On quadratic equations of q-regular tree and their applications in Graph Theory and Cryptography.

Vasyl Ustimenko[1][0000−0002−2138−2357] and Tymoteusz Chojecki[2][0000−0002−3294−2794]

[1] Royal Holloway University of London Vasyl.Ustymenko@rhul.ac.uk
[2] Maria Curie-Skłodowska University tymoteusz.chojecki@umcs.pl

Abstract. Graphs $D(n,q)$ and their connected components $CD(n,q)$ were defined 30 years ago. We observe shortly their applications to Extremal Graph Theory, Spectral Graph Theory, Algebraic Graph Theory, Symmetric Cryptography and Theory of Low Density Parity Check Codes. We introduce several new algorithms of Noncommutative Cryptography based on this graphs of large girth, In particular we propose modification of Diffie-Hellman protocol in terms of semigroup of walks of even length on the forest obtained as projective limit of $D(n,q)$ and the homomorphic image of this monoid, acting on the vector space $(F_q)^n$ as transformation group $G(n,q)$ of cubical polynomial transformation. The protocol allows users to elaborate collision vector from $(F_q)^n$ in time $O(n^2)$. The security of this schemes rests on the complexity of Conjugacy Power Problem for affine Cremona semigroup of automorphisms of $F_q[x_1,x_2,\ldots,x_n]$. Inverse protocol of El Gamal type allows to use these scheme for encryption or creating of digital signature. Several obfuscations of these algorithm are given.

Keywords: Application of graphs of large girth · Noncommutative Cryptography · Graph based key exchange protocols · Symbolic Computations

1 Introduction

Let us consider infinite dihedral group W given by generators s_1, s_2 and relations ${s_1}^2 = e$ and ${s_2}^2 = e$. Its Weyl geometry is the bipartite graph with partition sets $P = \{g\langle s_1\rangle | g \in W\}$ (white vertices in Fig. 1) and $L = \{g\langle s_2\rangle | g \in W\}$ (black vertices in Fig. 1) corresponding to binary relation I such that $\alpha I \beta$ if and only if the intersection of $\alpha \in P$ and $\beta \in L$ is nonempty. This graph is the binary tree depicted in Fig 1.

It is known that Tits geometry Γ of the adjoint group G of infinite dimensional Kac-Moody algebra with the Weyl group as above defined over finite field F_q is a $q+1$-regular forest (see [1] and Fig. 2 for $q=2$) Let B^+ (B^-) be Borel subgrops of containing root subroups corresponding to positive (negative) roots. Then Tits geometry Γ is the $q+1$-regular bipartite graph with partition sets $P' = \{gP_1 | g \in G\}$, $L' = \{gP_2 | g \in G\}$ where $P_i = B^+\langle s_i\rangle B^+$, $i = 1,2$ are standard maximal parabolic subgroups of G.

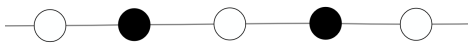


Fig. 1. Binary tree

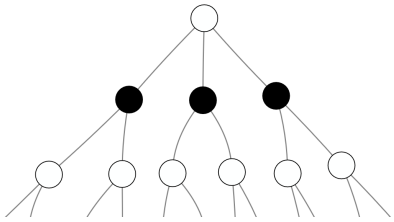


Fig. 2. Cubic tree

In [2] (see also [2], [3]) was noticed that the orbits F_i of B^- containing P_i are infinite dimensional vector spaces and incidence of element from $F_1 \cup F_2$ can be given by quadratic equations. The incidence structure on them with the set of points F_1, set of lines F_2 and the restriction I' of I on them is a bipartite q -regular forest.

In case of root system $\tilde{A}_1$ coordinates of vector spaces F_i corresponds to negative roots of kind α, β, $k(\alpha) + k(\beta)$, $(k+1)\alpha + k\beta, k\alpha + (k+1)\beta$, $k \geq 1$ where α and β are negative simple roots. So in the basis of α, β indexes presented as elements of the set Ω which consist on $(1,0), (0,1)$, $(k,k), (k+1,k), (k,k+1)$, $k \geq 1$. We can assume that points are indexed by elements of $\Omega - \{(0,1)\}$ and indexes of lines are elements of $\Omega - \{(1,0)\}$. In fact indexes of kind (k,k) corresponds to imaginary roots of $\tilde{A}_1$ and other indexes correspond to real roots. In [5] authors add twining roots $(i,i)'$ for imaginary roots of kind (k,k) and use extra variables to simplify the quadratic system of equations. It allows them to define an infinite regular forest $D(q)$ with points $(p_1, p_2, \dots, p_n, \dots)$ and lines $[l_1, l_2, \dots, l_n, \dots]$ and incidence relation given by the following equations:

$$\begin{aligned}
&p_2 - l_2 = l_1 p_1,\\
&p_3 - l_3 = l_1 p_2,\\
&p_4 - l_4 = p_1 l_2,\\
&p_i - l_i = p_1 l_{i-2},\\
&p_{i+1} - l_{i+1} = p_{i-2} l_1,\\
&p_{i+2} - l_{i+2} = p_i l_1,\\
&p_{i+3} - l_{i+3} = p_1 l_{i+1},
\end{aligned} \tag{1}$$

where $i \geq 5$, $i \mod 4 = 1$

The quadratic equations of single tree $CD(q)$ of $D(q)$ for odd q can be also written. They are written as conditions on points and lines given via quadratic system of equations in [6].

