$ the girth of the graph is at least $n+5$.

Let $\Gamma(n, K)$ be one of graphs $D(n, K)$ or $A(n, K)$. The graph $\Gamma(n, K)$ has so called defined linguistic colouring ρ of the set of vertices. We assume that $\rho(x_1, x_2, \ldots, x_n)=x_1$ for the vertex x (point or line) given by the tuple with coordinates $x_1, x_2, \ldots, x_n$. We refer to x_1 from K as the colour of vertex x.

It is easy to see that each vertex has unique neighbour of selected colour. Let N_a be operators of taking the neighbour with colour a from K. Let $[y_1, y_2, \ldots, y_n]$ be the line y of $\Gamma(n, K[y_1, y_2, \ldots, y_n])$ and $(\alpha(1), \alpha(2), \ldots, \alpha(t))$ and $(\beta(1), \beta(2), \ldots, \beta(t))$, t are the sequences of nonzero elements of the length at least 2. We form sequence of colours of points $a(1)=y_1+\alpha(1)$, $a(2)= y_1 +\alpha(1)+ \alpha(2), \ldots, a(t)= y_1 +\alpha(1)+ \alpha(2)\ldots+\alpha(t)$ and the sequence of colours of lines $b(1)= y_1 + \beta(1)$, $b(2)= y_1 + \beta(1)+\beta(2), \ldots$, $b(t)= y_1 +\beta(1)+ \beta(2) \ldots \beta(t)$ and consider the sequence of vertices from $\Gamma(n, K[y_1, y_2, \ldots, y_n])$: $v=y$, , ${}^1v=N_{a(1)}(v)$, ${}^2v=N_{b(1)}({}^1v)$, ${}^3v=N_{a(2)}({}^2v)$, … , ${}^{2t-1}v=N_{\alpha(t)}({}^{2t-2}v)$, ${}^{2t}v=N_{b(t)}({}^{2t-1}v)$.

Assume that $v={}^{2t}v=[v_1, v_2, \ldots, v_n]$ where v_i are from $K[y_1, y_2, \ldots, y_n]$. We consider bijective quadratic transformation $g(\alpha(1), \alpha(2),\ldots, \alpha(t) \mid \beta(1), \beta(2), \ldots, \beta(t))$, $t \geq 2$ of affine space K^n of kind $y_1 \rightarrow y_1 + \beta(t)$, $y_2 \rightarrow v_2(y_1, y_2)$, $y_3 \rightarrow v_3(y_1, y_2, y_3)$, … , $y_n \rightarrow v_n(y_1, y_{2,\ldots,} y_n)$.

It is easy to see that $g(\alpha(1), \alpha(2),\ldots, \alpha(t) \mid \beta(1), \beta(2), \ldots, \beta(t)) \bullet g(\gamma(1), \gamma(2),\ldots, \gamma(s) \mid \sigma(1), \sigma(2), \ldots, \sigma(t)) = g(\alpha(1), \alpha(2),\ldots, \alpha(t), \gamma(1)+\beta, \gamma(2)+\beta,\ldots, \gamma(s)+\beta \mid \beta(1), \beta(2), \ldots, \beta(s), \sigma(1)+\beta, \sigma(2)+\beta, \ldots, \sigma(s)+\beta)$ where $\beta= \beta(1)+ \beta(2) + \ldots +\beta(t)$.

THEOREM 1 [11]. Bijective transformations of kind $g(\alpha(1), \alpha(2),\ldots, \alpha(t) \mid \beta(1), \beta(2), \ldots, \beta(t))$, $t \geq 2$ *generate the subgroup* $G(\Gamma(n, K))$ *of transformations of* K^n *with maximal degree 3.*

Let F be a standard form of ${}^1T\, g(\alpha(1), \alpha(2),\ldots, \alpha(t) \mid \beta(1), \beta(2), \ldots, \beta(t))\, {}^2T$ where ${}^1T$ *and* ${}^2T$ are elements of $AGL_n(K)$ and $T=O(n)$. Then triple ${}^1T$, ${}^2T$, $(\alpha(1), \alpha(2),\ldots, \alpha(t), \beta(1), \beta(2), \ldots, \beta(t))$ be a trapdoor accelerator of F.

