On Extremal Expanding Algebraic Graphs and post-quantum secure delivery of passwords, encryption maps and tools for multivariate digital signatures.

Vasyl Ustimenko

University of Maria Curie Sklodowska, Lublin 20036, Poland
vasyl@hektor.umcs.lublin.pl

Abstract.

Expanding graphs are known due to their remarkable applications to Computer Science. We are looking for their applications to Post Quantum Cryptography. One of them is postquantum analog of Diffie-Hellman protocol in the area of intersection of Noncommutative and Multivariate Cryptographies .This graph based protocol allows correspondents to elaborate collision cubic transformations of affine space K^n defined over finite commutative ring K. Security of this protocol rests on the complexity of decomposition problem of nonlinear polynomial map into given generators.

We show that expanding graphs allow to use such output as a ''seed'' for secure construction of infinite sequence of cubic transformation of affine spaces of increasing dimension. Correspondents can use the sequence of maps for extracting passwords for one time pads in alphabet K and other symmetric or asymmetric algorithms.

We show that cubic polynomial maps of affine spaces of prescribed dimension can be used for transition of quadratic public keys of Multivariate Cryptography into the shadow of private areas.

Keywords: Extremal Graph Theory, Post Quantum Cryptography, Multivariate Cryptography, stable subgroups of affine Cremona group, Noncommutative Cryptography, key exchange protocols, random and pseudorandom sequences, digital signatures.

1. Introduction.

In March 2021 it was announced that prestigious Abel prize will be shared by A. Wigderson and L.Lovasz. They contribute valuable applications of theory of Extremal graphs and Expanding graphs to Theoretical Computer Science (see [1], [2] and further references). We have been working on applications of these graphs to Cryptography. This paper is dedicated to the problem of secure encryption of big files.

One time pad is a practical implementation of the idea of absolutely secure encryption. Symbiotic combination of this encryption tool with key exchange Diffie – Hellman protocol was widely used. Appearance of the first versions of quantum computers and cryptanalysis of algorithms based on

discrete logarithm problem demands new algorithm of ''post quantum secure'' generation of pseudorandom string S of characters from chosen alphabet. Quantum technologies allow to produce genuine random strings G of a chosen length. One time pad encryption of G with the key $\boldsymbol{S}$ will allow safe delivery of string G from correspondent to his/her partner.

In this paper we use sequence of known expanding graphs $A(n, q)$ for the solution of described above task in the case of alphabet F_q. Analogs of these graphs defined over arbitrary commutative ring K allow to introduce algorithm of postquantum secure generation of S in the case of the alphabet K.

In terms of graphs $A(n, K)$ we define polynomial transformation groups $GA(n, K)$ of affine space K^n related to $A(n, K)$. The most important "stability property" of $GA(n, K)$ is proven in terms of DYNAMICAL SYSTEMS on the variety K^n (see [3], [4] and further references).

Stability property means that in the chosen basis maximal degree of elements of $GA(n,K)$ has degree 3. Notice that composition of two randomly chosen nonlinear polynomial maps of degrees k and l in general position with the probability close to 1 will have degree kl.

Required properties of graphs $A(n,K)$ (see [5]) can be justified via enveloping family of graphs $D(n,K)$ and their connected components $CD(n,K)$ (see [6]).

We present a symbiotic combination of the algorithm of generation of potentially infinite string of characters with the postquantum secure Key Agreement Protocol based on computations in the group $GA(n,K)$.

The initial data for this string generator are given via ''seed of finite length'' in the form of tuple of characters of finite length. Correspondents can execute the Key Agreement Protocol with the collision map $\boldsymbol{G}$ from $GA(n,K)$ and extract required seed from G.

We hope that this combination is capable to replace in current postquantum reality a former symbiotic composition of Diffie-Hellman algorithm with classical one time pad.

One application gives alternative to one time pad encryption symmetric encryption algorithm. Its password can be extracted from the output of algorithm of generation of potentially infinite string of characters from K. The complexity of encryption process for this stream cipher is $O(n)$.

The encryption map of this algorithm is polynomial map of unbounded degree. It can be used similarly to public key without the change of password during unlimited time. Implemented simplified version of this algorithm with the encryption map of degree 3 can be used safely $O(n^2)$ times. Results of computer simulation will be presented. Given densities of cubical maps allow to evaluate ''usage interval'' of encryption with a taken password.

Correspondents can change the password via algorithm of generation of potentially infinite string of characters. No need to repeat the $GA(m,K)$

protocol which costs $O(m^{13})$ elementary operations. Execution time for the generation of element of $GA(n, K)$ is useful for the time evaluation of the main algorithm.

2. On current state of Post Quantum Cryptography.

Prototype models of probabilistic machine known as Quantum computer already exist. They can produce genuine random sequences of bits which can be used in information security instead of pseudo random strings.

Perfect symbiosis of one time encryption with Difiie - Hellman protocol for the key exchange can not be used safely anymore because discrete logarithm problem can be efficiently solved with the usage of Turing machine together with Quantum Computer. Combination of these two machines can be used for effective cryptanalysis of RSA (result of Peter Shor**,** 1995).

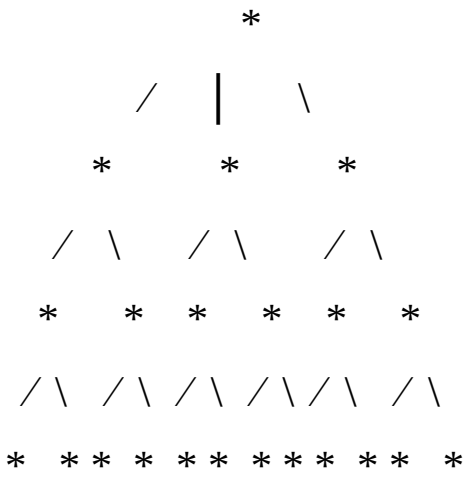
Investigation of public keys with potential resistance to quantum attacks has been supported by US NIST international project on Post Quantum standardisation process since 2017. In July 2020 the third round started for the final investigation of already selected algorithms . In the area of Multivariate Cryptography only rainbow-like oil and vinegar digital signatures are selected for the further investigation. They can not be used as encryption algorithms. This fact motivates different from public key directions of Multivariate Cryptography.