Let $D(n,q)$ ($CD(n,q)$) be the homomorphic image of $D(q)$ ($CD(q)$ respectively) under the homomorphism of deletion of coordinates of points and lines of $D(q)$ with indexes that $> n$ (see [7]). During last 30 years many important applications of these graphs to Extremal Graph Theory ([7], [8] and further references), Spectral Graph Theory (see [8] and further references) and Algebraic Graph Theory ([8], [9], [10]), Theory of LDPC Codes (see [11], [12], [13]) and Cryptography (see [14], [15], [8], [10] and furthere references).

In this paper we present new examples of such application - new efficient key exchange protocols of Noncommutative Cryptography and El Gamal type cryptosystems of Postquantum Cryptography to encrypt plaintexts with the speed $O(n^2)$. Many of applications are motivated by the fact that the girth of $D(n,q)$ is at least $n+5$. Recall that the girth of simple graph is the length of its minimal cycle. We can take any commutative ring K and consider the graphs $D(n,K)$ obtained via the change of F_q for K (see [14]). Alternative reseach on symmetric graph based cryptography can be found in [16]-[21].

In paper [14] was proven that in the case of integral domain K the girth of $D(n,K)$ is bounded below by $n+5$. So we define our algorithms in terms of $D(n,K)$ for finite commutative ring K.

2 On protocols of postquantum cryptography and subgroups of affine Cremona group.

Communication Theory widely uses finite commutative rings $(K,+,\times)$ for the representation of information pieces as tuples of kind $v=(p_1,p_2,\dots,p_n)\in K^n$ where coordinates p_i are elements of the alphabet K. Natural examples of commutative rings are modular arithmetic Z_{256}, finite field F_{256} order of which coincides with the size of binary alphabet. Family of commutative rings of kind Z_p for prime p and Z_{pq} for two prime numbers p and q are popular because of their use in Diffie-Hellman protocol and RSA algorithm.

Passwords in form of tuples v are used in symmetric encryption and as access data to use the resources of Information System. Key establishment algorithm is a secure procedure which allows correspondents Alice and Bob elaborate common tuple of kind $v=(v_1,v_2,\dots,v_k)$ with coordinates from finite alphabet K.

Diffie Hellman algorithm, which use generator a of cyclic subgroup in the multiplicative group Z_p^*, $(p-1,a)=1$ with the output b can be used for key establishment. Alice selects her private parameter $k(A)$. She computes $g(A)=a^{k(A)}$ and sends this element to Bob. He chooses his private key $k(B)$ computes $g(B)=a^k(B)$ and sends it via open channel to Alice. At the next stage Alice computes the collision element b as $(g^k(B))^{k(A)}$ and Bob computes it as $(g^k(A))^{k(B)}$. Piece of information b can be naturally converted into the tuple.

Correspondents select $d, d<p$ and used the presentation of $b=b_0+b_1d+\dots b_sd^s$, where b_i are elements of Z_d.

Other approaches to key establishment can be found in [22]-[27].

The security of Diffie-Hellman protocol (DH) rests on the complexity of Discrete Logarithm problem for Z_p^* which is NP hard for large p.

Adversary has to solve one of the eqations $a^x = g(A)$ or $a^x = g(B)$ in the group Z_p^* to break the procedure. Theoretical option to solve this problem in polynomial time on Quantum Computer was discovered by Peter Shor. It makes DH key establishment algorithm insecure in our Post-Quantum Era. Note that Diffie Hellman algorithm can be implemented with the generator a from the semigroup S. This implementation heavily depends on the way of presenting S in the memory of Turing Machine. If we change the group Z_p^* for isomorphic additive Z_{p-1} the discrete logarithm problem transforms to simple Diophantine equation. One of the ideas of Noncommutative Cryptography is to develop postquantum secure protocols with use of two or more generators non commuting generators of the semigroup. The following scheme of Twisted Diffie Hellman protocol proposes to use three non commuting generators g, h and h^{-1} of monoid S, which is a semigroup with unity, accordingly presented below logical scheme. Alice takes positive integers $k(A)$ and $r(A)$ and forms the *standard form* of $h^{-r(A)}g^{k(A)}h^{r(A)} = g_A$ (list of its monomial terms). Bob takes $k(B)$ and $r(B)$ and forms $h^{-r(B)}g^{k(B)}h^{r(B)} = g_B$ in its standard form. They exchange g_A and g_B and compute collision element X as ${}^Ag = h^{-r(A)}{g_B}^{k(A)}h^{r(A)}$ (Alice) and ${}^Bg = h^{-r(B)}{g_A}^{k(B)}h^{r(B)}$ (Bob).

Researchers hope that the implementation of this scheme with special monoid $S = M$ as a platform converts this scheme to secure postquantum protocol. Several monoids defined as abstract groups presented via generators and relations turned out to be not appropriate for secure implementations.

General concepts and constructive examples of potential cryptosystems of algebraic nature presented in [28]-[43]. Noncommutative Cryptography has own history, it is the area of intensive new research.

Corresponding cryptanalysis can be found in [44]-[50]. Anyway the search for appropriate platforms defined in terms of Combinatorial Group Theory is continue.

Note that adversary has to solve the Conjugacy Power Problem to solve one of the equations $h^x g^y h^{-x} = g_A$ or $h^x g^y h^{-x} = g_B$ for unknowns x and y.

We suggest the following Protocol 1 (P_1).

2.1 Protocol P_1 Twisted Diffie Hellman protocol mode on transformation semigroups.

Let us assume that M acts on some finite set N which is "sufficiently large".