We will use family of graphs $A(n, K)$ and $D(n, K)$ together with $A(n, K[y_1, y_2, \ldots, y_n])$ and $D(n, K[y_1, y_2, \ldots, y_n])$. Let $\Gamma(n, K)$ be one of those graphs defined over the commutative ring K with the unity.

Assume that correspondents Alice and Bob already completed some seed agreement protocol and elaborate seed $s=(s(1), s(2), \ldots, s(k))$. Without loss of generality we assume that $s(i)\neq 0$ for $i=1,2,\ldots, k$.

For the construction of multivariate frame they select parameters t and n together with sequences $(i_1, i_2, \ldots, i_t)$, $(j_1, j_2, \ldots, j_t)$ of elements from $M=\{1, 2,..,k\}$ and

matrices ${}^rU=({}^ru(i.j))$, $r=1, 2$ with ${}^ru(i,j)$ from M.

Correspondents take linear transformations ${}^1T$ and ${}^2T$ corresponding to matrices ${}^1A$ and ${}^2A$ with entries $s({}^1u(i.j))$ and $s({}^2u(i.j))$ and computes the standard form of $F= {}^1Tg(s(i_1), s(i_2),\ldots, s(i_t) \mid s(j_1), s(j_2),\ldots, s(j_t))\, {}^2T$.

We need some ''general frame generation algorithm''. The simple suggestion is the following.

We concatenate word $(s(1), s(2),\ldots, s(d))$ with itself and get infinite sequence $s_1, s_2,\ldots, s_i,\ldots$. *We identify* $({}^1u(1, 1), {}^1u(1,2), \ldots, {}^1u(1,n))$ with $(s_1, s_2, \ldots, s_n)$ and use the cyclic shift and set

$({}^1u(i, 1), {}^1u(i, 2), \ldots, {}^1u(1,n))=(s_i, s_{i+1}, \ldots, s_n, s_{n+1}, s_{n+2}, \ldots s_{n+i-1})$ for $i=2,3,\ldots,n$

We use reverse tuples to form matrix ${}^2U$. So $({}^2u(1, 1), {}^2u(1,2), \ldots, {}^2u(1,n))=$

$(s_n, s_{n-1},\ldots, s_1)$ and $({}^2u(i, 1), {}^2u(i,2), \ldots, {}^2u(1,n))=(s_{n+i-1}, s_{n+i-2},\ldots, s_{n+1}, s_n, s_{n-1}, \ldots, s_i)$ for $i=2, 3, \ldots, n$.

We set $(i_1, i_2,\ldots, i_t)$ and $(j_1, j_2, \ldots, j_t)$ as $(s_1, s_2,\ldots, s_t)$ and $(s_{1+t}, s_{2+t}, \ldots, s_{2t})$ respectively.

So they can use the sequence of symbols $C(F)$ as a password for the additive one time pad with plaintext $K^{d(F)}$ where $d(F)$ is the number of monomial terms for the multivariate map F.

Other multivariate frame can be used for the seed renovation. Noteworthy that alternatively correspondents can use a new session of the protocol for the seed elaboration.

Other option is to use the stream cipher on K^n where each ${}^rT$ is changed for the compositions of lower and upper unitriangular matrices ${}^rL$ and ${}^rU$ with nonzero entries from ${}^rA$. One of the option is to use transformations T_1: $y \rightarrow {}^1U\, {}^1L y+({}^1a(1,1), {}^1a(2,2), \ldots, {}^1a(n, n))$ and T_2: $y \rightarrow L^2U^2y+({}^2a(1,1), {}^2a(2,2), \ldots, {}^2a(n, n))$.

So correspondents use bijective *transformation* $F=T_1\, g(\alpha(1), \alpha(2),\ldots, \alpha(t) \mid \beta(1), \beta(2), \ldots, \beta(t))\, T_2$ for the encryption. The knowledge of trapdoor accelerator allows correspondents to encrypt or decrypt in time $O(n^2)$.

REMARK ON TRAPDOOR MODIFICATIONS. *In the case of* $K=F_q$, $q=2^r$, $r \geq 16$ *we can use operator* ${}^aJ$ *of changing the colour* p_1 *of the point* $(p_1, p_2, \ldots, p_n)$ *from the graph* $\Gamma(n, K))$ *for the ring element a.*

We can take the path in the graph $\Gamma(n, K[y_1, y_2,\ldots, y_n]))$ *corresponding to* $g(\alpha(1), \alpha(2),\ldots, \alpha(t) \mid \beta(1), \beta(2), \ldots, \beta(t))$ *with the starting point* $(y_1, y_2, \ldots, y_n)$ *and ending point* ${}^{2t}v$.

