Expanding Extremal Graphs and Implemented Solutions of Post Quantum Cryptography

Vasyl Ustimenko[1,2] and Oleksandr Pustovit[2]

[1]*University of Royal Holloway in London, Egham Hill, Egham TW20 0EX, United Kingdom*
[2]*Institute of Telecommunications and the Global Information Space of the National Academy of Sciences of Ukraine, 13 Chokolivsky ave., Kyiv, 02000, Ukraine*

Abstract

Extremal properties of graphs *CD(n, q)* and *A(n, q*) can be efficiently used for the construction of LDPC codes and stream ciphers. Recently pseudorandom walks on these graphs were used for the constructions of key agreement protocols of postquantum cryptography. We use these graphs to introduce a new algorithm for the generation of unperiodical infinite string of field characters. Its input is selected as a finite "seed" of elements of a corresponding finite field. This algorithm has postquantum stability i.e., the adversary has to deal with the intractable problem of postquantum cryptography to get the seed. We combine this algorithm with the postquantum secure protocol of noncommutative cryptography for the elaboration of collision seed. This combination can be used for one-time pad delivery of pseudorandom or random sequence from one person involved in protocol to another one and constructions of new MACs. We introduce the generalization of these algorithms for the case of a general finite commutative ring.

Keywords

Extremal Graph Theory, Post Quantum Cryptography, Computer Algebra, stable subgroups of affine Cremona group, key exchange protocols, random and pseudorandom sequences.

1. Introduction

In March 2021 it was announced that the prestigious Abel Prize will be shared by A. Wigderson and L. Lovasz. They contribute valuable applications of the theory of Extremal graphs [1, 2] and Expanding graphs [3] to Theoretical Computer Science. We have been working on applications of these graphs to Cryptography ([4, 5] and further references).

The one-time pad is a practical implementation of the idea of absolutely secure encryption. A symbiotic combination of this encryption tool with key exchange Diffie–Hellman protocol was widely used. The appearance of the first versions of quantum computers and cryptanalysis of algorithms based on discrete logarithm problems demands a new algorithm of "post-quantum secure" generation of pseudorandom string *S* of characters of the chosen alphabet. Quantum technologies allow the production of genuine random string G of a chosen length. One-time pad encryption of *G* with the key *S* will allow the safe delivery of string *G* from the correspondent to his/her partner [6–8].

In this paper, we use a 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 the introduction algorithm of postquantum secure generation of S in the case of alphabet *K*.

Our algebraic graphs-based technique differs from classical number-theoretical methods, you can compare our algorithms with those presented in [9–39].

These new algorithms are described in Section 3 in terms of graphs *A(n, K)* with references to their known properties and properties of polynomial transformation groups *GA(n, K)* of affine space K^n related to *A(n, K)*. The most important is the following "stability property" of *GA(n, K)*.

CPITS 2023: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2023, Kyiv, Ukraine
EMAIL: vasulustimenko@yahoo.pl (V. Ustimenko); sanyk_set@ukr.net (O. Pustovit)
ORCID: 0000-0002-2138-2357 (V. Ustimenko); 0000-0002-3232-1787 (O. Pustovit)

In the chosen basis maximal degree of elements of $GA(n, K)$ has degree *3*. Notice that the 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 $A(n, K)$ can be justified via an enveloping family of graphs $D(n, K)$ and their connected components $CD(n, K)$ (see Section 3 of the paper and further references). Known facts and conjectures about these graphs are presented there, and references on the usage of graphs in symmetric cryptography and the theory of LDPC codes are given.

Section 3 also describes applications of the main algorithm to the construction of new postquantum secure Message Authentication Codes (MACs). These constructions are the generalization of MACs presented in [40], it gives new options to increase the level of avalanche effect.

In Section 3 also a symbiotic combination of the main algorithm of generation of *a* potentially infinite string of characters with the postquantum secure Key Agreement Protocol based on computations in the group $GA(n, K)$ is described.

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

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

Application 3 from Section 3 gives an alternative to the one-time pad encryption symmetric encryption algorithm. Its password can be extracted from the output of the algorithm of generation of a potentially infinite string of characters from K. The complexity of this stream cipher is $O(n)$.

The encryption map of this algorithm is a polynomial map of unbounded degrees. It can be used similarly to a public key without the change of password for unlimited time. Implemented a simpler version of this algorithm with the encryption map of degree 3 can be used safely $O(n^2)$ times. Section 4 is dedicated to the idea of changing graphs $A(n, K)$ on well-known graphs $D(n, K)$. The results of the computer simulation are presented at the end of Section 4. Given densities of cubical maps allow us to evaluate the "usage interval" of encryption with a taken password.

Correspondents can change passwords via an algorithm of generation of potentially infinite strings of characters. No need to repeat the $GA(m, K)$ protocol which costs $O(m^{13})$ elementary operation. Execution time for the generation of the element of $GA(n, K)$ is useful for the time evaluation of the main algorithm of Section 3. Conclusions from Section 5.

2. On Current State of Post Quantum Cryptography

Prototype models of probabilistic machines known as Quantum computers already exist. They can produce genuine random sequences of bits that can be used in information security instead of pseudo-random strings.

The perfect symbiosis of one-time encryption with Diffie–Hellman protocol for the key exchange can't be used safely anymore because the Discrete logarithm problem can be efficiently solved with the usage of a Turing machine together with a Quantum Computer. A combination of these two machines can be used for effective cryptanalysis of RSA (the result of Peter Shor, 1995).

Investigation of public keys with potential resistance to quantum attacks has been supported by U.S. NIST international project supporting Post Quantum standardization process since 2017. In July 2020 the third round started for the final further investigation of already selected algorithms. In the area of Multivariate Cryptography, only rainbow-like oil and vinegar digital signatures are selected for further investigation. They can't be used as encryption algorithms.

During Third Round, some cryptanalytic instruments to deal with ROUV were found [41]. That is why different algorithms were chosen at the final stage. In July 2022 first four winners of the NIST standardization competition were chosen. They all are lattice-based algorithms.