Alice and Bob selects pseudorandom or genuinely random m from N together with generators g, h and h^{-1} from M. So they compute g_A and g_B accordingly to the described above scheme. After that Alice computes consecutively

$$h^{-1}(m) = {}^1m, h^{-1}({}^1m) = {}^2m, \ldots, h^{-1}({}^{r(A)-1}m) = a,$$

$$g_B(a) = {}^1a, g_B({}^1a) = {}^2a, \ldots, g_B({}^{k(A)-1}a) = a_1$$

and

$$h(a_1) = {}^1a_1, h({}^1a_1) = {}^2a_1, \ldots, h({}^{r(A)-1}a_1) = a_2.$$

Bob computes

$$h^{-1}(m) = {}^1m, h^{-1}({}^1m) = {}^2m, \ldots, h^{-1}({}^{r(B)-1}m) = b;$$

$$g_A(b) = {}^1b, g_A({}^1b) = {}^2b, \ldots, g_A({}^{k(B)-1}b) = b_1$$

and

$$h(b_1) = {}^1b_1, h({}^1b_1) = {}^2b_1, \ldots, h({}^{r(A)-1}b_1) = b_2.$$

They get the collision element $c = a_2 = b_2$.

In fact correspondents can apply elaborated $g(A)$ and $g(B)$ to several pseudorandom m_i, $i = 1, 2, \ldots, k$ from N.

If we take N as affine space K^n where K is finite commutative ring we get a key establishment algorithm.

Famous affine Cremona semigroup ${}^nCS(K)$ (see [51] and [52], [53] and further references) is a natural monoid acting on K^n.

Affine Cremona Semigroup ${}^nCS(K)$ is defined as endomorphism group of polynomial ring $K[x_1, x_2, \ldots, x_n]$. It acts naturally on the affine space $(K)^n$ as semigroup of polynomial transformation.

Element σ of the semigroup can be given via its values on variables, i. e. as the rule $x_i \to f_i(x_1, x_2, \ldots, x_n)$, $i = 1, 2, \ldots, n$. This rule induces the map

$$\sigma' : (a_1, a_2, \ldots, a_n) \to (f_1(a_1, a_2, \ldots, a_n), f_2(x_1, x_2, \ldots, x_n), \ldots, f_n(x_1, x_2, \ldots, x_n))$$

on the vector space $(K)^n$. We assume that σ is given in its standard form which is the list of f_i written as sums of their monomial terms ordered lexicographically. We define the density of f_i as the number of their monomial terms and density $den(\sigma)$ of endomorphism σ as maximum of densities of f_i. Degrees and densities of multivariate maps make an impact on the complexity of the compositions of two elements.

The Conjugation Power Problem in the Case of affine Cremona is unsolvable in polynomial time even with the use of Quantum Computing. Computer algebra of multivariate transformation implementations does not include yet effective quantum computations. In case of use of Turing machines the computation of the composition of two multivariate maps is very costly because of the product of two elements of degree r and s has degree rs. Recall that degree of σ is the maximum of degrees of f_i, It means that n-th degree of nonlinear element usually has exponential size and its computation is unfeasible. So we construct a subgroup $G(n, K)$ of cubic transformations of ${}^nCS(K)$ in the next section and will use it as platform for the implementation of the Twisted Diffie -Hellman protocol for monoids acting on the affine space K^n.

In fact we will use the following modification of scheme (1).

2.2 Protocol 2 (P_2).

Let us assume that S be an abstract semigroup and ϕ is the homomorphism of S into Cremona semigroup ${}^nCS(K)$. Assume that H stands for the image $\phi(S)$ which is a monoid. Alice and Bob shares elements g, h and h' such that $\phi(h, h')$ is the unity. Alice and Bob selects their private numbers $r(A), k(A)$ and $r(B), k(B)$ respectively. They compute

$$s(A) = h^{r(A)} g^{k(A)} (h')^{r(A)}$$

and

$$s(B) = h^{r(B)} g^{k(B)} (h')^{r(B)}$$

together with their homomorphic images $g(A) = \phi(s(A))$ and $g(B) = \phi(s(B))$. Alice keeps $h(A) = \phi(h^{r(A)})$ and $h'(A) = \phi((h')^{r(A)})$ in a secure way. Bob computes $h(B) = \phi(h^{r(B)})$ and $h'(B) = \phi((h')^{r(B)})$ for him only. Alice and Bob exchange $g(A)$ and $g(B)$. They have two following options

(a) Select pseudorandom tuple v from K^n and elaborate collision vector $c(v)$ via consecutive computations

$$h(A)(v) = {}^1v, g(B)({}^1v) = {}^2v, h'(A)({}^2v) = {}^3v$$

(for Alice),

$$h(B)(v) = {}^1u, g(A)({}^1u) = {}^2u, h'(B)({}^2u) = {}^3u$$

(for Bob). They privately keep $c(v) = {}^2v = {}^3u$ They can select several options for v and keeps several collision vectors i^c, $i = 1, 2, \ldots, k$. We refer to this scheme as ${}^aP_2$.

(b) Alice computes the standard form of the composition $C(A)$ of $h(A), g(B)$ and $h'(A)$. Bob computes the $C(B) = h(B)g(A)h'(B)$ in its standard form. So correspondents can use the sequence of coefficients of multivariate map $C = C(A) = C(B)$ ordered lexicographically.

We consider also the following Cryptosystems of El Gamal type which are modifications of schemes of [54].