We change ${}^{2t}v$ *for* $v ={}^aJ({}^{2t}v)=((y_1)\wedge 2, v_2, .., v_n)$, $a=(y_1)^2$ *and consider the rule*

$y_1 \rightarrow (y_1)^2$, $y_2 \rightarrow v_2(y_1, y_2)$, $y_3 \rightarrow v_3(y_1, y_2, y_3)$, … , $y_n \rightarrow v_n(y_1, y_{2,\ldots,} y_n)$. *This rule induces bijective quadratic transformation* $h(\alpha(1), \alpha(2),\ldots, \alpha(t) \mid \beta(1), \beta(2), \ldots, \beta(t))$ *of vector space* K^n.

Then polynomial degree of inverse for $G=T_1\, h(\alpha(1), \alpha(2),\ldots, \alpha(t) \mid \beta(1), \beta(2), \ldots, \beta(t))\, T_2$ *is at least* 2^{r-1} *, descryption of this graph based accelerator can be found in* [20].

Noteworthy that the map F and its inverse are cubic transformations. Adversary has to intercept more than $n^3/2$ pairs of kind plaintext/ciphertext to restore F or its inverse. Theoretically interception of $O(n^3)$ pairs will allow adversary to break the stream cipher in time $O(n^{10})$ via linearisation attacks. It is

easy to see that the transformation G is resistant to linearization attacks.

REMARK 1. In the case of $\mathbb{\Gamma}(n, K)$ based encryption we can use sparce frame given by two numbers r and n and sequences $(i_1, i_2, \ldots, i_t)$, $(j_1, j_2, \ldots, j_t)$ of elements from $M=\{1, 2,..,k\}$

together with two sequences $({}^1i, {}^2i, \ldots, {}^{n-1}i)$ *and* $({}^1j, {}^2j, \ldots, {}^{n-1}j)$ from M^{n-1}. *So Alice and Bob form linear transformations* ${}^1\tau$ *and* ${}^2\tau$ *such that* ${}^1\tau(y_1)=y_1+s({}^1i)y_2+ s({}^2i)y_3+\ldots s({}^{n-1}i)y_n$, ${}^2\tau(y_1)=y_1+s({}^1i)y_2+ s({}^2i)y_3+\ldots s({}^{n-1}i)y_n$, ${}^j\tau(y_i)=y_i$ *for* $j=1,2$ *and* $i\geq 2$.

So correspondents compute the standard form of $F= {}^1\tau g(s(i_1), s(i_2), \ldots, s(i_t) \mid s(j_1), s(j_2), \ldots, s(j_t)) {}^2\tau$ and able to use string $C(F)$.

Let us assume that $t=O(n^{\alpha})$ *where* $0\leq\alpha<1$. Then inverse problem of restoration of sparce *frame is harder than finding the algorithm of computing* F^{-1} *in time* $O(n^{\alpha+1})$. *Recall that solving nonlinear system of polynomial equations is known NP hard problem,* if the *inverse map* F^{-1} *is cubic it can be found in time* $O(n^{10})$.

We implemented described above algorithm of generating $C(F)$ in the case of finite fields F_q, $q=2^m$

of characteristic *2*, arithmetical rings Z_q and Boolean rings B(m, 2) of order 2^m .

REMARK 2. We can treat element $\alpha_1+ \alpha_2x+ \alpha_3x^2\ldots \alpha_m x^{m-1}$ *of* F_q, $q=2^m$ *as a sequence of elements* $(\alpha_1, \alpha_2, \ldots, \alpha_m)$ *of* F_2 *(element of Boolean ring) or number* $\alpha_1+ \alpha_2 2+ \alpha_3 2^2\ldots \alpha_m 2^{m-1}$ *(element of* Z_q *).*

The results of computer simulations are presented in [19 uk, archive 2019]. Some of these tables and graphs are reproduced below for readers convenience.