3. Equations of q-regular tree and string processing.

The description of q-regular tree T_q in terms of equations was introduced in 1995 via the construction of graphs $CD(n,q)$ (see [6] and further references).. In fact T_q coincides with well defined projective limit $CD(q)$ of graphs $CD(n,q)$ where n tends to infinity.

It was discovered later that special homomorphic images $A(n,q)$ of $CD(n,q)$ form a family of q-regular small world graphs. Well defined projective limit $A(n, q)$, $n=2,3,\ldots$ coincides with T_q.

$q = 3$



This construction allows to introduce T_q as q - regular bipartite graph with points of kind $(p)=(p_1, p_2,\dots,p_1,\dots)$ and lines $[l]=[l_1, l_2,\dots,l_i, \dots]$ where only finite number of coordinates p_i and l_i are different from zero and point (p) and line $[l]$ are incident if and only if the following relations hold.

$p_2-l_2=l_1p_1$, $p_3-l_3=p_1l_2$, $p_4-l_4=l_1p_3$, ..., $p_{2s}-l_{2s}=l_1p_{12s-1}$, $p_{2s+1}-l_{2s+1}=p_1l_{2s-}$, ...

Brackets and parenthesis allow us to distinguish points from lines.

Projections of (p) and $[l]$ onto $(p_1, p_2,\dots,p_n)$ and $[l_1, l_2,\dots,l_n]$ define graph homomorphism on graph $A(n, q)$ with point set and line set isomorphic to $(F_q)^n$ and incidence given by first $n-1$ equations in the definition of T_q.

We can change finite field F in the given above construction for arbitrary commutative ring K with unity and get infinite graph T_K together with bipartite graph $A(n, K)$ for which two copies of K^n form partition sets. If K is integrity ring then $T_K=A(K)$ is also an infinite tree but existence of zero divisors lead to the appearance of cycles in these graphs.

The first coordinates $\dot{\rho}(p)= p_1$ and $\dot{\rho}([l])=l_1$ are natural colours of points (p) and $[l]$ of graphs $A(n, K)$ and $A(K)$.

The following *linguistic* property holds. For each vertex v there is a unique neighbour u of chosen colour $\dot{\rho}(u)=a$. Let $N_a(v)$ be the operator of taking the neighbour of v with colour a.

The walk in the graph $A(n, K), n=2,3,\dots$ of length m started at the given point $p=(p_1 , p_2,\dots)$ can be given by sequence $a(1), a(2),\dots,a(m)$ of colours. This is a sequence $(p), v_1=N_{a(1)}(p), v_2=N_{a(2)}(v_1),,\dots, v_m=N_{a(m)}(v_{m-1})$.

We refer to string $(a(1), a(2),..,a(m))$ as the direction of the walk. In the case of even m we consider transformation ${}^nC(a(1), a(2),\dots, a(m))$ of K^n into itself defined in the following way.

Take the list of variables $x_1,x_2,\dots,x_n$ and consider $K[x_1, x_2,\dots,x_n]$ together with new graph $A(n, K[x_1, x_2,\dots, x_n])$ given by the same equations as in the case $A(n, K)$.

Take special starting point $(x)=(x_1, x_2,\dots.,x_n)$ and colour string $x_1+a(1), x_1+a(2),\dots, x_1+a(m)$ compute

$(x), v_1=N_{a(1)+x(1)}(p), v_2=N_{a(2)+x(1)}(v_1),\dots, v_m=N_{a(m)+x(1)}(v_{m-1})$ where $x_1=x(1)$.

Finally take the polynomial transformation $C(a(1), a(2),\dots,a(m)))$ of K^n into itself sending (x) to v_m. This transformation is given by the rule $(x)\rightarrow(f_1, f_2, \dots f_n)= v_m$.

We see that each point to point walk w on vertices of such graph which starts in the chosen origin (i.e 0 point) can be given by its direction which is a tuple of kind $w= (a_1, a_2,\dots, a_{2s})$ with $a_i \in K$.

With such direction we associate the tuple ${}^nC(w)=(f_1, f_2, \dots f_n)$, where $f_i \in R=K[x_1, x_2, \dots , x_n]$. It can be proven that maximal degree of $f_i \in R$ ($deg(f_i)$) is 3. We identify this tuple with the map ${}^nC(w)$ of kind $x_i\rightarrow f_i(x_1, x_2,\dots x_n)$, $i=1,2,\dots,n$ which is a bijective polynomial transformation of affine space $(K)^n$.

The natural composition of walks from *0* origin can be formally given by the following rule.

For $w=(a_1, a_2, \dots a_{2s})$ and $u=(u_1, u_2, \dots u_{2t})$ their composition $w \circ u$ is the tuple $(a_1, a_2, \dots a_{2s}, a_{2s}+u_1, a_{2s}+u_2, \dots, a_{2s}+u_{2t})$.

Let $\sum(K)$ be the semigroup of all directions with the introduced above operation. This is a semi direct product of free semigroup over alphabet K and additive group $(K,+)$ which can be considered as modification of a free product $(K, +)$ with itself .

It is easy to check that the composition ${}^nC(w)$ and ${}^nC(u)$ coincides with ${}^nC(w \circ u)$. So transformations ${}^nC(w)$, $w \in \sum(K)$ form a subgroup $GA(n, q)$ of group $Aut\ K[x_1, x_2, \dots, x_n]$ which acts on the affine space $(K)^n$ as group $CG((K)^n)$ (affine Cremona group [36]) of all bijective polynomial maps of $(K)^n$ into itself. It means that the map $\acute{\eta}_n: \sum(K) \to GA(n, K)$ sending w to ${}^nC(w)$ is a homomorphism and its image $GA(n, K)$ is a stable one of degree 3, i.e. maximal degree of the map from this group is 3.