This fact motivates different from public key directions of Multivariate Cryptography such as the search for Postquantum Secure Key Agreement Protocols able to substitute symbiotic combinations of Diffie–Hellman protocol and one-time pad.

3. Equations of Q-Regular Tree and String Processing

The description of the q-regular tree T_q in terms of equations was introduced in [42] where graphs $CD(n, q)$ were introduced. 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 in the sense of [1]. Well-defined projective limit $A(n, q)$, $n = 2, 3, \ldots$ coincides with T_q. [4].

This construction allows introducing T_q as a q-regular bipartite graph with points of kind

$$(p) = (p_1, p_2, \ldots, p_1, \ldots)$$

and lines

$$[l] = [l_1, l_2, \ldots, l_i, \ldots],$$

where only a 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

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

Brackets and parenthesis allow us to distinguish points from lines.

Projections of (p) and $[l]$ onto $(p_1, p_2, \ldots, p_n)$ and $[l_1, l_2, \ldots, l_n]$ define graph homomorphism on graph $A(n, q)$ with point set and line set isomorphic to $(F_q)^n$ and the incidence is given by first $n\text{-}1$ 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 the integrity ring then $T_K = A(K)$ is also an infinite tree but the existence of zero divisors leads to the appearance of cycles in these graphs.

The first coordinates $\dot{\rho}(p) = p_1$ and $\dot{\rho}([l]) = l_1$ are the natural colors 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 neighbor u of chosen color $\dot{\rho}(u) = a$. Let $N_a(v)$ be the operator of taking the neighbor of v with color a.

The walk in the graph $A(n, K)$, $n = 2, 3, \ldots$ of length m started at the given point $p = (p_1, p_1, \ldots)$ can be given by sequence $a(1), a(2), \ldots, a(m)$, this is a sequence

$$(p), v_1 = N_{a(1)}(p), v_2 = N_{a(2)}(v_1), \ldots, v_m = N_{a(m)}(v_{m-1}).$$

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

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

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

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

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

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

$${}^nC(w) = (f_1, f_2, \ldots f_n),$$

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

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

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

$$(a_1, a_2, \ldots a_{2s}, a_{2s} + u_1, a_{2s} + u_2, \ldots, a_{2s} + u_{2t}).$$

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 a modification of a free product $(K, +)$ with itself.

It is easy to check that the composition ${}^nC(w)$ ${}^nC(u)$ coincides with ${}^nC(w \circ u)$. So transformations ${}^nC(w), w \in \sum(K)$ form a subgroup $GA(n, q)$ of group $Aut\ K[x_1, x_2, \ldots, x_n]$ which acts on the affine space $(K)^n$ as group $CG((K)^n)$ (affine Cremona group) 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 $K[y_1, y_2, ..., y_m]$ and consider the special direction $(y) = (y_1, y_2, ..., y_m)$ of graph $A_n(K[y_1, y_2, ..., y_m])$ where m is even number.

Elements of this group are $\acute{\eta}_n(C(y))$ where $\acute{\eta}_n$ is a homomorphism of $\sum(K[y_1, y_2, ..., y_m])$ onto $C((K[y_1, y_2, ..., y_m])^n)$. Each of them can be written as a rule $x_i \rightarrow f_i(x_1, x_2, ..., x_n, y_1, y_2, ..., y_m)$, $i = 1, 2, ..., n$. The degree of each polynomial in variables $x_1, x_2, ..., x_n$ (deg_x) is bounded by 3. It possible to prove that degree of f_i in variables $y_1, y_2, ..., y_m$ $(deg_y(f_i))$ is i.

***A(K)* based string generation algorithm**:

Choose even parameters m and increasing sequence of even numbers $n(1), n(2), n(k)$, where $n(1) \le m$, $n(1) < n(2) < C^3_{n(1)}$, $n(2) < n(3) < C^3_{n(2)}$, ..., $n(2) < n(k) < C^3_{n(k-1)}$.

Consider the word $(y) = (y_1, y_2, ..., y_m)$ and a string of characters $b_1, b_2, ..., b_n$ from K^*. Form affine transformation T of K^n to K^n given by the rule

$$x_1 \rightarrow b_1x_1+b_2x_2+... b_nx_n, x_i \rightarrow x_i, i = 1, 2, ..., n.$$

Step 1. Compute $F(1) = T\acute{\eta}_n(y)T^{-1}$ for $n = n(1)$ given by tuple $({}^yf_1, {}^yf_2, ... {}^yf_n)$ $f_n = f(y)$. Take polynomial $f(y) = b_1{}^yf_1+b_2{}^yf_2+ ...+b_n{}^yf_n$ and list $(z_1, z_2, ..., z_t)$, $t = C^3_n$ of its coefficients in front of monomial terms $x_ix_jx_k$ where i,j,k are different elements of $\{1, 2, ...n\}$. Let

$$^3v(f(y)) = (z_1, z_2, ..., z_t) = y(1).$$

Take operator $D_n = d/dx_1+ d/dx_2+...+d/dx_n$. Let us list $r = C^2_n$ coefficients of $D(f(y))$ in front of x_ix_j, $i \neq j$ and get $^2v(f(y)) = (u_1, u_2, ..., u_1)$. Finally list coefficients of $D^2(f(y))$ in front of x_i and get $^1v(f(y)) = (q_1, q_2, ..., q_n)$.

Step 2. Notice that $y(1) = {}^3v(f(y))$ is an element $(y'_1, y'_2, ..., y'_{m(1)})$ of $\sum(K[y_1, y_2, ..., y_m])$. Select $n(2)$. Consider the list of variables $x_1, x_2, ... x_{n(2)}$ under the assumption that the indexes correspond to first $n(2)$ triples of kind $\{k, r, s\}$ accordingly to a lexicographical order. Let c be this correspondence. We set $^1b_i = b_rb_sb_k$ *if* $c(i) = \{r, s, k\}$ and form linear transformation $T(1)$ of kind $x_1 \rightarrow {}^1b_1x_1+{}^1b_2x_2+...{}^1b_nx_{n(2)}$, $x_i \rightarrow x_i$, $i = 2, 3, ..., n(2)$.