Table 1. Number of monomial terms of the cubic map of induced by the walk on the graph $D(n, F_{2^{32}})$, case of sparce frame.

	length of the walk r				
n	16	32	64	128	256
16	3649	3649	3649	3649	3649
32	41355	41356	41356	41356	41356
64	440147	529052	529053	529053	529053
128	3823600	6149213	7405944	7405945	7405945

Table 2. Density of the cubic map of induced by the walk on graph $D(n, F_{2^{32}})$, case of general frame.

	length of the word				
n	16	32	64	128	256
16	6544	6544	6544	6544	6544
32	50720	50720	50720	50720	50720
64	399424	399424	399424	399424	399424
128	3170432	3170432	3170432	3170432	3170432

Table 3. Density of the cubic map of linear degree induced by the graph $A(n, F_{2^{32}})$, case II

	length of the walk				
n	16	32	64	128	256
16	5623	5623	5623	5623	5623
32	53581	62252	62252	62252	62252
64	454375	680750	781087	781087	781087
128	3607741	6237144	9519921	10826616	10826616

Table 4. Density of the map of linear degree induced by the graph $A(n, F_{2^{32}})$, case III

	length of the walk				
n	16	32	64	128	256
16	6544	6544	6544	6544	6544
32	50720	50720	50720	50720	50720
64	399424	399424	399424	399424	399424
128	3170432	3170432	3170432	3170432	3170432

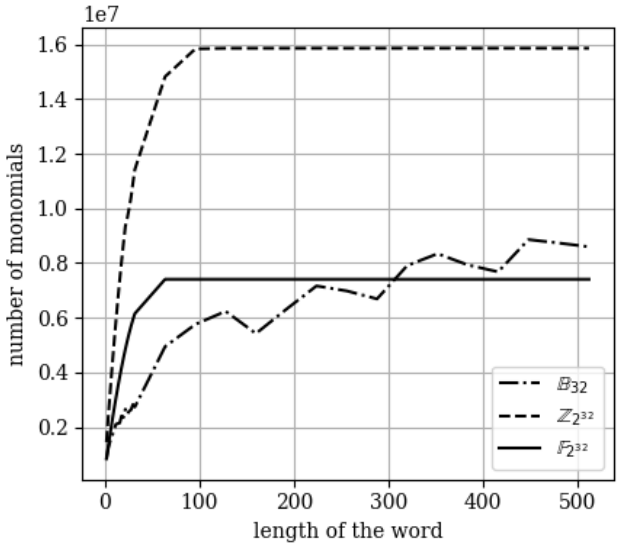

Figure 1. Number of monomial terms of the cubic map induced by the walk on the graph ($n = 128$) (graph $D(n, K)$, $K = B(32), Z_{2^{32}}, F_{2^{32}}$), case of sparce frame.

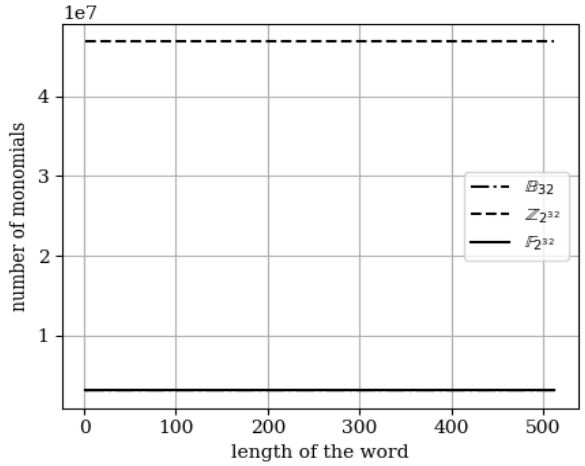

Figure 2. Number of monomial terms of the map induced by the walk on graph ($n = 128$) (graph $D(n,K), K = B(32), Z_{2^{32}}, F_{2^{32}}$), case of general frame.

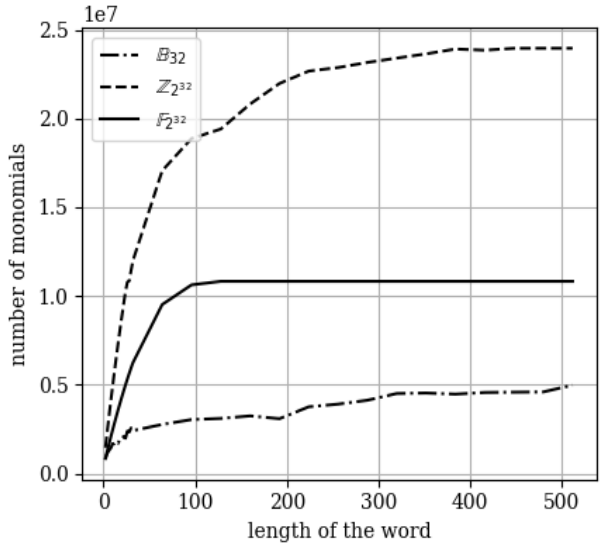

Figure 3. Number of monomial terms of the cubic map induced by the graph ($n = 128$) (graph $A(n,K), K = B(32), Z_{2^{32}}, F_{2^{32}}$), case of sparce frame.