Similarly we can define homomorphism $\acute{\eta}$ of $\sum(K)$ onto $GA(K)$ acting on points of infinite graph $A(K)$.

For studies of walks corresponding to directions (y) of length m we extend the field K to commutative ring $K[y_1, y_2, \dots, y_m]$ and consider the special direction $(y)=(y_1, y_2, \dots, y_m)$ of graph $A_n(K[y_1, y_2, \dots, y_m])$ where m is even number.

Elements of this group are $\acute{\eta}_n(C(y))$ where $\acute{\eta}_n$ is a homomorphism of $\sum(K[y_1, y_2, \dots, y_m])$ onto $CG((K[y_1, y_2, \dots, y_m])^n)$.

Each of them can be written as a rule $x_i \to f_i(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m)$, $i=1,2,..n$. Degree of each polynomial in variables $x_1, x_2, \dots, x_n$ (deg_x) is bounded by *3*.

It possible to prove the following statement.

PROPOSITION 1 *Degree of f_i in variables $y_1, y_2, \dots, y_m$ $(deg_y(f_i))$ is i.*

TAHOMA PROTOCOL ([7] uses tame homomorphism $\acute{\eta}_n$ of $\sum(K)$ into $GA_n(K)$).

Alice selects parameters n and m and words $w_1, w_2, .,.. w_k$, $k>1$ and words u and $\boldsymbol{z}$ of finite even length from $\sum(K)$.

Let $u=(a_1, a_2, \dots, a_s)$. We refer to $Rev(u)=(-a_s+a_{s-1}, -a_s+a_{s-2}, \dots , -a_s+a_1 , -a_s)$ as a reversing string for u. It is easy to see that $\eta_n(uRev(u))$ is the unity of affine Cremona semigroup $CG(K^n)$.

Alice selects affine transformation $T_1 \in AGL_n(K)$ and $T_2 \in AGL_m(K)$ in '' general position" and computes T_1^{-1} together with T_2^{-1}. She forms $F_i = T_1 \acute{\eta}_n(uw_i Rev(u)) T_1^{-1}$ and $G_i = T_2 \acute{\eta}_m(zw_i Rev(z)) T_2^{-1}$ for $i=1,2,\dots,k$.

She sends pairs (F_i, G_i), $i=1,2,\dots k$ to Bob.

He uses formal alphabet $\{x_1, x_2,..., x_k\}$ to write word $x_{i(1)}^{k(1)}x_{i(2)}^{k(2)}...x_{i(s)}^{k(s)}$ of finite length **s.** Bob computes specialisations $F=F_{i(1)}^{k(1)}F_{i(2)}^{k(2)}...F_{i(s)}^{k(s)}$ and $G=G_{i(1)}^{k(1)}G_{i(2)}^{k(2)}...G_{i(s)}^{k(s)}$. He sends F to Alice but keeps $\boldsymbol{G}$ for himself.

Alice has to restore the standard form of G from F. She knows that standard projection of $A(n, K)$ onto $A(m, K)$ induces the homomorphism μ of $GA(n, K)$ onto $GA(m,k)$ for which $\mu(\acute{\eta}_n(w_i))= \acute{\eta}_m(w_i)$. Element F equals $T_1 \acute{\eta}_n(u) \acute{\eta}_n (w_{1(1)}^{k(1)}w_{i(2)}^{k(2)}...w_{i(s)}^{k(s)}) \acute{\eta}_n(u)^{-1}T_1^1$.

So Alice computes $\acute{\eta}_n (w_{1(1)}^{k(1)}w_{i(2)}^{k(2)}...w_{i(s)}^{k(s)})=F'$ because of her knowledge about T_1 and u. She applies μ to F' and gets $\acute{\eta}_m (w_{1(1)}^{k(1)}w_{i(2)}^{k(2)}...w_{i(s)}^{k(s)})=G'$. Finally Alice computes G as $T_2 \acute{\eta}_m(z)G'\acute{\eta}_m(Rev(z))T_2^{-1}$. The collision transformation G has standard form $x_i \rightarrow g_i (x_1 , x_2 ,...,x_m)$, $i=1, 2,..., m.$

SECURITY RESTS ON THE PROBLEM OF DECOMPOSITION OF G INTO WORD OF GENERATORS F_i, $i=12,...,k.$

IT IS POST QUANTUM INTRACTABLE.

This algorithm was presented in Security track of COMPUTING 2019 conference in London (see [8]).

Correspondents can use the concatenation of coefficients of g_i listed in the lexicographical order as a password for one time pad encryption. They can use the following

algorithm of generation of potentially infinite string of characters.

Let g be a cubical map from $CS_n(K)$ of kind $x_i \rightarrow g_i$. $i=1, 2,...,n.$ To simplify definitions we assume that n is even. We define $v(g)$ as tuple of coefficients of $g_1+g_2, ...+g_n$ written in front of terms $x_ix_jx_k$, $|\{i,jk\}|=3$ ordered in the lexicographical order. Length of $v(g)$ is C^3_n.

We define $reg(d)=d'$ for $d=(d(1),d(2),....,d(t)) \epsilon K^t$, $t \geq 2$ as the string with $d'(1)=d(1)$, $d'(2)=d(2)$, if i>.2 *then* $d'(i)=d(i)+d'(i-2)$ if $d(i)\neq 0$, and $d'(i)=d'(i-2)+1$ for the case $d'(i)=0$ **.**

Definition. *Blow-up of g* (*Blow(g)*) *is the map* $\acute{\eta}_1(reg(v(g)), \boldsymbol{t}= C^3_n$**.**

We can consider ${}^mBlow$ via application of *Blow* exactly m times, $m\geq 1$. Noteworthy that ${}^mBlow(g)$ is bijective cubical transformation,

Let ${}^mv(g)$ be the tuple $v({}^mu(g))$,

Application 1. So Alice can take modern implementation of quantum computer *(number of qubits can be rather small, 2 or 4 are sufficient numbers to play)* and use this machine to create **''***genuine***''** random sequence $P=(p(1), p(2),..., p(m(s))$ in the alphabet**.** She can elaborate common string $a=(a(1), a(2),..., a(s))$ together with Bob via a postquantum secure protocol.