2.3 Cryptosystem E.

Assume that S is abstract semigroup, ϕ is a homorphism of S into ${}^nCS(K)$ and its image H is the monoid. Suppose that Alice and Bob shares g, h amd h' sach that $\phi(h')$ is the inverse of $\phi(h)$ and $\phi(g)$ is an invertible endomorphism. Alice knows element g' such that $\phi(gg')$ is unity. Alice selects her numbers $r(A)$ and $k(A)$. She computes $h(A) = \phi(h^r(A))$ and $h'(A) = \phi((h')^{r(A)})$ for herself and $g(A)$ as

$$\phi(h^{r(A)})(g')^{k(A)}(h')^{r(A)}.$$

She sends $g(A)$ to Bob. He acts as in the case of protocol P_2 selecting $r(B)$ and $k(B)$ an computing $g(B)$ as

$$\phi(h^{r(B)})g^{k(B)}(h')^{k(B)}.$$

Bob computes $h(B) = \phi(h^{r(B)})$ and $h'(B) = \phi((h')^{r(B)})$ as well. After the exchange of $g(A)$ and $g(B)$ correspondents have two options.

(a) They can communicate via the following scheme. Alice writes her message p. She computes ${}^1p$ as $h(A)(p)$, ${}^2p$ as $g(B)^{k(A)}({}^1p)$ (via consecutive application of $g(B)$ to vector) and ${}^3p$ as $h'(B)({}^2p)$. Alice sends the ciphertext ${}^3p$ to Bob.

He computes ${}^1c$ as $h(B)({}^3p)$. ${}^2c$ as $g(A)^{k(B)}({}^1c)$ (via the consecutive application of $g(A)$ to vector) and ${}^3c = h'(B)$ to ${}^2c$. We can see that ${}^3c$ coincides with the plaintext p of Alice.

Similarly Bob writes his message p. He computes ${}^1p$ as $h(B)(p)$, ${}^2p$ as $g(A)^{k(B)}({}^1p)$ (via consecutive application of $g(A)$ to vector) and ${}^3p$ as $h'(B)({}^2p)$. Bob sends the ciphertext ${}^3p$ to Alice. She computes ${}^1c$ as $h(A)({}^3p)$, ${}^2c$ as $g(B)^{k(A)}({}^1c)$ (via the consecutive application of $g(B)$ to vector) and ${}^3c = h'(A)$ to ${}^2c$. We can see that ${}^3c$ coincides with the plaintext p of Bob.

Remark 1. Security of Protocol P_2 and Cryptosystem E are based on the complexity of Conjugacy Power Problem for elements $\phi(h)$ and $\phi(g)$ of $\phi(S)$.

We assume that the computations in S are essentially faster then in $\phi(S)$.

Remark 2. (desynchronised mode). Alice and Bob shares distinct elements ${}^1L$ and ${}^2L$ from the general affine group $AGL_n(K)$. They can use ${}^1L\phi(h){}^1L^{-1}$ and ${}^2L\phi(g){}^2L^{-1}$ instead of generators $\phi(h)$ and $\phi(g)$ in the semigroup ${}^nCS(K)$.

Remark 3. (hidden semigroup S). Alice use her knowledge on S and ϕ but she sends to Bob elements ${}^1L\phi(h){}^1L^{-1}$ and ${}^2L\phi(g){}^2L^{-1}$ in their standard form to Bob. So he use the Twisted Diffie Hellman protocol and its inverse version with these generators in their standard forms.

3 Walks on infinite graphs. and cubic transformations of affine spaces.

Note that quadratic equations (1) of infinite graph $D(K)$ gives the description of neighbourhood of each vertex via the infinite system linear system written in its row echelon form. If we take the point $(c) = (c_1, c_2, \dots)$ then its neighbourhood is described by the equations (1) with variables p_i and l_i is specialised as $p_i = c_i$. So the choice of $l_1 = a$, $a \in K$ defines the neighbour $N_a((c))$. We refer to the first coordinate c_1 of point (c) (or line $[c] = [c_1, c_2, \dots]$ as the colour of the point (line respectively).

So we have well defined operator $N_a(v)$ of taking thr neighbour of v Let $I = I(K)$ stands for the incidence relation of the bipartite graph $D(K)$. If we take fixed point (u) of colour b and the sequence $s = (a_1, b_1, a_2, b_2, \dots, a_k, b_k)$ of elements K then it defines the walk of the graph of kind

$$uIv_1Iu_1Iv_2Iu_2I \dots v_kIu_k$$

where v_i stands for the point of colour b_i and u_i is the line of colour a_i.

The standard homomorphism $\eta = \eta_n$ of $D(K)$ onto $D(n, K)$ defined via deleting coordinates with indexes $> n$ allows us to take the sequence

$$\eta(u), \eta(v_1), \eta(u_1), \eta(v_2), \eta(u_2), \dots, \eta(v_k), \eta(u_k).$$

Graph $D(K)$ is defined over arbitrary commutative ring K. So we can consider the graph $\widetilde{D(K)} = D(K[x_1, x_2, \dots x_n, \dots])$ where $x_i, i = 1, 2, \dots$ form an infinite set of unknowns. If K is an integrity domain, i. e. commutative ring does not contain zero divisors, then both graphs $D(K)$ and $\widetilde{D(K)}$ are forests. Even in the case of finite K the neighbourhood of each vertex of $\widetilde{D(K)}$ is an infinite set.