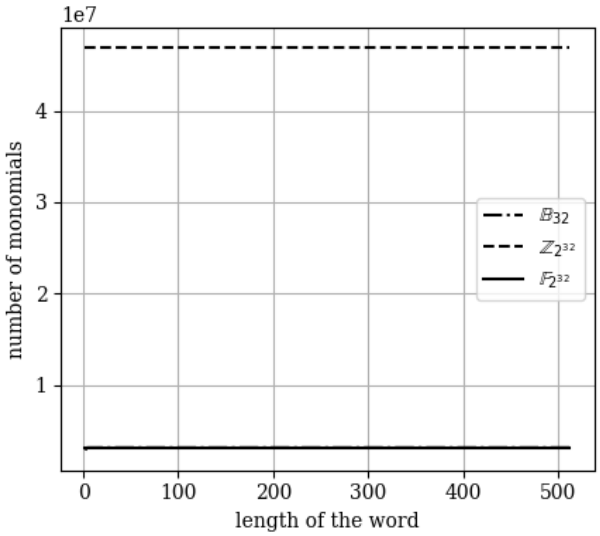

Figure 4. Number of monomial terms of the map induced by the walk on graph ($n = 128$) (graph $A(n,K), K = B(32), Z_{2^{32}}, F_{2^{32}}$), case of general frame.

III. EXAMPLE OF THE SEED ELABORATION PROTOCOL OF MULTIVARIATE NATURE.

Presented above algorithms of generation of potentially infinite sequences of ring elements use seeds in the form of tuples of nonzero elements. Such seeds can be elaborated via protocols of Noncommutative Cryptography (see [21]-[25]) based on the various platform.

We will use one of the simplest protocols of Noncommutative Cryptography *which* is straightforward generalization Diffie -Hellman algorithm. The scheme is presented below.

A. Twisted Diffie-Hellman protocol.

Let ***S*** be an abstract semigroup which has some invertible elements.

Alice and Bob share element $g \epsilon S$ and pair of invertible elements h, h^{-1} from this semigroup.

Alice takes positive integer $t = k_A$ and $d = r_A$ and forms $h^{-d}g^t h^d = g_A$. Bob takes $s = k_B$ and $p = r_B$.

and forms $h^{-p}g^s h^p = g_B$. They exchange g_A and g_B and compute collision element X as ${}^A g = h^{-d} g_B{}^t h^d$ and ${}^B g = h^{-p} g_B{}^t h^p$ respectively.

The security of the scheme rest on the Conjugation Power Problem, adversary has to solve the problem $h^{-x}g^y h^x = b$ where b coincides with g_B or g_A. The complexity of the problem depends heavily on the choice of highly noncommutative platform S.

We will use the semigroups of polynomial transformations of affine space K^n of kind $x_1 \to f_1(x_1, x_2, \ldots, x_n)$, $x_2 \to f_2(x_1, x_2, \ldots, x_n), \ldots, x_n \to f_n(x_1, x_2, \ldots, x_n)$ where f_i, $i=1,2,\ldots n$. Noteworthy that in case of $n=1$ the composition of two nonlinear transformations of degree s and r will have degree rs. The same fact holds for the majority of nonlinear transformations in n variables.

For the feasibility of the computations in the semigroup of transformation we require the property of computing n elements in a polynomial time $O(n^{\alpha})$, $\alpha>0$. We refer to this property as Multiple Composition Polynomiality Property (MCP). Below we present one of the MCP type families for which Conjugation Power Problem is postquantum untractable, i. e. usage of Quantum Computer for Cryptanalysis does not lead to the change of its *NP* hard status.