Correspondents computes $g=T\acute{\eta}_n(reg(a))T'$ where even n and nonsingular matrices T,T' are agreed via open channel and start computation of $B= {}^lBlow(g) \epsilon CS_k(K)$ with $k\geq m(t).$

Alice takes tuple E of first $m(s)$ coordinates. She sends $E+P$ to Bob. He restores P.

Presented above algorithm allows correspondents to use one time pad encryption as many time as they want.
Assume that correspondents have common tuple of characters $(p=(p_1, p_2, \ldots, p_t)\epsilon K^t$ elaborated via some protocol (the seed). Instead of creation of potentially infinite string of characters from this seed they can use single computation *of* $\acute{\eta}_m(p)=G$ of kind $x_1 \rightarrow g_1$, $x_2 \rightarrow g_2, \ldots, x_m \rightarrow g_m$. So they take tuple u of nonzero coefficients of $g_1+g_2+\ldots g_m$ and use the string *reg(u)* or its part as password. The length of tuple *reg(u)* in the case of *m=128 and various t (*length of the word) is given by the following figure.

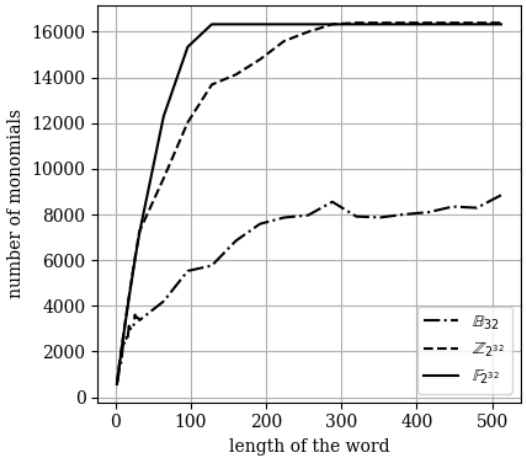


Fig. 1. Number of monomial terms of the cubic map induced by the graph *A(128, K)* for $K=F_q$ (-----), $K=Z_q$(- - -) , $q=2^{32}$ and Boolean ring *B(32)* (.-.-.-).

Application 2 (practical expansion of seed tuple in a single step). Assume that H is a cubical map $x_i \rightarrow h_i(x_1, x_2, \ldots, x_t)$, $i=1,2,\ldots, t$. It has a triangular structure. Let $h=h_1+h_2\ldots+h_t$. We can consider matrix $A=(a_{ij})$ where a_{ij} is coefficient of polynomial h in front of $x_1^2x_j$ if this coefficient differs from *0*, otherwise $a_{ij}=1$.

Let U be matrix with entries $u(i,j)$ such that $u(i,j)= a_{ij}$ for $j>i$, $u(i,i)=1$ and $u(i,j)=0$ for $i<j$.

Assume that L stands for the matrix with entries $l(i,j)$ such that $l(i,i)=1$ and $l(i,j)= a_{ij}$ for $i<j$ and $l(i,j)=0$ for $i>j$. We compute $T=LU=\Delta(H)$ together with T^{-1}.
We introduce $Cong(H)$ as element THT^{-1}.
We introduce *Blow'(G)* as *Cong(Blow(G))*. The usage of *Blow'(G)* instead of *Blow(G)* in described above algorithm of generation of potentially infinite

sequences of cubical bijective polynomials leads to creation of maps without obvious invariant subspaces.

Let $p=(p_1, p_2, \ldots, p_t)\epsilon K^t$, where parameter t is even. We consider $reg(p) \epsilon \sum(K)$, select "sufficiently large" number m and compute $Cong(\acute{\eta}_m(reg(p))=H\epsilon CG_m(K)$.

Let $v_m(p)$ be a string of nonzero coefficients of cubical map H ordered in the lexicographical order. We define $Zoom_{m,t}(p)$ as $reg(v_m(p))$. We denote the length of $Zoom_{m,t}(p)$ as $z(m,t)(p)$. Computer experiment shows that the value of this parameter practically depends on m and t and does not depend on the pseudorandom string p. In fact if t is ''sufficiently large" then practically we have the function from single variable m.

Table 1. Number of monomial terms z(m,t) of the cubic map induced by the graph $A(m, Fq)$. $q=2^{32}$

	length of the word t				
m	**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

Correspondents can use ''zoom operator'' several times.

REMARK. Instead of $Cong(g)$ correspondents can use the following modification of this operator. We can take string of coefficients $grad^2(g_1+g_2+\ldots+g_n)=a_1x_1+a_2x_2+\ldots+a_nx_n+a_0$ standing in front of monomial terms $\mathbf{x}_i$ and form tuple $(b_1,b_2,\ldots,b_n)$ with $b_i=a_i$ for $a_i\neq 0$ and $b_i=1$ for $a_i=0$. Secondly we consider affine transformation T of kind $x_1\rightarrow x_1+b_1x_2+b_2x_3+\ldots b_{n-1}x_n+b_n$, $x_j\rightarrow x_j$, $j=2,3,\ldots,n$. We define $Sparse(g)$ as TgT^{-1}.

Example 1.

Let us assume that Alice and Bob execute described above protocol and get collision map g from $R\ GA(m,K)R^{-1}$ where R is some matrix known for Alice and parameter m is even.

They use g as the seed for generation of potentially infinite string of characters. Alice use this string for the transfer of ''genuine'' random parameters $(r_1, r_2,\ldots r_s)$ with potentially infinite s. Let us assume that correspondent has to send his/her partner large tuple $p=(p_1, p_2,\ldots, p_1)$.

Correspondents can take integer parameter d of kind $clog_3(l)$ for some constant c.

They can agree on parameter $h=O(l)$ and form strings
$k(1)=(r_1, r_2, \ldots, r_h)$, $k(2)=(r_{h+1}, r_{h+1}, ,,, ,r_{2h}), \ldots,$
$k(d)=(r_{h(d-1)+1}, r_{h(d-1)+2}, \ldots, r_{hd})$.