We consider an induced subgraph D' of $\widetilde{D(K)}$ of vertexes with colours from $K[x_1]$. We take some point of D' of kind

$$(p) = (f(x_1), f_2(x_1, x_2, \dots), f_3(x_1, x_2, \dots), \dots)$$

of colour $f(x_1)$ and sequence w of elements

$$(A_1(x_1), B_1(x_1), A_2(x_1), B_2(x_1), \dots A_k(x_1), B_k(x_1))$$

from $K[x_1]^k$. It defines walk w in D' with starting point p and colours of other vertexes taken from the sequence

$$B_1(f(x_1)), A_1(f(x_1)), B_2(f(x_1)), A_2(f(x_1)), \dots$$

We refer to the sequence w as symbolic word. If we have other symbolic word

$$w' = (A'_1(x_1), B'_1(x_1), A_2(x_1), B'_2(x_1), \dots, A_l(x_1))$$

we can take walk w and extend it from its last point ${}^1p$ of colour $B_k(f(x_1))$ (via consecutive adding neighbours with colours

$$A'_1(B_k(f_1(x_1)), B'_1(B_k(f_1(x_1)), A'_2(B_k(f_1(x_1)), B'_2(B_k(f_1(x_1)), \dots .$$

This construction motivates the definition of composition of symbolic words w and w' as

$$(A_1(x_1), B_1(x_1), A_2(x_1), B_2(x_1) \dots A_k(x_1), B_k(x_1),$$
$$A'_1(B_k(x_1)), B'_1(B_k(x)), A'_2(B_k(x_1)), B'_2(B_k(x_1)), \dots, A'_l(B_k(x_1)), B'_l(B_k(x_1)))$$

This operation will define semigrout $SD(K)$. We can see that this is the semidirect producy of free semigroup of words in the alphabet $K[x_1]$ and Cremona semigroup ${}^1CS(K)$.

We define homomorphism ϕ of $SD(K)$ onto $End(K[x_1, x_2, \dots]$ such $\phi(w)$ for $w = (A_1, B_1, A_2, B_2, \dots, A_k, B_k)$ is endomorphism sending the tuple $(x_1, x_2, x_3, \dots)$ to $(u_1, u_2, u_3, \dots)$ which is the ending point of the walk of length $2k$ starting from $(x) = (x_1, x_2, \dots)$ and containing vertexes with colours $A_1, B_1, A_2, B_2, \dots, A_k, B_k$ of the graph $D'(K)$.

The rule $\eta_n(\phi)$ define the homomorphism ϕ_n of $SD(k)$ onto ${}^nCS(K)$. Endomorphisms $\phi(w)$ and $\phi_n(w)$ are automorphism if and only if B_k is an automorphism of $K[x_1]$. (see [10] and further references).

Assume that $W(K) = \phi(CD(K))$ and $W(n, K) = \phi_n(CD(K)$.

For each symbolic word

$$w = (A_1, B_1, A_2, B_2, \dots A_k, B_k)$$

we define w^* as the tuple

$$({B_k}^{-1}(A_k), {B_k}^{-1}(B_{k-1}), {B_k}^{-1}(A_{k-1}), \dots, {B_k}^{-1}(B_1), {B_k}^{-1}(A_1), {B_k}^{-1}).$$

We can check that $\phi(w \times w^*) = e$ and $\phi_n(w \times w^*) = e$ for $n \geq 2$.

Let us consider the subsemigroup $S(K)$ of $CD(K)$ formed by symbolic words with coordinates of kind $x_1 + c, c \in K$. So $G(K) = \phi(S(K))$ and $G(n, K) = \phi_n(S(K))$ are subroups of $W(K)$ and $W(n, K)$ respectively.

Theorem 1. *[55]. Maximal degree of elements of $G(n, K)$ is 3.*

We can encode the pair of symbolic words of kind

$$w = (x_1 + a_1, x_1 + b_1, \dots, x_1 + a_k, x_1 + b_k),$$
$$w^* = (x_1 - b_k + a_k, x_1 - b_k + b_{k-1}, x_1 - b_k + a_{k-1}, \dots, x_1 - b_k + a_1, x_1 + b_k)$$

as

$$(a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_k)$$

and

$$(-b_k + a_k, -b_k + a_{k-1}, \dots, -b_k + a_1 - b_k + b_{k-1}, -b_k + b_{k-2}, \dots, -b_k + b_1, -b_k).$$

Note that

$$(a_1, a_2, \dots a_k, b_1, b_2, \dots, b_k) \times (a'_1, , a'_2, \dots, a'_l, b'_1, b'_2, \dots b'_l) =$$
$$(a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_k, -b_k + a'_1, b_k + a'_2, \dots,$$
$$- b_k + a'_l, -b_k + b'_1, -b_k + b'_2, \dots, -b_k + b'_l)$$

4 On the complexity of algorithms based on the semigroup $S(K)$ and its homomorphism ϕ_n.

For the implementation of protocol ${}^aP_2$ or cryptosystem E semigroup $S(K)$ and hoomorphism ϕ_n where K is a commutative ring with unity we have to assume that parameters $k(A)$ and $k(B)$ are essentially large than the characteristic of the ring. In case of large characteristic the symbolic word $g = (a_1, a_2, a_k, b_1, b_2, \dots, b_k)$ has to be selected with $b_k = 0$.

We implement also versions of these algorithm ${}^aP'_2$ and E' with hidden homomorphism ϕ_n where Alice uses idea of Remark 1.

Remark 4. So she selects transformation of kind $T = Lu$ where $L \in AGL_n(K)$, $u \in W(n, K)$. So, she selects generators g and h from $S(K)$ and sends generators $\tilde{g} = L\phi_n(g)L^{-1}$, $\tilde{h} = T\phi_n(h)T^{-1}$ in the case of u taken outside of $G(n, K)$ we use L of density $O(1)$.

Let us start with elements of cryptanalysis in the case of implementation of protocol ${}^qP_2$ and cryptosystem E in the case when adversary knows the graph $D(n, K)$.

We select the case $K = F_q$ where q is even prime number for the implementation. In this case graphs $D(F_q)$ is an infinite regular forest and the graph $D(F_q[x_1, x_2, \ldots, x_n])$ is an infinite forest of infinite degree. Adversary is able to do the computation in the open semigroup $S(F_q)$.