Compute $F(2) = T(1)\acute{\eta}_{n(2)}({}^3v(f(y(1)))T(1)^{-1}$, $n < n(2) \le C^3_n$ given via the tuple $({}^{y(1)}f_1, {}^{y(1)}f_2, \ldots, {}^{y(1)}f_{n(2)})$.

Let $f(y(1)) = {}^{y(1)}f_{n(2)}$ and $^3v(f(y(1)) = ({}^2z_1, {}^2z_2, ...{}^2z_{t(1)}) = y(2)$ be the list of coefficients in front of monomial terms $x_ix_jx_k$ where i,j,k are different elements of $\{1, 2, ..., n(2)\}$.

Take operator $D_{n(2)} = d/dx_1+d/dx_2+... d/dx_{n(2)}$. List $r = C^2_{n(2)}$ coefficients of $Df(y(1))$ in front of x_ix_j, $i \neq j$ and get $^2v(f(y(1))) = ({}^2u_1, {}^2u_2, ...{}^2u_{n(2)})$.

Finally list coefficients of $D^2{}_{n(2)}f(y(1))$ in front of x_i and get $^1v(f(y(1)) = ({}^1u_1, {}^1u_2, ...{}^1u_{n(2)})$.

Step 3. Use $n(3)$, $n(2) < n(3) \le C^3_{n(2)}$. Consider the list of variables $x_1, x_2, ... x_{n(3)}$ under the assumption that the indexes correspond to first $n(3)$ triples of kind $\{k, r, s\}$ accordingly to a lexicographical order. Let c be this correspondence. We set

$$^2b_i = {}^1b_r{}^1b_s{}^1b_k \text{ if } c(i) = \{r,s,k\}$$

and form linear transformation $T(2)$ of kind

$$x_1 \rightarrow {}^1b_1x_1+{}^1b_2x_2+...{}^1b_nx_{n(3)}, x_i \rightarrow x_i, i = 2,3, ... ,n(3).$$

Compute $F(3) = T(2)\acute{\eta}_{n(3)}({}^3v(f(y(2)))T(2)^{-1}$, $n < n(2) \le C^3_n$ given via the tuple $({}^{y(1)}f_1, {}^{y(1)}f_2, \ldots, {}^{y(1)}f_{n(2)})$.

Let $f(y(2)) = {}^{y(2)}f_{n(3)}$ and

$$^3v(f(y(2)) = ({}^2z_1, {}^2z_2, ...{}^2z_{t(1)}) = y(3)$$

be the list of coefficients in front of monomial terms $x_ix_jx_k$ where i,j,k are different elements of $\{1, 2, ..., n(3)\}$.

Continue this process till the last potentially infinite Step k. After the end of the computation process we have to take sequence $e(1), e(2), ..., e(k)$ with $e(i) \in \{1, 2, 3\}$ and concatenate $^{e(1)}v(f(y))$, $^{e(2)}v(f(y(1)),...,$ $^{e(k)}v(f(y(k-1))$ to get tuple R_k as an output.

Application 1. Correspondents use chosen Key Agreement Protocol to elaborate two collision strings of kind $b = (b_1, b_2, ..., b_n)$, $b_i \in K-\{0\}$ and $a = (a_1, a_2, ..., a_m)$ such that $a_i \neq a_{i+2}$, $i = 1, 2, ..., m-1$, $a_2 \neq 0$.

They specialize variables y_i as $y_1 = a_1$, $y_2 = a_2, ..., y_m = a_m$, form affine transformation T corresponding to vector b, and execute "numerical implementation" of $A(K)$ based string generation algorithm. The output contains cubical maps $F(1), F(2), ..., F(k)$ depending on $n(i)$ variables.

Alice and Bob agree on $e(1), e(2), ..., e(k)$ in an open way or with the usage of secure agreement protocol. So they can use concatenation $C = (c_1, c_2, ..., c_l)$ of specializations

$$^{e(1)}v(f(y)), {}^{e(2)}v(f(y(1)), ..., {}^{e(k)}v(f(y(k-1))$$

with $y_i = a_i$, $i = 1, 2, ... m$ as cryptographical stable string of polynomial length $l = l(n, k)$.

One of the correspondents can generate a random or quasirandom string produced by a

modern quantum device of characters $P = (p_1, p_2, ..., p_l)$ to send $P+C = (p_1+c_1, p_2+c_2, ..., p_n+c_n)$ to his/her partner. So they can use substrings of C as passwords for one-time pad encryption. In [43] we present the results of computer simulation via the table of number monomial terms in polynomial maps $F(i)$, $i = 1, 2, ..., n$.

Application 2. Correspondents use chosen Key Agreement Protocol to elaborate one collision string of kind $b = (b_1, b_2, ..., b_n)$, $b_1 \in K-\{0\}$. They form affine transformation T corresponding to vector b. They use symbolic implementation of the presented above $A(n, K)$ based string processing algorithm working with variables y_i, $i = 1, 2, ..., m$. The output of this algorithm is ${}^{e(k)}v(f(y(k-1)) = {}^{e(k)}d(y_1, y_2, ..., y_m)$, where $e(k) \in \{1, 2, 3\}$.

They take text $a_1, a_2, ..., a_m$ of large length m, $m>>n(k)$ apply following parity regularization procedure which produce string $a'_1, a'_2, ..., a'_m$ such that $a_1 = a_1'$, $a_2' = a_2$ if $a_2 \neq 0$ and $a'_2 = a_2+1$ in opposite case, $a'_{i+2} = a_{I+2}$ if $a_{i+2} \neq a'_i$ and $a'_{i+2} = a_{i+2}+1$ otherwise for $i = 1, 2, ..., m-2$.