Let K be a finite commutative ring with the multiplicative group K^* of regular elements of the ring. We take Cartesian power ${}^nE(K) =(K^*)^n$ and consider an Eulerian semigroup ${}^nES(K)$ of transformations of kind

$$\begin{aligned} x_1 &\to \mu_1 x_1^{a(1,1)} x_2^{a(1,2)} \dots x_m^{a(1,n)}, \\ x_2 &\to \mu_2 x_1^{a(2,1)} x_2^{a(2,2)} \dots x_m^{a(2,n)}, \\ &\dots \\ x_m &\to \mu_n x_1^{a(n,1)} x_2^{a(n,2)} \dots x_m^{a(n,n)}, \end{aligned} \qquad (1)$$

where $a(i,j)$ are elements of arithmetic ring Z_d, $d=|K^*|$, $\mu_i \in K^*$.

Let ${}^nEG(K)$ stand for Eulerian group of invertible transformations from ${}^nES(K)$. Simple example of element from ${}^nEG(K)$ is a written above transformation where $a(i,j)=1$ for $i \neq j$ or $i=j=1$, and $a(j,j)=2$ for $j \geq 2$. It is easy to see that the group of monomial linear transformations M_n is a subgroup of ${}^nEG(K)$. So semigroup ${}^nES(K)$ is a highly noncommutative algebraic system. Each element from ${}^nES(K)$ can be considered as transformation of a free module K^n *(see 15)*.

We implemented described above protocol with the platform ${}^nES(K)$ in the cases of fields $K=F_q$, $q=2^m$ and arithmetical rings $K=Z_q$. The output of algorithm is the element as above with elements $a(i,j)$ from multiplicative group F^*_q (case of the field) or group Z_t, $t=2^{m-1}$ in the case of elements of arithmetical ring. We form matrix $B=(\mu_i \mu_j)^{a(i,j)}$ of regular elements of K and treat as the sequence of elements of length n^2. In necessary we identify nonzero field element $a_0+a_1x+a_2x^2+\dots+a_{m-1}x^{m-1}$ with the tuple $(a_0, a_1, \dots, a_{m-1})$ from the Boolean ring $B(m. 2)$ of order 2^m.

For the generation on invertible element h from the protocol we use transformation E which is obtained as composition of " upper triangular element" ${}^1E$

$$\begin{aligned} x_1 &\to q_1 x_1^{a(1,1)} x_2^{a(1,2)} \dots x_n^{a(1,n)}, \\ x_2 &\to q_2 x_2^{a(2,2)} x_3^{a(2,3)} \dots x_n^{a(2,n)}, \\ &\dots, \\ X_{n-1} &\to q_{n-1} x_{n-1}^{a(n-1,n-1)} x_n^{a(n-1,n)} \\ x_n &\to q_n x_n^{a(n,n)}, \end{aligned} \qquad (2)$$

and lower triangular element

$$\begin{aligned} x_1 &\to r_1 x_1^{b(1,1)}, \\ x_2 &\to r_2 x_1^{b(2,1)} x_2^{b(2,2)}, \\ &\dots, \\ x_n &\to r_n x_1^{b(n,1)} x_2^{b(n,2)} \dots x_n^{b(n,n)} \end{aligned} \qquad (3)$$

where q_i and r_i are regular elements *of* K, elements $a(i,j)$, $b(i,j)$ are from the group Z_t, where t is the order of multiplicative group of the ring, residues $a(i,i)$, $b(i,i)$ are mutually prime with the modulo t.

Noteworthy that computation of the inverse elements of ${}^1E$ and ${}^2E$ is straightforward.

In fact we can use other platforms of affine transformation, and more general protocols in terms of semigroup of transformations of K^n and its homomorphic image (see [16]-[19]). Security of generalised protocols rests on the complexity of Word Decomposition problem. It is about the decomposition of element w of semigroup S into combination of given generators of S. This problem is harder than its particular case of Conjugation Power Problem.

IV. Conclusions and topics for further research.

We suggest the protocol based communication scheme for a Postquantum usage. It uses nonlinear transformation of affine space K^n where K is a finite commutative ring with unity. Convenient for practical application choices for K are finite field of characteristics *2* of order 2^s, arithmetic ring Z_t, $t=2^s$ and Boolean ring $B(s, 2)$.

Correspondents Alicia and Bob can use the following communication scheme or its modification.

1. Firstly, they have to generate a ‘’seed of information’’. Correspondents agree on the parameter s, basic commutative field K which is the F_q or arithmetic rings Z_t and the dimension n of the affine space.