Recall that two elements $a = (a_1, a_2, \ldots, a_k)$, $b = (b_1, b_2, \ldots, b_l)$ of even length of size $O(1)$ of this semigroup of random or pseudorandom nature are publicaly known as well as positive integer n. So adversary computes elements $h = \phi_n(a)$ and $g = \phi_n(b)$ in their standard forms. He/she has to solve the Conjugacy Power Problem with these generators and righthandside $g(A)$ (or $g(B)$) of $G(n, q)$ which is NP hard for the case of computations in ${}^nCS(F_q)$. Notice that degrees of $g(A)$ and $g(B)$ coinside with 3.

Computer experiment (see below) justifies that the densities of $g(A)$ and $g(B)$ are of size $O(n)$ and for sufficiently large $2r(A) + k(A)$ ($2r(B) + k(B)$ respectively) the densities of these map are constant.

So the adversary can not use degrees and densities for evaluation of private keys size.

Alternatively adversary can use the pseudorandom message v (in the case of algorithm E the tuple $v = p$ is the plaintext) and try to look at walks between v and $g(A)(v)$ (or $g(B)$) to get some info on possible size of $r(A)$ and $k(A)$ (or $r(B)$ and $k(B)$).

This option turns out to be computationally difficult because the complexity of finding the shortest path in the graph of order m is $m\log(m)$ (Dijkstra algorithm or other options). In our case $m = 2q^n$ and complexity is exponential. Thus the option is unfeasible. In fact for Cayley expanding graphs some faster algorithms are known but graph $D(n, q)$ is not a Cayley graph.

Let us consider the complexity of ${}^aP_2$ for Alice and Bob. Let us assume that even length of a and b are of size $O(1)$ and the parameters $r(A), k(A), r(B)$ and $k(B)$ are size of $O(n^\alpha)$ where $0 \leq \alpha \leq 1$. So the computing of $s(A) = a^{r(A)}b^{k(A)}(a^*)^{r(A)}$, $s(B) = a^{r(B)}b^{k(B)}(a^*)^{r(B)}$ and other symbolic words of $S(F_q)$ of length $O(n^\alpha)$ requires $O(n^\alpha)$ elementar operations. These calculations have no impact on general complexity of algorithm. The computer experiment indicates that densities of $\phi_n(w)$ for symbolic word w of length $O(n)$ is $O(n)$. So the computation of standard form of the bijective map $\phi_n(w)$ costs $O(n^2)$ elementary operations. The output of the algorithm X for each user is a combination of $O(1)$ already computed elements of $G(n, q)$ of density $O(n)$. Thus total time of computation of the tuple $X(v)$ is $O(n^2)$.

Below please find the output of our computer simulations for the density evaluation of elements $\phi_n(w)$ of symbolic word of length $l, l \leq n$ and execution evaluation.

Table 1. Total number of monomial terms of the $\phi_n(w)$

n	length l			
	32	**64**	**124**	**248**
16	112	47	145	112
32	456	288	545	462
64	1815	1456	2113	1882
128	5399	6479	8321	7602
256	12567	20047	32988	30286

Table 2. Generation time for the map (ms)

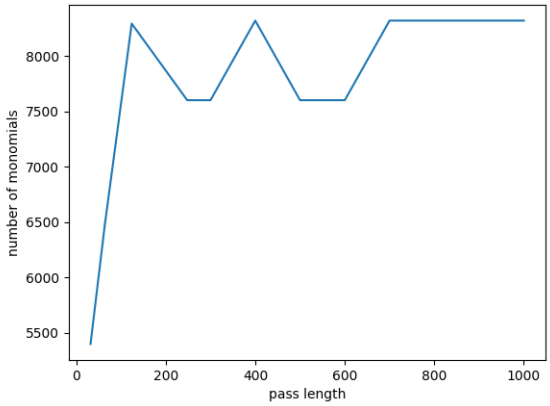
n	length l			
	32	**64**	**124**	**248**
16	12,71	20,41	39,85	70
32	35,6	62,8	132,4	252,9
64	97	234,5	567,2	1211
128	260,9	1121,9	3692,7	7300,8
256	640,2	3268,6	12556,5	34079,7

5 Conclusion.

The paper [7] published 30 year ago presents the iInfinite q-regular tree as well defined projective limit $D(q)$ of incidence structures $D(n, q)$, $n = 2, 3, \ldots$ with the sets of points and lines isomorphic to $(F_q)^n$ and the incidence relation given in a form of quadratic equations in terms of coordinates of elements. The projective limit of connected components $CD(n, q)$ is the q-regular tree.

We shortly observe application of these results to Extremal Graph Theory, Theory of Algebraic Graphs, Expanding graphs, Theory of LDPC codes and Cryptography. Recent paper [8] presents results on spectra of $CD(n, q)$. We present some new applications of these graphs to Noncommutative Cryptography dedicated to construction of Post Quantum analoque of Diffie-Helman key exchange protocol in terms of albebraic objects with noncommutative binary operations. We use the semigroup $S(F_q)$ of walks of even length on $D(q)$ and its homomorphism onto noncommutative group $G(n, q)$ of cubic transformation of the vector space F_q which is one of partition sets of $D(n, q)$.

Fig. 3. Number of monomial terms of the cubic map induced by the graph, $n = 128, F_{2^{24}}$



We suggest the package of protocols and algorithms of El Gamal type for which the security rests on the Complexity of Conjugacy Power Problem for affine Cremona group of automorphisms of $F_q[x_1, x_2, \ldots, x_n]$. The output of protocols are given in the form of vector from $(F_q)^n$ or cubic transformation of this vector space of prescribed density ($O(n)$ or $O(n^2)$).

These form of output allows users to consider the algorithm as key establishment procedure. Output vectors can be used as passwords for entering Information System or passwords of symmetric cipher.