Alice and Bob compute ${}^{e(k)}d(a'_1, a'_2, ..., a'_m) = d_k(a)$, $k = 1, 2, ..., s$ and treat them as a sequence of digests of text a. Each of $d_k(a)$ is a Message Authentication Code (MAC) depending on the key $b = (b_1, b_2, ..., b_n)$. The computer experiment described in [40] demonstrates a high avalanche effect of digest $d_1(a)$. A single change of character a implies the change of 98% of characters of the digest. The experiment shows the increase of avalanche effect for $d_k(a)$, $k>1$ with the growth of parameter i. The following algorithm is developed in the spirit of noncommutative cryptography [44–55].

The protocol [56]. For elaboration of string $b_1, b_2, ..., b_n$ and $a_1, a_2, ..., a_m$ we use the following protocol which also uses 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 z of finite even length from $\sum(K)$. Let $u = (a_1, a_2, ..., a_s)$. We refer to $Rev(u) = (-a_s+a_{s-1}, -a_s+a_{s-2}, ..., -a_s+a_1, -a_s)$ 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 $F_i = T_1\acute{\eta}_n(uw_iRev(u))T_1^{-1}$ and $G_i = T_2\acute{\eta}_n(zw_iRev(z))T_2^{-1}$ for $i = 1, 2, ..., k$. She sends pairs (F_i, G_i), $i = 1, 2, ... k$ 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 G for himself.

Alice has to restore the standard form of G from F. She knows that the 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 $x_i \rightarrow g_i(x_1, x_2, ..., x_m)$, $i = 1, 2, ..., m$.

So correspondents can take vectors b and a of length l and t as appropriate numbers of first coordinates of ${}^3v(g_i)$ and ${}^3v(g_j)$ for chosen distinct i and j (see also [57] for modifications of $GA(n, K)$).

Complexity estimates. The theoretical complexity of the above-presented protocol $O(n^{13})$ coincides with the complexity of computation of the superposition of two polynomial transformations of K^n of degree 3.

The security of protocol rests on the post-quantum hard problem of decomposition of an element from the group of bijective affine transformation of affine space K^n into a word of several generators. The output of this protocol is used as a "seed" of the fast algorithm $(O(m))$ for generating tuples of non-periodic potentially infinite length m. Their pseudo-random properties are currently under investigation. We hope that new MACs will be effectively used for the detection of file integrity.

Application 3. Alice and Bob eject vectors b and a of the length n (potentially infinite number) and r (even constant) from the collision map of the presented protocol or use the presented above method of generation of potentially infinite non-periodic strings. Without loss of generality we assume that $b = (b_1, b_2, ..., b_n) \in (K^*)^n$ and for $(a_1, a_2, ..., a_r)$ the following relations hold $a_2 \neq 0$, $a_i \neq a_{i+2}$, $i = 1, 2, ..., n-2$. Correspondents form transformation

$$T(b): x_1 \rightarrow x_1+b_1x_2+b_2x_1+...+b_{n-1}x_n+b_n,\ x_i \rightarrow x_i,\ i = 1, 2, ... n-1.$$

Let $f_1(x), f_2(x), ..., f_r(x)$ be a string *of* polynomials from $K[x]$ of even length r and linear degree in variable n. We consider a transformation $T[f_1, f_2, ..., f_r]$ of K^n onto K^n obtained via chain of vertices $A(n, K)$ with initial point $(x) = (x_1, x_2, ..., x_n)$

and vertices $[v_1], (v_2), [v_3], ...,(v\_r)$ of colours $f_1(x_1), f_2(x_1) ..., f_r(x,)$. The map $T[f_1, f_2, ..., f_r]$ sends $(x_1, x_2, ..., x_n)$ to...(v_r). It is easy to see that if equation $f_r(x) = a$ has a unique solution for arbitrary a then $T[f_1, f_2, ..., f_r]$ is a bijection.

So Alice and Bob can agree via open channel on sparse (i.e. computable in time $O(1)$) polynomials xg_i of linear degree $a(i)n+b(i), a(i) \neq 0, i = 1, 2, ...r$ and select g_r as αx^t where α is an element of K*. They will use $f_i = xg_i+a_i$ and the map $E = T(b)T[f_1, f_2, ..., f_r]T(b)^{-1}$ as the encryption map. This stream cipher is fast (time execution is $O(n)$), the password $b_1, b_2, ..., b_n, a_1, a_2, ..., a_r$ is protected via postquantum secure protocol. That is why the adversary has the only remaining option to collect a lot of pairs of kind plaintext/ciphertext and try to approximate map E. It is unfeasible because the degree of the polynomial map is unbounded ($\geq \beta n$ for positive constant β).

Practically we can use simple encryption maps of kind $G = T(b)\acute{\eta}((a_1, a_2, ..., a_r)T(b)^{-1}$, i.e. $g_i = i$ for each i and $a(i) = 1$. In this case, *both* degrees of G and G^{-1} coincide with 3. So adversary has a chance to interpret $O(n^3)$ message and in time $O(n^{10})$ approximate these maps via linearisation attacks.

Noteworthy that there is a simple solution to prevent mentioned above attacks. The density $d(G)$ of G of kind $x_1 \rightarrow g_i(x_1, x_2, ..., x_n)$, $i = 1, 2, ..., n$ is a total number of monomial expressions in polynomials g_i.

So correspondents can restrict a maximal number of messages for exchange by average density $a(G) = d(G)/n$.

We find out that $d(G)$ is depending on parameters n, r ann ring K. Results of computer simulations for the cases of finite fields F_q, arithmetical rings Z_q and Boolean rings $B(8)$, $B(16)$, $B(32)$ of cardinality q, where $q \in \{2^8, 2^{16}, 2^{32}\}$. Evaluation of time for generation of transformation G gives a good approximation of the execution time of the encryption process.

4. Connections of A(n, q) with Graphs D(n, q), Other Graph-based Algorithms

The missing definitions of graph-theoretical concepts in the case of simple graphs which appears in this paper can be found in [1]. All graphs we consider are simple ones, i.e. undirected without loops and multiple edges.