They form transformations G_i of kind $Cong(\acute{\eta}_1(k(i)))$, $i=1.2,\ldots, d$.

Alice and Bob form $G(i)= Cong (\acute{\eta}_k(u(i))$, $i=1,2,\ r$. They will use composition E of $G(j)$, $j=1,2,\ldots, r$

Noteworthy that degree of E is about 3^r, where r is linear function from l. Parameter l is ''potentially infinite'' positive number. So degree of E is not bounded by constant.

This fact makes impossible the linearization attacks by adversary or other kind of attacks via interception of pairs of kind known plaintext/corresponding ciphertext.

To increase speed of encryption and decryption correspondents have to use the decomposition of E into $G(i)$ and representation of each $G(i)$ as $\Delta(u(i))\ u(i)\ \Delta(u(i))^{-1}$ where $u(i)=\acute{\eta}_1(k(i)))$.

So for the encryption of the plaintext p of length l correspondent has to execute computation of the value of $G(i)$ in a given vector h times.

The computation of value of linear transformation
$\Delta(u)$ or its inverse takes $O(l^2)$. Computation of each $u(i)$ takes $O(l^2)$ in the case when the string $k(i)$ is known. So encryption with E takes $O(l^2 ln(l))$. .
Noteworthy that the knowledge of $rev(k(i))$ allows computation of value for $u(i)^{-1}$ with the speed of computation $u(i)$. So encryption and decryption take the same time.

Noteworthy that speed of proposed nonlinear encryption is close to execution time of encryption with linear map which is $O(l^2)$.

Example 2.

Let us consider modification of algorithm described in the previous example. We construct strings $k(1),k(2),\ldots,k(d)$ of length $O(1)$. The usage of operator *Sparse* instead of *Cong* allows us to construct $H_i= Sparse(\acute{\eta}_1(k(i)))$, $i=1.2,\ldots, d$ instead of G_i.

New encryption E' is defined as the composition of H_1. The execution of each H_i_takes linear time $O(l)$.

So the execution time of E' is close to the speed of reading the file.

4. On quadratic multivariate cryptography.

In July 2020 the list of algorithms selected for the Third Round of NIST competition was published. In the case of digital signatures preliminary analysis indicates some advantages of algorithms based on quadratic public rules of Multivariate Cryptography. These systems provide the smallest sizes of the used hashed messages and digital signatures.

Recall that classical multivariate signature system is based on public quadratic map P' of vector space $\boldsymbol{F_q^m}$ onto $F_q{}^n$ of kind $P'= T_1PT_2$ where the

map P is given by rule $x_i \rightarrow f_i(x_1, x_2, \dots, x_m)$, $i=1,2,\dots,n$ defined by quadratic polynomials f_i and bijective affine transformations T_1, T_2 of spaces $F_q{}^m$ and $F_q{}^n$**.** Users Alice and Bob use selected encryption function F and hash function which creates hash vector $H(c)$ from vector space $F_q{}^m$. Alice writes the plaintext p and computes corresponding ciphertext c. The knowledge of the decomposition T_1PT_2 and private algorithm to compute value of P^{-1} in a given point allows Alice to compute some reimage $P'^{-1}(H(c))=(u_1, u_2, \dots, u_n)=u$ of $H(c)$ (so called *signature)* and to send u to Bob via an open channel. He checks the identity $P'(u)=H(c)$. This is his confirmation that ciphertext is sent by Alice. Finally he decrypts via his decryption tool. The security of presented above algorithm rests on the complexity of the problem of computation of reimage for non-bijective P'. This is a well known general *NP* hard problem.

We can change finite field for general commutative ring.

Noteworthy that in the case of Unbalanced Oil and Vinegar system the partition of variables into two parts of '' oil'' and ''vinegar'' unknowns and special form of P allow Alice to compute element from $P^{-1}(H(c))$. She uses a specialisation of ''vinegar'' variables via substitution of pseudorandom parameters, such specialisation reduces the search for reimage via solving the system of linear equations.

We start the search for the options to modify general digital scheme of multivariate cryptography which eliminates attacks investigated in [10] and [11]. Additionally we search for modifications of public keys of quadratic multivariate cryptography. These schemes use system of nonlinear polynomial equations

$${}^1p(x_1,x_2,\dots,x_n) = {}^1p_{i,j} \cdot x_ix_j + {}^1p_i \cdot x_i + {}^1p_0$$

$${}^2p(x_1,x_2,\dots,x_n) = {}^2p_{i,j} \cdot x_ix_j + {}^2p_i \cdot x_i + {}^2p_0$$

…

$${}^mp(x_1,x_2,\dots,x_n) = {}^mp_{i,j} \cdot x_ix_j + {}^mp_i \cdot x_i + {}^mp_0$$ where ${}^kp_{i,j}, {}^kp_i$ are elements of selected commutative ring K. The transformation rule P of the tuple $(x_1,x_2,\dots,x_n)$, into $({}^1p(x_1,x_2,\dots,x_n), {}^2p(x_1,x_2,\dots,x_n), \dots, {}^mp(x_1,x_2,\dots,x_n))$ has to be supported by the algorithm of computation of its reimage. For example, in the case of ''oil and vinegar'' variables $x_1,x_2,\dots,x_n$ are subdivided into two groups and specialization of representatives of one of them converts system of quadratic equations to solvable system of linear equations.

The quadratic multivariate cryptography map consists of two bijective affine transformations S and T of dimensions n and m, and a quadratic element P' of kind SPT**.** The standard form of P' has to be given publicly.

So public user Bob can compute image of vector $(v_1,v_2,\dots,v_n)$ in time $O(n^3)$.

The key holder Alice knows the decomposition of *P'* into *SPT*. We assume that this knowledge allows Alice to compute the reimage in time $O(n^2)$.

That condition holds for the majority of investigated examples of multivariate schemes.

One of the approaches for modification is based on the idea that the map *P'* is not given publicly [12].

In this paper we assume that correspondents execute the protocol of non-commutative cryptography based on the platform of stable multivariate transformations of degree 2 in *n* variables (see [13]) or degree 3 as in the case of presented platform *GA(n,k)*.