Alice selects elements ${}^1E$ of kind (2) and ${}^2E$ of kind (3). She computes $h={}^1E{}^2E$ and its inverse h^{-1}. She selects transformation g of kind (1) and sends the triple (h, h^{-1}, g) to her partner Bob via an open channel. Alice and Bob conduct described in section 3 algorithm. So they elaborate a collision element C of kind (1) with coefficients μ_i and $a(i, j)$ in a secure way.

They form the matrix $B =(b(i,j))$ with entries $(\mu_i \mu_j)^{a(i,j)}$. Correspondents arrange these entries accordingly to the lexicographical order and get the seed in a form a tuple $(s(1), s(2), \dots, s(n^2))$.

Noteworthy that the complexity of this protocol is $O(n^4)$.

1. Correspondents has to agree via an open channel on the commutative ring R. They can treat characters $s(i)$ as field elements, residuals or elements of Boolean ring $B(s, 2)$.
2. They will use elaborated seed for the creation of cryptographically strong potentially infinite sequence $(b(1), b(2), \dots, b(t))$ from R^t for some parameter t.

Correspondents agree on potentially infinite parameter m, the graph $\mathbb{\Gamma}_m(R)$ ($A(m, R)$ or $D(m, R)$) and type of the frame for multivariate accelerator (general frame of section 2 or sparce frame of Remark 1) and parameter r (length of the path).

They construct multivariate accelerator which is the cubic transformation F acting on the affine space R^m.

3. They can exchange the information with the usage of the following options.

(a) Compute the standard form of F and tuple $C(F)=(c_1, c_2,\ldots, c_l)$, where $l=l(r, m, R)$ depends on the choice during step 2. Experiment demonstrate that parameter l does not depends on the coordinates of the seed, $n^2<l<n^3$. Correspondents use one type pad. One of them creates the plaintext $(p)=(p_1, p_2, \ldots, p_l)$ and sends to his/her partner ciphertext $(p)+C(F)$. After this action correspondents can go to the next step.

(b) Correspondents use their knowledge on the frame for F and use bijective trapdoor accelerator for encryption of plaintexts from R^n. They can exchange up to $n^3/2$ messages and after that go to step 4. In the case of large fields of characteristic 2 correspondents can change F for G described in the remark on trapdoor modification presented above. They can use this G without time limitations.

4. The change of seed. There are two following options.

(a) Correspondents repeat the step 2 with the same seed $s(1), s(2), \ldots$ with different data which include new graph of kind $\Gamma_{m'}(R')$ and different type of frame in comparison with previous frame usage. They create corresponding accelerator G and take $C(G)$ as a new seed.

(b) Alice and Bob change the seed via the new session of described twisted Diffie-Hellman protocol. After the step 4 they doing sequence of actions (2) and (3) for the encryption with the new seed and go to step 4 again. We plan to test sequences of kind $C(F)$ for the presented above graph based cubic transformations via various approaches for the investigation of pseudorandom sequences (see [26]).

REFERENCES

[1] Bruce Schneier, Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C, John Wiley & Sons, 784 p.

[2] D. Boneh and V. Shoup, *A Graduate Course in Applied Cryptography*, *Stanford University, free on-line course.*

[3] Easttom, W. (2021). Random Number Generators. In: Modern Cryptography. Springer, Cham. https://doi.org/10.1007/978-3-030-63115-4_12

[4] V. Grozov, A. Guirik, M. Budko, and M. Budko, "Development of a Pseudo-Random Sequence Generation Function Based on the Cryptographic Algorithm "Kuznechik,"" Proc. 12th Int. Congr. on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT 2020), Czech Republic, pp. 93-98, 2020, DOI:10.1109/ICUMT51630.2020.9222457.

[5] Balkova, Lubomira; Bucci, Michelangelo; De Luca, Alessandro; Hladky, Jiri; Puzynina, Svetlana (September 2016). "Aperiodic pseudorandom number generators based on infinite words". *Theoretical Computer Science*. 647: 85–100. arXiv:1311.6002. doi:10.1016/j.tcs.2016.07.042. S2CID 2175443.

[6] I. Sparlinski(with J. Kaszian and P. Moree) Periodic structure of the exponential pseudorandom number generator. *Applied Algebra and Number Theory: Essays in Honour of Harald Niederreiter,* Cambridge Univ. Press, Cambridge, 2014, 190-203.