When it is convenient, we shall identify Γ with the corresponding anti-reflexive binary relation on $V(\Gamma)$, i.e. $E(\Gamma)$ is a subset of $V(\Gamma)\times V(\Gamma)$. The girth of a graph Γ, denoted by $g = g(\Gamma)$, is the length of the shortest cycle in Γ. The diameter $d = d(\Gamma)$ of the graph Γ is the maximal length of the shortest pass between its two vertices.

Let $g_x = g_x(\Gamma)$ be the length of the minimal cycle through the vertex x from the set $V(\Gamma)$ of vertices in graph Γ. We refer to $Cind(\Gamma) = max\{g_x, x \in V(\Gamma)\}$ as the cycle indicator of the graph Γ.

The family Γ_i of connected k-regular graphs of constant degree is a family of small world graphs if $d(\Gamma_i) \leq clog_k(v_i)$, for some constant $c, c>0$.

Recall that family of regular graphs Γ_i of degree k and increasing order v_i is a family of graphs of large girth if $g(\Gamma_i) \geq clog_k(v_i)$, for some independent constant $c, c>0$.

We refer to the family of regular simple graphs Γ_i of degree k and order v_i as a family of graphs of large cycle indicator, if $Cind(\Gamma_i) \geq clog_k(v_i)$ for some independent constant c, c>0.

Notice that for vertex—transitive graph its girth and cycle indicator coincide. Defined above families plays an important role in Extremal Graph Theory, the Theory of LDPC codes, and Cryptography (see [4] and further references).

Below we consider an alternative definition of a family of graphs $A(n, K)$ and introduce graphs $D(n, K)$ where $n>5$ is a positive integer and K is a commutative ring. In the case of $K = F_q$ we denote $A(n, q)$ and $D(n, q)$, respectively. We define these graphs as homomorphic images of infinite bipartite graphs $A(K)$ and $D(K)$ for which partition sets P and L are formed by two copies of Cartesian power K^N, where K is the commutative ring and N is the set of positive integer numbers. Elements of P will be called points and those of L lines. To distinguish points from lines we use parentheses and brackets. If $x \in V$, then $(x) \in P$ and $[x] \in L$.

The description is based on the connections of these graphs with Kac-Moody Lie algebra with extended diagram A_1.

The vertices of $D(K)$ are infinite-dimensional tuples over K. We write them in the following way $(p) = (p_{0,1}, p_{1,1}, p_{1,2}, p_{21}, p_{22}, p'_{22}, p_{23}, ..., p_{i,i}, p'_{i,i}, p_{i,i+1}, p_{i+1,i}, ...)$,

$[l] = [l_{1,0}, l_{1,1}, l_{1,2}, l_{21}, l_{22}, l'_{22}, l_{23}, ... ,l_{i,i}, l'_{i,i}, l_{i,i+1}, l_{i+1,i}, ...]$. We assume that almost all components of points and lines are zeros. The condition of incidence of point (p) and line $[l]$ ($(p)I[l]$) can be written via the list of equations below.

$l_{i,I}\, p_{i,i} = l_{1,0}\, p_{i-1,i}$; $l'_{i,i}$-$p'_{i,i} = l_{i,i-1}\, p_{0,1}$; $l_{i,i+1}$-$p_{i,i+1} = l_{i,i}\, p_{0,1}$; $l_{i+1,i}$-$p_{i+1,i} = l_{1,0}\, p'_{i,i}$. These four relations are defined for $i \geq 1$, ($p'_{1,1} = p_{1,1}$, $l'_{1,1} = l_{1,1}$).

Similarly, we define graphs *A(K)* on the vertex set consisting of points and lines

$(p) = (p_{0,1}, p_{1,1}, p_{1,2}, p_{21}, p_{22}, p_{23}, \ldots, p_{i,i}, p_{i,i+1}, \ldots)$,

$[l] = [l_{1,0}, l_{1,1}, l_{1,2}, l_{21}, l_{22}, l_{23}, \ldots, l_{i,i}, l_{i,i+1}, \ldots]$

such that point *(p)* is incident with the line *[l]* $((p)I[l])$, if the following relations between their coordinates hold: $l_{i,i}$-$p_{i,i} = l_{1,0}\, p_{i-1,i}$; $l_{i,i+1}$-$p_{i,i+1} = l_{i,i}\, p_{0,1}$.

It is clear that the set of indices $A = \{(1; 0), (0; 1), (1; 1), (1; 2), (2; 2), (2; 3), \ldots, (i-1, i), (i, i), \ldots\}$ is a subset in $D = \{(1, 0), (0; 1), (1, 1), (1, 2), (2; 2), (2, 2)', \ldots, (i\text{-}1, i); (i; i-1); (i, i); (i, i)', \ldots\}$. Points and lines of *D(K)* are functions from $K^{D\text{-}\{(1,0)\}}$ and $K^{D\text{-}\{(0,1)}$ and their restrictions on $A\text{-}\{(1,0)\}$ and $A\text{-}\{(0,1)\}$ define homomorphism Ψ of graph *D(K)* onto *A(K)*.

For each positive integer $m \geq 2$ we consider subsets *A(m)* and *D(m)* containing the first $m+1$ elements of *A* and *D* concerning the above orders.

Restrictions of points and lines of *D(K)* onto $D(m)\text{-}\{(1,0)\}$ and $D(m)\text{-}\{(0,1)\}$ define graph homomorphism ${}^{D}\Delta(m)$ with image denoted as *D(n, K)*. Similarly restrictions of points and lines of *A(K)* onto $A(m)\text{-}\{(1, 0)\}$ and $A(m)\text{-}\{(0, 1)\}$ defines homomorphism ${}^{A}\Delta(m)$ of graph *A(K)* onto graph denoted as *A(m, K)*.