They extract the collision map ***G*** from the semigroup $CS_n(K)$ and extract the tuple *v(G)* defined as the list of coefficients in font of terms $x_ix_jx_k$ where *i, j, k* are different *(deg (G)=3)* or terms x_ix_j , $i \neq j$ (*deg (G)=2)* .

%%%%%They use tuple *v(G)* as the ''seed'' for elaboration of potentially infinite string of characters $(p_1, p_2,....p_s)$. This string allows Alice to deliver''genuine'' random string $(r_1, r_2,...., r_s)$ to Bob.

Let *P'* be given by quadratic polynomials ${}^ip'(x_1, x_2,..., x_n)$, $i=1,2,...m$.

Each polynomial is presented as string ${}^ia=({}^ia_1, {}^ia_2,..., {}^ia_k)$, $k=n(n-1)/2+n+1$ of its coefficients written in a standard lexicographical order. Alice forms vectors $r(1)=(r_1, r_2,..., +r_k)$, $r(2)=r_{1+k}+r_{2+k}+...+r_{2k}$,..., $r(m)=r_{1+k(m-1)}+r_{2+k(m-1)}+...+r_{mk}$. She sends vectors ${}^ia+r(i)$, $i=1,2,...,k$ to Bob. He restores polynomials ${}^ip'(x_1, x_2,..., x_n)$, $i=1,2,..., m$.

So Alice and Bob share *P'* and keep this map in their private storages *The map P' is not given publicly.*

Correspondents execute described above algorithm of digital signatures in secure private mode.

OPTIONS FOR ADVERSARY.

Adversary can try to intercept several pairs of kind (tuple $P'(v_1, v_2, ,...,v_n)$, corresponding reimage $(v_1, v_2,..., v_n)$). He/she treats coefficients of the quadratic map as $(n(n-1)/2+n+1)$ variables.

One interception provides *m* equations.

Adversary need more than $n(n-1)/2$ pairs of kind the image/corresponding reimage of *P'*. If he/she gets more pairs than number of equations then adversary has a chance to solve the system and transfer standard form of *P'* from private shadow to his own possession.

The remaining part of the job is cryptanalytic studies of explicitly given *P'* to find the procedure of finding the reimage for this map.

REMARK. Correspondents can agree on the execution of signature procedure at most $[n^2/4]$ times.

After reaching this number of exchanges correspondents have to change the map *P'* for other quadratic multivariate rule *P''*. The following options have to be considered.

(a) Alice works with the same P but change S and T for other pair (S', T') of bijective affine transformations. She uses $P''=S'PT'$.

(b) Alice changes internal parameters of P and gets the map Q with changed procedure of reimage computation. She uses decomposition $P'' =S'QT'$.

After choiosing the map Alice can select other part of common sequence $(r_1, r_2,..., r_s)$ for the safe delivery of P'' to Bob. If necessary Alice and Bob can use other session of the protocol to construct new parameter ${}^{i}a'$ together with other session of quantum computation to produce new string of characters r'_i.

REMARK 1. *Described above method can be used for maps P' of bounded degree >2.*

REMARK 2.

The usage of quantum computers and parameters r_i means that the described digital signature scheme belongs to the list of algorithms of Quantum Cryptography.

REMARK 3.

Instead of parameters r_i correspondents can simply use elements a_i , which are computed as polynomials of exponentially growing degrees. This change leads to deterministic algorithms of Postquantum Cryptography.

REMARK 4. *For each n we construct quadratic stable subgroup $E_n(K)$ of affine Cremona group $CG_n(K)$. So we can use presented above protocol with quadratic platform (see [13] and further references).We get complexity $O(n^7)$ instead of $O(n^{13})$.*

This stable platform is also constructed in terms of expanding graphs. Corresponding families of graphs are geometrical expanders in sense of Noga Alon. They are of unbounded degree. These platforms contain large noncommutative subgroups generated by elements of exponential order.

5. Stable Chaos in the case of intergrity ring with unity of characteristic zero.

Affine Cremona groups in the cases of $K=C$ and $K=R$ are classical objects of Algebraic Geometry. Let us discuss more general case of integrity ring with unity of characteristic zero.

Assume that $w=(d_1, d_2,...,d_t)$ is an element of $\sum(K)$ with $d_t\neq 0$. In this case $\acute{\eta}(w)\epsilon CG_n(K)$ is a cubical map of infinite order and cyclic group generated by TgT^{-1} with $T\epsilon AGL_n(K)$ is an infinite stable group of degree 3

Let us assume that we have several elements $w(i)$ with the last coordinate different from zero. Then $<\acute{\eta}_n(w(1)), \acute{\eta}_n(w(2)), \acute{\eta}_n(w(m))>$, $m>1$ is an infinite stable subgroup of cubical transformations with infinite generators.

Let g be a cubical transformation of $CS_n(K)$ then elements $CongBlow^i(g)$, $i>1$generate a cyclic stable subgroup of $GA(n, K)$.

Noteworthy that $<Cong(Blow)^i(g_1), Cong(Blow)^i(g_2)>$ is not stable subgroup but for the majorty of pairs g_1, g_2 of cubical transformations composition *of* $Cong(Blow)^i(g_1)$ and $Cong(Blow)^i(g_2)$ has degree 9.
Studies of stable subgroups of affine Cremona groups $CG_n(K)$ is an interesting task. Note that all algorithms presented in the paper have the same complexity estimations counted via numbers of basic operatio (+, ◦) of general commutative rings. In the case of integrity rings K , $1<K<R$ the absolute values of polynomial coefficients of polynomial maps $\acute{\eta}_n(w)$ are growing fast with the growth of n or length l of the word w.

So in many cases memory restrictions of the computer do not allow to implement the computation of the map.