For these algorithms the complexity of execution for each user is given. In the fastest case it is $O(n^2)$ (case of open graph for which we present results of computer simulations), in the worthiest case of hidden graph The complexity is estimated as $O(n^9)$.

Both cases compare well with the complexity $O(n^{13})$ of the protocols based on Navigation Problem with the same platform of group conjugated with $G(n, q)$ via linear transformation (see [56] and further references). Protocols presented in the paper are defined in more general case of graphs $D(n, K)$ where K is arbitrary finite commutative ring. There is a possibility to change the graph $D(n, K)$ for other graphs over K defined in [8] via quadratic equations. Such a change preserves the complexity estimates. We did not observe the research on the applications of graphs $D(n, K)$ to construction of public keys. Recent results in this direction can be found in [57].

References

1. F. Buekenhout (Editor), Handbook on Incidence Geometry, North Holland,Amsterdam, 1995.

2. V. A. Ustimenko, On some properties of Chevalley groups and their generalisations, In: Investigations in Algebraic Theory of Combinatorial ob-jects, Moskow, Institute of System Studies, 1985, 134 - 138 (in Russian), Engl.trans.: Kluwer, Dordrecht, 1992, pp. 112-119.
3. V. Ustimenko, Affine system of roots and Tits geometries, Voprosy teorii grupp i gomologicheskoy algebry, Yaroslavl, 1989, pp.155-157.
4. V. Ustimenko. On the embeddings of some geometries and flag systems in Lie algebras and superalgebras, in Root systems, representations and geometries, Kiev, IM AN UkrSSR, pp. 3–16, 1990.
5. F. Lazebnik, V. Ustimenko, Explicit construction of graphs with arbitrary large girth and of large size, Discrete Applied Mathematics 60 (1995), 275-284.
6. F. Lazebnik, V. Ustimenko, A. Woldar, A characterization of the components of the graphs $D(k, q)$. Discrete Mathematics Volume 157, Issues 1-3, 1 October 1996, Pages 271-283.
7. 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.
8. Chojecki, T., Erskine, G., Tuite, J. Ustimenko V. On affine forestry over integral domains and families of deep Jordan-Gauss graphs. European Journal of Mathematics 11, 10 (2025). https://doi.org/10.1007/s40879-024-00798-2. ‘
9. T. Shaska, V. Ustimenko, On the homogeneous algebraic graphs of large girth and their applications. Linear Algebra and its Applications Volume 430, Issue 7, 1 April 2009, Pages 1826-1837
10. V. Ustimenko, Graphs in terms of algebraic geometry, symbolic computations and secure communications in post-quantum world, UMCS Editorial House, Lublin, 2022, 198.
11. Guinand P., Lodge J., Tanner type codes arising from large girth graphs, Canadian Workshop onInformation Theory CWIT ’97, Toronto, Ontario, Canada, June 3-6 (1997): 5 (PDF) LDPC codes based on algebraic graphs. Available from: https://www.researchgate.net/publication/265833663_LDPC_codes_based_on_algebraic_graphs [accessed Sep 08 2025].
12. Guinand P., Lodge J., Graph theoretic construction of generalized product codes, IEEE Interna-tional Symposium on Information Theory ISIT’97 Ulm, Germany June 29-July 4 (1997): 111 (PDF) LDPC codes based on algebraic graphs. Available from: https://www.researchgate.net/publication/265833663_LDPC_codes_based_on_algebraic_graphs[accessed Sep 08 2025].
13. D. MacKay and M. Postol, Weakness of Margulis and Ramanujan Margulis Low Density Parity Check Codes, Electronic Notes in Theoretical Computer Science, 74 (2003), 8pp.
14. Ustimenko, V.A. On linguistic dynamical systems, families of graphs of large girth, and cryptography. J Math Sci 140, 461-471 (2007). https://doi.org/10.1007/s10958-007-0453-2
15. Polak M, Zhupa E., Keyed hash function from large girth expander graphs, Albanian J. Math., 2022, V. 16, No 1 25 - 39.
16. A. Paszkiewicz, Z. Kotulski, K. Kulesza, J. Szczepanski, Proposals of graph based ciphers theory and implementations. Research Gate, 2001.
17. Costache, A., Feigon, B., Lauter, K., Massierer, M., Puskas, A. , Ramanujan Graphs in Cryptography. In: Balakrishnan, J., Folsom, A., Lalin, M., Manes, M. (eds), Research Directions in Number Theory. Association for Women in Mathematics Series, vol 19. Springer,