We also consider the map $\Delta(m)$ on vertices of graph *D(m, K)* sending its point $(p) \epsilon K^{D(m)\text{-}\{(1,0)\}}$ to its restriction into $D(m) \cap A\text{-}\{(1, 0)\}$ and its line $[l] \epsilon K^{D(m)\text{-}\{(0,1)\}}$ to its restriction onto $D(m) \cap A\text{-}\{(0, 1)\}$. This map is a homomorphism of *D(m, K)* onto $A(n, k)$, $n = |D(m) \cap A| - 1$.

Graph $D(q) = D(F_q)$ is a q-regular forest. Its quotients *D(n, q)* are edge transitive graphs. So their connected components are isomorphic. Symbol *CD(n, q)* stands for the graph which is isomorphic to one of such connected components.

Family CD(n, q), n = 2, 3, ... is a family of large girth for each parameter q, q>2 (see [42] and further references).

The question "*Whether or not CD(n, q) is a family of small world graphs"* is still open.

Graph A(q), q>2 is a q-regular tree. Graphs A(n, q) are not vertex-transitive.

They form a family of graphs with a large cycle indicator, which is a q-regular family of small-world graphs [58].

The question "*Whether or not A(n, q), n = 2, 3, ... is a family of large girth"* is still open.

Graphs *CD(n, q)* and *A(n, q)* are expanding graphs (see [59], [60], and [3] for basic definitions) with spectral gap $q - 2\sqrt{q}$.

Groups *GD(n, K)* and *GA(n, K)* of cubical transformations of affine space K^n associated with graphs *D(n, K)* and *A(n, K)* are interesting objects of algebraic transformation group theory because of the composition of two maps of degree 3 for the vast majority of pairs will have degree 9. Applications of these groups to Symmetric Cryptography are observed in [5], [43] (see also [61–63]).

The illustration of densities of cubic map constructed with the usage of graphs $A(n, F_q)$ and appropriate linear conjugators are given below detailed description of the simulation process reader can find in [64].

Table 1

The number of monomial terms of the cubic map induced by the graph $A(n, F_q)$, $q=2^{32}$.

	length of the word				
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 2

Generation time for the map (ms) (graph, $A(n, F_q)$, case of usage of sparse linear conjugators)

	length of the word				
n	**16**	**32**	**64**	**128**	**256**
16	20	60	128	260	540
32	308	788	1776	3760	7716
64	3193	8858	23231	53196	113148
128	54031	137201	368460	950849	2164037

Table 3

Number of monomial terms of the cubic map induced by the graph $A(n, F_q)$, case of dense linear conjugators

	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 4
Generation time for the map (ms) case of dense linear conjugators

	length of the word				
n	**16**	**32**	**64**	**128**	**256**
16	76	148	288	576	1148
32	1268	2420	4700	9268	18405
64	22144	40948	78551	153784	304240
128	460200	819498	1532277	2970743	5836938

5. Conclusions

The main result of the paper is a complex cryptographical algorithm based on a highly noncommutative group of polynomial transformations $GA(n, K)$ of K^n, $n = 2, 3, \ldots$ defined over finite commutative ring K with a unity.

In current postquantum reality the idea to change the cyclic group of Diffie–Hellman protocol for a noncommutative group or semigroup with several generators can lead to safe protocols of Algebraic Postquantum Cryptography (APQ).

We suggest using $GA(m, K)$ for the safe elaboration of collision polynomial map G of degree 3 from K^n to K^m. G is written in its standard form of Computer Algebra. We can use $O(m^4)$ of its coefficients for the extraction of some "seed" S of size $s(m)$.

The protocol costs $O(m^{13})$ elementary operations. The security rests on the complexity of the known hard problem of APQ to find the decomposition of G into given generators from the affine Cremona group of polynomial transformations of K^m.

Correspondents can use a family of groups $GA(n, K)$ for simultaneous construction of potentially infinite string R of characters from K^n of length n with the complexity $O(n)$. Recovery of seed S is connected with the hard APQ problem of solving the system of nonlinear equations of unbounded degree.

Parts of R can be used as one-time pad keys, passwords of symmetric stream ciphers, or in key-dependent Message Authentication Codes.

We also presented new APQ stable MACs and stream cipher to work with the text of length t in time $O(t)$ defined in terms of graphs from the family $A(n, K)$.

6. Acknowledgments

This research is partially supported by British Academy Fellowship for Researchers under Risk 2022.

7. References

[1] B. Bolloba's, Extremal Graph Theory, Academic Press, London, 1978.

[2] A. Grzesik, D. Král, L.M. Lovász, Elusive Extremal Graphs, Preprint (2018).

[3] S. Hoory, N. Linial, A. Wigderson. Expander Graphs and Their Applications, Bull. Amer. Math Soc. 43 (2006) 439–561. doi:10.1090/s0273-0979-06-01126-8

[4] M. Polak, et al., On the Applications of Extremal Graph Theory to Coding Theory and Cryptography, Electron. Notes Discret. Maths. 43 (2013) 329–342. doi:10.1016/j.endm.2013.07.051

[5] V. Ustimenko, et al., On the Constructions of New Symmetric Ciphers Based on Non-Bijective Multivariate Maps of Pre-Scribed Degree, Secur. Commun. Netw. (2019). doi:10.1155/2019/2137561

[6] A. Bessalov, et al., Modeling CSIKE Algorithm on Non-Cyclic Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 1–10.

[7] A. Bessalov, et al., Implementation of the CSIDH Algorithm Model on Supersingular Twisted and Quadratic Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3187, no. 1 (2022) 302–309.

[8] A. Bessalov, et al., Computing of Odd Degree Isogenies on Supersingular Twisted Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 2923 (2021) 1–11.

[9] P. Beelen, J.M. Doumen, Pseudorandom sequences from elliptic curves, Finite Fs. Appls. Codin. Theory Cryptogr. Relat. Areas (2002) 37–52. doi:10.1007/978-3-642-59435-9_3

[10] S.R. Blackburn, et al., Predicting the Inversive Generator, Lecture Notes in Comput. Sci. 2898 (2003) 264–275. doi:10.1007/978-3-540-40974-8_21

[11] S.R. Blackburn, et al., Predicting Nonlinear Pseudorandom Number Generators, Math.