6. Conclusions

Constructions of analogs of Diffie Hellman protocol for Post Quantum Cryptography is an important direction of Noncommutative Cryptography (see [17]-[35]). Some of suggested protocols use groups or semigroups given via generators and relations as platforms for the protocol. We work in the area of intersection of Noncommutative and Multivariate cryptography without the usage of methods of Combinatorial Group Theory or its generalization on Semigroups. As platforms for protocol we use special subgroups and subsemigroups of affine Cremona group $CG_n(K)$ (see [36]) which is a collection of all endomorphisms of $K[x_1, x_2,..., x_n]$. Each element from $CS_n(K)$ is presented in its standard form $x_i \rightarrow f_i(x_1, x_2,..., x_n)$, $i=1,2,...,n$ where monomial terms of f_i are listed accordingly lexicographical order. In section 3 we present the protocol proposed in [7]. It uses the properties of progective limit $GA(K)$, $n=2,3,...$ defined via the family of groups $GA(n, K)$ constructed via known small world graphs $A(n, K)$. Let $A(K)$ be the projective limit of $A(n,K)$. We introduced the semigroup of walks $\sum(K)$ on $A(K)$ and homomorphisms $\acute{\eta}:\sum(K)\rightarrow GA(K)$, $\acute{\eta}_n:\sum(K)\rightarrow GA(n,K)$, $\mu:A(K)\rightarrow A(n,K)$ forming commutative directed triangle. The protocol uses hidden conjugates of $GA(n, K)$ and $GA(m,K)$,$n>m$ and hiddent homomorphism between them. The collision element g from $CG_m(K)$ has degree 3.

The security of protocol rests on the problem of decomposition of $h \in CG_n(K)$ into composition of known generators.

This problem is more general than Conjugacy Power Problem of Noncommutative Cryptography. It is untractable even in the case of the usage of Turing Machine and Quantum Computer.

Complexity of this asymmetric protocol for public user Bob is $O(n^{13})$.

The main goal of the paper is safe expansion of ''seed '' g on finite sequence of cubical $g_i = Blow^i(g) \in CG_{n(i)}(K)$ where sequence $n(1)<n(2)<... n(k)$ is defined by the rule $n(i+1) = C^3_{n(i)}$, $n(0)=n$. Coefficients of $g(i)$ are polynomial expressions from seed variables of degree $n(1)+n(2)+...+n(k)$. The complexity of algorithm is $O(n(k)^4)$. Correspondents can use strings of coefficients of g_i or their parts as passwords of symmetrical cryptography.

It means that they need just a single usage of expensive Tahoma protocol and to use iterative expansion to get larger string of common characters.

In section 4 we consider application of these results for the "privatization" of algorithms of Multivariate Cryptography, i. e. El Gamal type transition of public key data into safe private zone.

Of course further investigation of coordinates $R(K)$ is needed with the usage of various NIST tests on pseudo randomness.

Summary

Discovery of explicit constructions of expanding graphs (sequence CD(n, q) and modifications of this family) of increasing girth were used in many constructions of Extremal Graph Theory and Theory of LDPC codes (see upper bounds for cages in [37] or papers [38], [39] on Coding Theory),.

It also has an impact on Algebraic Geometry, first constructions of *large stable subgroups of affine Cremona group CG_n(K) over general commutative ring K* had been obtained . In particular large groups of cubical (or even quadratic) transformations of a free module were found.

Discovery of homomorphism of $\sum(K)$ (semigroups of walks on infinite q-regular tree in the case $K=F_q$) onto stable group G leads to Construction of analog of Diffie-Hellman protocol which is secure in sense of Post Quantum Cryptography. This result is based on the ideas of NONCOMMUTATIVE CRYPTOGRAPHY. Possibility of the change of finite field for general commutative ring were considered.

So we have symbiotic combination of this protocol with one time pad or other symmetric encryption algorithm.

Multiple usage of mentioned above homomorphisms can be used for the secure expansion of the output of postquantum secure protocol *to potentially infinite sequences* g_n of cubical elements of affine Cremona groups $CG_n(K)$ where n tends to infinity. One can extract special tuples of coefficients of maps g_m for their usage for safe delivery of pseudorandom sequences of characters produced by quantum computer. We discuss the usage of these sequences for the delivery of multivariate maps capable to provide digital signature schemes and schemes for the message exchange.

The content of the paper was presented by author at the international conference ‘’Modern Stochastic: Theory and Applications, 5’’, Kyiv, June 2021 (section "Reliability, queueing and information security" dedicated to the development of scientific ideas and research of academician of National Academy of Sciences of Ukraine ***Igor Kovalenko*** (16.03.1935 – 19.10.2019)).

References

1 A. Grzesik, D. Kr´al’, L. M. Lov´asz, Elusive extremal graphs, preprint (2018), arXiv:1807.01141

2, N Hoory, A. Linial, A.Wigderson. Expander graphs and their applications, Bull. Amer. Math Soc., 43, pp 439-561, 2006

3.V. A. Ustimenko, U. Romanczuk, On Dynamical Systems of Large Girth or Cycle Indicator and their applications to Multivariate Cryptography, in "Artificial Intelligence, Evolutionary Computing and Metaheuristics ", In the footsteps of Alan Turing Series: Studies in Computational Intelligence, Volume 427/2013, 257-285.

4. V. Ustimenko, U. Romanczuk, On Extremal Graph Theory, Explicit Algebraic Constructions of Extremal Graphs and Corresponding Turing Encryption Machines, in "Artificial Intelligence, Evolutionary Computing and Metaheuristics ", In the footsteps of Alan Turing Series: Studies in Computational Intelligence, Vol. 427, Springer, January , 2013, 257-285.

5. V. Ustimenko, On extremal graph theory and symbolic computations, Dopovidi National Academy of Sci, Ukraine, 2013, N2, pp 42-49.

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

7. V. Ustimenko, On new symbolic key exchange protocols and cryptosystems based on hidden tame homomorphism,. *Dopov. Nac. akad. nauk Ukraine,2018, n 10, pp.26-36.*

8. V. Ustimenko, M. Klisowski , On Noncommutative Cryptography with cubical multivariate maps of predictable density, Proceedings of ‘’Computing 2019’’ conference, London, 16-17, July , Volume 2, Part of Advances in Intelligent Systems and Computing (AISC, volume 99, pp, 654-674.