[7] François Panneton, Pierre L'Ecuyer, and Makoto Matsumoto. 2006. Improved Long-period Generators Based on Linear Recurrences Modulo 2. ACM Trans. Math. Software 32, 1 (March 2006), 1–16.

[8] J. Hastad, R. Impagliazzo, L.A. Levin and M. Luby. A Pseudorandom Generator from any One-way Function. SIAM Journal on Computing, Volume 28, Number 4, pages 1364–1396, 1999.

[9] S. Blackburn, S. Murphy, K. Paterson, Comments on theory and applications of cellular automata to cryptography, IEEE Trans. Comput. 46 (1997).

[10] Wikramaratna, R.S. Theoretical and empirical convergence results for additive congruential random number generators, Journal of Computational and Applied Mathematics (2009), doi:10.1016/j.cam.2009.10.015

[11] M. Herrero-Collantes and J.C. Garcia-Escartin, "Quantum random number generators," Review of Modern Physics, vol. 89 (1), pp. 1-54, 2016. DOI:10.1103/RevModPhys.89.015004.

[12] D. Johnston, Random number generators – principles and practices. A guide for engineers and programmers. DeG Press, 2018.

[13] F.Lazebnik V. Ustimenko and A.J.Woldar, A new series of dense graphs of high girth, Bulletin of the AMS 32 (1) (1995), 73-79.

[14] V. A. Ustimenko On the extremal graph theory and symbolic computations, Dopovidi National Academy of Sci, Ukraine, 2013, No. 2, p. 42-49.

[15] V. Ustimenko, Graphs in terms of Algebraic Geometry, symbolic computations and secure communications in Post-Quantum world, University of Maria Curie Sklodowska Editorial House, Lublin, 2022, 198 p.

[16] V. Ustimenko, M. Klisowski, On Noncommutative Cryptography with cubical multivariate maps of predictable density, In "Intelligent Computing'', Proceedings of the 2019 Computing Conference, Volume 2, Part of Advances in Intelligent Systems and Computing (AISC), volume 99, pp. 654-674.

[17] *V. Ustimenko, M. Klisowski, On D(n; q) quotients of large girth and hidden homomorphism based cryptographic protocols, Communication Papers of the 17th Conference on Computer Science and Intelligence Systems, M. Ganzha, L. Maciaszek, M. Paprzycki, D. Ślęzak (eds). ACSIS, Vol. 32, pages 199–206 (2022),* DOI**:** http://dx.doi.org/10.15439/2022F54

[18] V.Ustimenko, On new symbolic key exchange protocols and cryptosystems based on a hidden tame homomorph**ism,** Dopovidi National Academy of Sci, Ukraine, 2018, n10, p.26-36.

[19] V. Ustimenko, M. Klisowski, On Noncommutative Cryptography and homomorphism of stable cubical multivariate transformation groups of infinite dimensional affine spaces, Cryptology ePrint Archive, 2019/593.

[20] V. Ustimenko, On Extremal Algebraic Graphs and Multivariate Cryptosystems, Cryptology ePrint Archive, 2022/593

[21] Alexei G. Myasnikov, Vladimir Shpilrain, Alexander Ushakov. Noncommutative Cryptography and Complexity of Group-theoretic Problems, American Mathematical Society, 2011.

[22] D. N. Moldovyan, N. A. Moldovyan, A New Hard Problem over Noncommutative Finite Groups for Cryptographic Protocols, International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2010: Computer Network Security pp 183-194.

[23] Delaram Kahrobaei, Bilal Khan, A non-commutative generalization of ElGamal key exchange using polycyclic groups, In IEEE GLOBECOM 2006 - 2006 Global Telecommunications Conference [4150920] DOI: 10.1109/GLOCOM.2006.

[24] B. Tsaban, Polynomial-time solutions of computational problems in noncommutative-algebraic cryptography , J. Cryptol. 28, No. 3 (2015), 601-622.

[25] V. A. Roman'kov, A nonlinear decomposition attack, Groups Complex. Cryptol. 8, No. 2 (2016), 197-207.**27**.

[26] Bassham, L. , Rukhin, A. , Soto, J. , Nechvatal, J. , Smid, M. , Leigh, S. , Levenson, M. , Vangel, M. , Heckert, N. and Banks, D. (2010), A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD,[online],https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906762 (Accessed May 8, 2023)