Comp. 74 (2005) 1471–1494. doi:10.1090/S0025-5718-04-01698-9
[12] J. Bourgain, Mordell's Exponential Sum Estimate Revisited, J. Amer. Math. Soc. 18 (2005) 477–499. doi:10.1090/S0894-0347-05-00476-5
[13] N. Brandstätter, A. Winterhof, Some Notes On the Two-Prime Generator, IEEE Trans. Inform. Theory, 51(10) (2005) 3654–3657. doi:10.1109/TIT.2005.855615
[14] T.W Cusick, C. Ding A. Renvall, Stream Ciphers and Number Theory, North-Holland Math. Libr. 66 (2004).
[15] G. Dorfer, A. Winterhof, Lattice structure and linear complexity profile of nonlinear pseudorandom number generators, Appl. Algebra Engrg. Comm. Comput. 13 (2003) 499–508. doi:10.1007/s00200-003-0116-6
[16] Y.-C. Eun, H.-Y. Song, M.G. Kyureghyan, One-Error Linear Complexity Over Fp of Sidelnikov Sequences, Sequences and Their Applications SETA 2004, Lecture Notes in Comput. Sci. 3486 (2005) 154–165. doi:10.1007/11423461_9
[17] É. Fouvry, et al., On the Pseudorandomness of the Signs of Kloosterman Sums, J. Aust. Math. Soc. 77 (2004) 425–436.
[18] J.B. Friedlander, C. Pomerance I. Shparlinski, Period of the Power Generator and Small Values of Carmichael's Function, Math. Comp. 70 (2001) 1591–1605.
[19] J.B. Friedlander, C. Pomerance I. Shparlinski, Corrigendum to: Period of the Power Generator and Small Values of Carmichael's Function, Math. Comp. 71 (2002) 1803–1806.
[20] J.B. Friedlander, I. Shparlinski, On the Distribution of the Power Generator, Math. Comp.70 (2001) 1575–1589.
[21] D. Gomez-Perez, J. Gutierrez, I. Shparlinski, Exponential Sums with Dickson Polynomials, Finite Fields Appl. 12 (2006) 16–25.
[22] J. Gutierrez, D. Gomez-Perez, Iterations of Multivariate Polynomials and Discrepancy of Pseudorandom Numbers, Appl. Algebra, Algebraic Algorithms Error-Correcting Codes, Lecture Notes in Comput. Sci. 2227 (2001) 192–199.
[23] J. Gutierrez, I. Shparlinski, A. Winterhof, On the Linear and Nonlinear Complexity Profile of Nonlinear Pseudorandom Number-Generators, IEEE Trans. Inform. Theory, 49 (2003) 60–64.
[24] K. Gyarmati, On a Family of Pseudorandom Binary Sequences, Period. Math. Hungar. 49 (2004) 45–63. doi:10.1007/s10998-004-0522-y
[25] F. Hess, I. Shparlinski, On the Linear Complexity and Multidimensional Distribution of Congruential Generators Over Elliptic Curves, Des. Codes Cryptogr. 35 (2005) 111–117. doi:10.1007/s10623-003-6153-0
[26] D.R. Kohel, I. Shparlinski, On Exponential Sums and Group Generators for Elliptic Curves Over Finite Fields, Algorithmic Number Theory, LNCS, 1838 (2000) 395–404. doi:10.1007/10722028_24
[27] T. Lange, I. Shparlinski, Certain Exponential Sums and Random Walks on Elliptic Curves, Canad. J. Math. 57 (2005) 338–350. doi:10.4153/CJM-2005-015-8
[28] W. Meidl, A. Winterhof, On the Linear Complexity Profile of Explicit Nonlinear Pseudorandom Numbers, doi:10.1016/S0020-0190(02)00335-6 Inform. Process. Lett. 85 (2003) 13–18.
[29] W. Meidl, A. Winterhof, On the Linear Complexity Profile of Some New Explicit Inversive Pseudorandom Numbers, J. Complexity, 20 (2004) 350–355. doi:10.1016/j.jco.2003.08.017
[30] W. Meidl, A. Winterhof, On the Autocorrelation of Cyclotomic Generators, Finite Fields and Applications, LNCS, 2948 (2004) 1–11. doi:10.1007/978-3-540-24633-6_1
[31] H. Niederreiter, Linear Complexity and Related Complexity Measures for Sequences, Progress in Cryptology—INDOCRYPT 2003, LNCS, 2904 (2003) 1–17. doi:10.1007/978-3-540-24582-7_1
[32] H. Niederreiter, Constructions of (t, m, s)-Nets and (t, s)-sequences, Finite Fields Appl. 11 (2005) 578–600. doi:10.1016/j.ffa.2005.01.001
[33] H. Niederreiter, I. Shparlinski, On the Distribution of Inversive Congruential Pseudorandom Numbers in Parts of the Period, Math. Comp., 70 (2001) 1569–1574. doi:10.1090/S0025-5718-00-01273-4
[34] H. Niederreiter, I. Shparlinski, Recent Advances in the Theory of Nonlinear Pseudorandom Number Generators, Monte Carlo and quasi-Monte Carlo Methods, 2000, 86–102 (2002). doi:10.1007/978-3-642-56046-0_6

[35] H. Niederreiter, A. Winterhof, On the Distribution of Some New Explicit Nonlinear Congruential Pseudorandom Numbers, Sequences and Their Applications SETA 2004, LNCS, 3486 (2005) 266–274. doi:10.1007/11423461_19

[36] I. Shparlinski, On the Linear Complexity of the Power Generator, Des. Codes Cryptogr. 23 (2001) 5–10. doi:10.1023/A:1011264815860

[37] I. Shparlinski, Cryptographic Applications of Analytic Number Theory. Complexity Lower Bounds and Pseudorandomness, PCS, 22 (2003). doi:10.1007/978-3-0348-8037-4