9. O. Pustovit, V.Ustimenko, A new stream algorithms generating sensetive digests of digital documents, Mathematical modelling in economics, 2019, N3, P. 18-33

10. Shuhei Nakamura and Yasuhiko Ikematsu and Yacheng Wang and Jintai Ding and Tsuyoshi Takagi. Shuhei Nakamura and Yasuhiko Ikematsu and Yacheng Wang and Jintai Ding and Tsuyoshi Takagi, New Complexity Estimation on the Rainbow-Band-Separation Attack, ePrint Archive: Report 2020/703.

11.Jintai Ding and Joshua Deaton and Vishakha and Bo-Yin Yang, The Nested Subset Differential Attack: A Practical Direct Attack Against LUOV which Forges a Signature within 210 Minutes, ePrint Archive: Report 2020/967

12. V. Ustimenko, On Multivariate Algorithms of Digital Signatures on Secure El Gamal Type Mode. ePrint Archive, Report 2020, 984.

13.V. Ustimenko, On the usage of postquantum protocols defined in terms of transformation semigroups and their homomophisms, Theoretical and Applied Cybersecurity, National

Technical University of Ukraine "Igor Sikorsky Kiev Polytechnic Institute", Volume 1, No. 2, pp. 32-44 (2020).
14, V. Ustimenko, On Multivariate Algorithms of Digital Signatures of Linear Degree and Low Density, ePrint Archive: Report 2020/1015.
15, V.Ustimenko, On Multivariate Algorithms of Digital Signatures Based on Maps of Un bounded Degree Acting on Secure El Gamal Type Mode., Report 2020/1116.
16, N.Alon, Eigenvalues,geometric expanders.sorting in rponds,and Ramsey Theory, Combinatorica,6 (3), 1986,207-219,
17, D. N. Moldovyan, N. A. Moldovyan, A New Hard Problem over Non-commutative 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.
18. L. Sakalauskas., P. Tvarijonas , A. Raulynaitis, Key Agreement Protocol (KAP) Using Conjugacy and Discrete Logarithm Problema in Group Representation Level}, INFORMATICA, 2007, vol. !8, No 1, 115-124.
19. V. Shpilrain, A. Ushakov,Theconjugacy search problem in public key cryptography: unnecessary and insufficient,Applicable Algebra in Engineering, Communication and Computing, August 2006, Volume 17, Issue 3–4, pp 285–289.
20. 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.
21. Alexei Myasnikov; Vladimir Shpilrain; Alexander Ushakov (2008). Group-based Cryptography. Berlin: BirkhäuserVerlag.
22. Zhenfu Cao (2012). New Directions of Modern Cryptography. Boca Raton: CRC Press, Taylor & Francis Group. ISBN 978-1-4665-0140-9
23. Benjamin Fine, et. al. "Aspects of Non abelian Group Based Cryptography: A Survey and Open Problems". arXiv:1103.4093.
24. Alexei G. Myasnikov; Vladimir Shpilrain; Alexander Ushakov (2011). Non-commutative Cryptography and Complexity of Group-theoretic Problems. American Mathematical Society.
25. Anshel, I., Anshel, M., Goldfeld, D.: An algebraic method for public-key cryptography. Math. Res.Lett. 6(3–4), 287–291 (1999).
26. Blackburn, S.R., Galbraith, S.D.: Cryptanalysis of two cryptosystems based on group actions. In: Advances in Cryptology—ASIACRYPT ’99. Lecture Notes in Computer Science, vol. 1716, pp. 52–61. Springer, Berlin (1999).
27. C Ko, K.H., Lee, S.J., Cheon, J.H., Han, J.W., Kang, J.S., Park, C.: New public-key cryptosystem using braid groups. In: Advances in Cryptology—CRYPTO 2000, Santa Barbara, CA. Lecture Notes in Computer Science, vol. 1880, pp. 166–183. Springer, Berlin (2000)
28. Maze, G., Monico, C., Rosenthal, J.: Public key cryptography based on semigroup actions. Adv.Math. Commun. **1**(4), 489–511.
29. P.H. Kropholler, S.J. Pride , W.A.M. Othman K.B. Wong, P.C. Wong, Properties of certain semigroups and their potential as platforms for cryptosystems, Semigroup Forum (2010) 81: 172–186.
30. A. Lopez Ramos, J. Rosenthal, D. Schipani, R. Schnyder, Group key management based on semigroup actions, Journal of Algebra and its applications, vol.16 (2019).
31. Gautam Kumar and Hemraj Saini, Novel Noncommutative Cryptography Scheme Using Extra Special Group, Security and Communication Networks ,Volume 2017, Article ID 9036382, 21 pages, https://doi.org/10.1155/2017/9036382

32. V. A. Roman'kov, A nonlinear decomposition attack, Groups Complex. Cryptol. 8, No. 2 (2016), 197-207.

33. V. Roman'kov, An improved version of the AAG cryptographic protocol, Groups, Complex., Cryptol, 11, No. 1 (2019), 35-42.

34. A. Ben-Zvi, A. Kalka and B. Tsaban, Cryptanalysis via algebraic span, In: Shacham H. and Boldyreva A. (eds.) Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part I, Vol. 10991, 255{274, Springer, Cham (2018).

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

36.. Max Noether, Luigi Cremona , Mathematische Annalen 59, 1904, p. 1–19.

37. F. Lazebnik, V. Ustimenko and A. Woldar, New upper bound on the order of cages, Electronic Journal of Combinatorics, Volume 4 (1997), No. 2, Paper R13.

38.P. Guinnand and J.Lodge, Tanner type codesarising from large girth graphs, Proceedings of the 1997 Canadien Workshop on Information Theory (CWIT 97), Toronto,pp.5-7, June 1997.

39. T. Shaska, V. Ustimenko On the homogeneous algebraic graphs of large girth and their applications, Linear Algebra and its Applications Article, Volume 430, Issue 7, 1 April 2009, Special Issue in Honor of Thomas J. Laffey.