18. P.L. K. Priyadarsini, A Survey on some Applications of Graph Theory in Cryptography, Journal of Discrete Mathematical Sciences and Cryptography, https://www.tandfonline.com/doi/abs/10.1080/09720529.2013.878819.
19. W. M. Al Etaiwi, Encryption Algorithm Using Graph Theory, Journal of Scientific Research & Reports, 3(19): 2519-2527, 2014; Article no.JSRR.2014.19.004
20. Denis X. Charles, Eyal Z. Goren, Kristin E. Lauter., Cryptographic hash functions from expander graphs. Journal of Cryptology, 2009, V. 22, 93 - 113.
21. Tomkins H, M. Nevins M, Salmasian H. New Zemor-Tillich type hash functions over GL2(F). J. Math. Cryptol.,2020, V. 32, No.1. 236 - 253.
22. Van Oorschot, P.C. (2020). Authentication Protocols and Key Establishment. In: Computer Security and the Internet. Information Security and Cryptography.Springer, Cham. https://doi.org/10.1007/978-3-030-33649-3_4
23. Abdalla, M. (2014). Password-Based Authenticated Key Exchange: An Overview. In: Chow, S.S.M., Liu, J.K., Hui, L.C.K., Yiu, S.M. (eds) Provable Security. ProvSec 2014. Lecture Notes in Computer Science, vol 8782. Springer, Cham. https://doi.org/10.1007/978-3-319-12475-9_1
24. Tim Taubert, Christopher A. Wood: SPAKE2+, an Augmented Password- Authenticated Key Exchange (PAKE) Protocol. RFC 9383: 1-25 (2023)
25. Jiaxin Pan Runzhi Zeng, A Generic Construction of Tightly Secure Password-based Authenticated Key Exchange, IACR e-print archive 2023/1334.
26. Malik, A., Kushwah, R. A Secure Authentication and Key Establishment Protocol for IoT Devices Using ECCMD. SN COMPUT. SCI. 6, 803 (2025). https://doi.org/10.1007/s42979-025-04354-x
27. Kumar, K., Ahlawat, P. (2024). A Survey on Path Key Establishment. In: Roy, N.R., Tanwar, S., Batra, U. (eds) Cyber Security and Digital Forensics. REDCYSEC 2023. Lecture Notes in Networks and Systems, vol 896. Springer, Singapore. https://doi.org/10.1007/978-981-99-9811-1_5
28. J.A. Lopez Ramos, J. Rosenthal, D. Schipani and R. Schnyder, Group key management based on semigroup actions, Journal of Algebra and its applications, 2017, vol.16 (08):1750148.
29. Alexei G. Myasnikov; Vladimir Shpilrain and Alexander Ushakov (2011), Noncommutative Cryptography and Complexity of Group-theoretic Problems, American Mathematical Society.
30. 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
31. Habeeb, M.; Kahrobaei, D.; Koupparis, C.; Shpilrain, V. (2013). "Public Key Exchange Using Semidirect Product of (Semi)Groups". Applied Cryptography and Network Security. ACNS 2013. Lecture Notes in Computer Science. Vol. 7954. Springer. pp. 475-486.
32. D. N. Moldovyan and 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.
33. L. Sakalauskas, P. Tvarijonas and A. Raulynaitis, Key Agreement Protocol (KAP) Using Conjugacy and Discrete Logarithm Problem in Group Representation Level, INFORMATICA, 2007, vol. 18, No 1, 115-124.
34. V. Shpilrain, A. Ushakov, The conjugacy 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.

35. Delaram Kahrobaei and 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.
36. Alexei Myasnikov; Vladimir Shpilrain and Alexander Ushakov (2008), Group-based Cryptography, Berlin: Birkhduser Verlag.
37. Zhenfu Cao (2012), New Directions of Modern Cryptography. Boca Raton: CRC Press, Taylor & Francis Group. ISBN 978-1-4665-0140-9.
38. Benjamin Fine, et. al. Aspects of Non abelian Group Based Cryptography: A Survey and Open Problems, arXiv:1103.4093.
39. Anshel, M. Anshel and D. Goldfeld, An algebraic method for public-key cryptography, Math. Res.Lett. 6(3-4), 287-291 (1999). 169 -173/
40. S.R. Blackburn and S.D. Galbraith, 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).
41. K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J.S. Kang and C. Park, New publickey 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)
42. G. Maze, C. Monico and J. Rosenthal, Public key cryptography based on semigroup actions, Adv.Math. Commun. 1(4), 489-507 (2007).
43. P.H. Kropholler and 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.
44. V. A. Roman'kov, A nonlinear decomposition attack, Groups Complex. Cryptol. 8, No. 2 (2016), 197-207.27.
45. V. Roman'kov, An improved version of the AAG cryptographic protocol, Groups, Complex., Cryptol, 11, No. 1 (2019), 35-42.
46. 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).
47. B. Tsaban, Polynomial-time solutions of computational problems in noncommutative-algebraic cryptography, J. Cryptol. , No. 3 (2015), 601-622.
48. V. Roman'kov, Cryptanalysis of a new version of the MOR scheme, arXiv:1911.00895 [cs.CR].
49. V. Roman'kov, Cryptanalysis of two schemes of Baba et al. by linear algebra methods. CoRR abs/1910.09480 (2019).
50. Adi Ben-Zvi, Arkadius G. Kalka, Boaz Tsaban, Cryptanalysis via Algebraic Spans. CRYPTO (1) 2018: 255-274
51. M. Noether, Luigi Cremona, Mathematische Annalen, 59 (1904), pp. 1-19.
52. I.R. Shafarevich, On some infinite dimension groups II, Izv. Akad. Sci. Ser. Math. 2 (1) (1981), 214-226.
53. Yu. Bodnarchuk, Every regular automorphism of the affine Cremona group is inner, Journal of Pure and Applied Algebra 157 (2001) 115-119.
54. V. Ustimenko, On new symbolic key exchange protocols and cryptosystems based on hidden tame homomorphism, Reports of Nath Acad of Sci, Ukraine, 2018 V. Ustimenko, N. 10, 2018, pp. 26 -36.
55. A.Wroblewska, On some properties of graph based public keys, Albanian Journal of Mathematics, Volume 2, Number 3, 2008, 229-234, Proceedings of NATO Advanced Studies Institute: "New challenges in digital communications".

56. Ustimenko, V., Klisowski, M.: On new protocols of noncommutative cryptography in terms of homomorphism of stable multivariate transformation groups. J. Algebra Discrete Math. 220-250, (2023), http://dx.doi.org/10.12958/adm1523.
57. V. Ustimenko, On Schubert cells of Lie geometries and public keys of multivariate cryptography, Contemporary Mathematics, AMS, Volume 830, 2025, https://doi.org/10.1090/conm/830/16568