[38] I. Shparlinski, A. Winterhof, On the Linear Complexity of Bounded Integer Sequences Over Different Moduli, Inform. Process. Lett. 96 (2005) 175–177. doi:10.1016/j.ipl.2005.08.004

[39] A. Topuzoğlu, A. Winterhof, On the Linear Complexity Profile of Nonlinear Congruential Pseudorandom Number Generators of Higher Orders, Appl. Algebra Engrg. Comm. Comput, 16 (2005) 219–228. doi:10.1007/s00200-005-0181-0

[40] O. Pustovit, V. Ustimenko, A New Stream Algorithms Generating Sensetive Digests of Digital Documents, Math. Modell. Econs. 3 (2019) 18–33. doi:10.15439/2021F80

[41] A. Canteaut, F.X. Standaert, Advances in Cryptology – EUROCRYPT 2021, 40th Annual International Conference on the Theoryand Applications of Cryptographic Techniques Zagreb, Croatia, October 17–21, 2021. doi:10.1007/978-3-030-77870-5

[42] F. Lazebnik, V. Ustimenko, A.J. Woldar, A New Series of Dense Graphs of High Girth, Bull. Amer. Math. Soc. 32(1) (1995) 73–79. doi:10.1090/s0273-0979-1995-00569-0

[43] V. Ustimenko, M. Klisowski, On Noncommutative Cryptography with Cubical Multivariate Maps of Predictable Density, Advs. Intell. Systs. Computing (AISC) 998 (2019) 654–674. doi:10.1007/978-3-030-22868-2_47

[44] D.N. Moldovyan, N.A. Moldovyan, A New Hard Problem over Non-commutative Finite Groups for Cryptographic Protocols, Computer Netw. Secur. (2010) 183–194. doi:10.1007/978-3-642-14706-7_14

[45] V. Shpilrain, A. Ushakov, The Conjugacy Search Problem in Public Key Cryptography: Unnecessary and Insufficient, Appl. Algebra Eng. Commun. Comput. 17 (2006) 285–289. doi:10.1007/s00200-006-0009-6

[46] D. Kahrobaei, B. Khan, A Non-Commutative Generalization of ElGamal Key Exchange using Polycyclic Groups, IEEE Globecom 2006, San Francisco, CA, USA, 2006. doi: 10.1109/GLOCOM.2006.

[47] A. Myasnikov, V. Shpilrain, A. Ushakov, Group-based Cryptography, Birkhäuser Verlag, 2008.

[48] Z. Cao, New Directions of Modern Cryptography, CRC Press, Taylor & Francis Group, 2012. doi:10.1201/b14302

[49] G. Maze, C. Monico, J. Rosenthal, Public Key Cryptography Based on Semigroup Actions, Adv. Math. Commun. 1(4) (2007) 489–507. doi:10.3934/amc.2007.1.489

[50] P.H. Kropholler, et al., Properties of Certain Semigroups and Their Potential as Platforms for Cryptosystems, Semigroup Forum 81 (2010) 172–186. doi:10.1007/S00233-010-9248-8

[51] G. Kumar, H. Saini, Novel Noncommutative Cryptography Scheme Using Extra Special Group, Secur. Commun. Netws. (2017). doi: 10.1155/2017/9036382

[52] V. Roman'kov, A Nonlinear Decomposition Attack, Groups Complex. Cryptol. 8(2) (2016), 197–207. doi:10.1515/gcc-2016-0017

[53] V. Roman'kov, An Improved Version of The AAG Cryptographic Protocol, Groups Complex. Cryptol. 11(1) (2019) 35–42. doi:10.1515/gcc-2019-2003

[54] A. Ben-Zvi, A. Kalka, B. Tsaban, Cryptanalysis via Algebraic Span, Annu. Int. Cryptol. Conf. 1(10991) (2018) 255–274. doi:10.1007/978-3-319-96884-1_9

[55] B. Tsaban, Polynomial-Time Solutions of Computational Problems in Noncommutative-Algebraic Cryptography, J. Cryptol. 28(3) (2015) 601–622. doi:10.1007/s00145-013-9170-9

[56] V. Ustimenko, On The Families of Stable Transformations of Large Order and Their Cryptographical Applications, Tatra Mt. Math. Publ., 70 (2017), 107–117. doi:10.1515/tmmp-2017-0021

[57] V. Ustimenko, U. Romanczuk-Polubiec, A. Wroblewska, Expanding Graph of the Extremal Graph Theory and Expanded Platforms of Post-Quantum Cryptography, Anns Comput. Sci. Inf. Systs. 19 (2019) 41–46.

[58] V. Ustimenko, On Extremal Graph Theory and Symbolic Computations, Reports of the National Academy of Sci. Ukraine 2(2) (2013) 42–49.
[59] V. Ustimenko, On a Group Theoretical Constructions of Expanding Graphs, J. Algebra Discret. Maths. 3 (2003) 102–109.
[60] V. Ustimenko, U. Romanczuk, On Extremal Graph Theory, Explicit Algebraic Constructions of Extremal Graphs and Corresponding Turing Encryption Machines, Artif. Intell. Evolut. Computing Metaheuristics 427 (2013) 257–285. doi:10.1007/978-3-642-29694-9_11
[61] V. Ustimenko, Coordinatisation of Trees and their Quotients, Voronoj's Impact on Modern Science, Kyiv, Institute of Mathematics, 2 (1998) 125–152.
[62] V. Ustimenko, CRYPTIM: Graphs as Tools for Symmetric Encryption, Int. Symp. Appl. Algebra Algebraic Algorithms Error-Correct. Codes 2227 (2001) 278–286. doi:10.1007/3-540-45624-4_29
[63] V. Ustimenko, On the Extremal Graph Theory for Directed Graphs and Its Cryptographical Applications, Codin. Theory Cryptogr. 3 (2007) 181–200. doi:10.1142/9789812772022_0012
[64] V. Ustimenko, Graphs in Terms of Algebraic Geometry, Symbolic Computations and Secure Communications in Post-Quantum world, UMCS Editorial House, Lublin, 2022.