On desynchronised multivariate El Gamal algorithm

Vasyl Ustimenko

Institute of Mathematics, Maria Curie-Sklodowska University,
pl. M. Curie-Sklodowskiej 5, 20-031 Lublin, Poland
vasyl@hektor.umcs.lublin.pl
http://www.umcs.pl/en/

Abstract. Families of stable cyclic groups of nonlinear polynomial transformations of affine spaces K^n over general commutative ring K of increasing with n order can be used in the key exchange protocols and related to them El Gamal multivariate cryptosystems. We suggest to use high degree of noncommutativity of affine Cremona group and modify multivariate El Gamal algorithm via the usage of conjugations for two polynomials of kind g^k and g^{-1} given by key holder (Alice) or giving them as elements of different transformation groups. We present key exchange protocols based on *twisted discrete logarithms problem* which uses noncommutativity of semigroup. Recent results on the existence of families of stable transformations of prescribed degree and density and exponential order over finite fields can be used for the implementation of schemes as above with feasible computational complexity. We introduce an example of a new implemented quadratic multivariate cryptosystem based on the above mentioned ideas.

Keywords: Multivariate Cryptography, stable transformations, shifted multivariate El Gamal algorithm, desyncronisation diagram

1 Introduction

Multivariate cryptography [1] is one of the directions of Post Quantum Cryptography (PQC). Some examples of multivariate cryptography algorithms can be constructed in terms of algebraic graph theory (see section 2, which is a brief introduction to this area). Section 3 is devoted to Diffie - Hellman type key exchange algorithm for cyclic subgroup of affine Cremona group and related idea of a stable transformation of affine space over general commutative ring. Basic version of multivariate El Gamal algorithm is also discussed there, some results on constructions of examples of families of stable transformations are observed. Notice that one can use more general families of transformations of bounded degree and large order instead of stable transformations in mentioned above protocol and cryptosystem. For instance, in the case of finite fields one can use classical Singer transformations τ_n of vector spaces ${F_q}^n$ of order $q^n - 1$

(see [2] or [3] and further references) and a family of stable maps g_n of degree d. Then elements of kind $f_n = {g_n}^{-1}\tau_n g_n$ form a family of order $q^n - 1$ and degree bounded by d^2. Notice that inverses of f_n also have degree $\leq d^2$. In the majority of known cases of stable families of g_n mentioned in section 3 one can easily check that related transformations f_n are nonlinear. Such elements can be used as generators of cyclic groups used in multivariate Diffie-Hellman protocols an multivariate El Gamal cryptosystems.

Section 4 is devoted to shifted El Gamal cryptosystem, which uses high level of noncommutativity in affine Cremona group. We also consider more general protocols than Diffie Hellman scheme where key holder uses conjugations in noncommutative group. Security of such modified protocols is connected with *twisted discrete logarithm* problem. The idea of desynchronisation over diagram is used to modify El Gamal algorithm where conjugates of g^k and g^{-1} are elements of different factor groups presented in section 5. Next section is devoted to explicit constructions of families of stable transformations of prescribed degree. In section 7 we consider the generalisation of *twisted discrete logarithm problem* with usage of commuting subgroups A and B of a chosen semigroup. In the last section we introduce implemented desynchronised El Gamal algorithm based on quadratic stable transformations of large order.

2 On Post Quantum and Multivariate Cryptography

Post Quantum Cryptography serves for the research of asymmetrical cryptographical algorithms which can be potentially resistant against attacks based on the use of quantum computer.

The security of currently popular algorithms is based on the complexity of the following three known hard problems: integer factorisation, discrete logarithm problem, discrete logarithm for elliptic curves.

Each of these problems can be solved in polynomial time by Peter Shor's algorithm for theoretical quantum computer.

Despite that the known nowadays small experimental examples of quantum computer are not able to attack currently used cryptographical algorithm, cryptographers already started research on postquantum security. They also should mind new results of general complexity theory such as complexity estimations of isomorphism problem obtained by L. Babai [4].

The history of international conferences on Post Quantum Cryptography (PQC) started in 2006.

We have to notice that Post Quantum Cryptography differs from Quantum Cryptography, which is based on the idea of usage of quantum phenomena to reach better security.

Modern PQC is divided into several directions such as Multivariate Cryptography, Lattice base Cryptography, Hash based Cryptography, Code base Cryptography, studies of isogenies for superelliptic curves.

The oldest direction is Multivariate Cryptography which uses polynomial maps of affine space K^n defined over a finite commutative ring K into itself as encryption tools. It exploits the complexity of finding solution of a system of nonlinear equations from many variables. Multivariate cryptography uses as security tools a nonlinear polynomial transformations of kind:

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

acting on the affine space K^n, where $f_i \in K[x_1, x_2, \ldots, x_n]$, $i = 1, 2, \ldots, n$ are multivariate polynomials given in standard form, i. e. via a list of monomials in chosen order. Important ideas in this direction reader can find in ([6], [7], [8]).

Current task is a search of an algorithm with resistance to cryptoanalytic attacks based on ordinary Turing machine. Multivariate cryptography has to demonstrate practical security algorithm which can compete with RSA, Diffie-Hellman protocols, popular methods of elliptic curve cryptography (see [1], [9]).

This is still a young promising research area with the current lack of known cryptosystems with the proven resistance against attacks with the use of ordinary Turing machines. Studies of attacks based on Turing machine and Quantum computer have to be investigated separately because of different nature of two machines, deterministic and probabilistic respectively.

Recall that K stands for a commutative ring. Symbol $S(K^n)$ stands for the affine Cremona semigroup of all polynomial transformations of affine space K^n.

Multivariate cryptography started from studies of potential for the special quadratic encryption multivariate bijective map of K^n, where K is an extension of finite field F_q of characteristic 2. One of the first such cryptosystems was proposed by Imai and Matsumoto, cryptanalysis for this system was invented by J. Patarin. The survey on various modifications of this algorithm and corresponding cryptanalysis the reader can find in [1]. Various attempts to build secure multivariate public key were unsuccessful, but the research of the development of new candidates for secure multivariate public keys is going on (see for instance [10] and further references).

Applications of Algebraic Graph Theory to Multivariate Cryptography were recently observed in [11]. This survey is devoted to algorithms based on bijective maps of affine spaces into itself. Applications of algebraic graphs to cryptography started from symmetric algorithms based on explicit constructions of extremal graph theory and their directed analogue. The main idea is to convert an algebraic graph in a finite automaton and to use the pseudorandom walks on the graph as encryption tools. This approach can be also used for the key exchange protocols. Nowadays the idea of "symbolic walks" on algebraic graphs when a walk on a graph depends on parameters given as special multivariate polynomials in variables depending of plainspace vector brings several public key cryptosystems. Other source of graphs suitable for cryptography is connected with finite geometries and their flag system. (see [11] and further references). Bijective multivariate sparse encryption maps of rather high degree based on walks in algebraic graphs were proposed in [12].

One of the first usage of non bijective map of multivariate cryptography was in *oil and vinegar* cryptosystem analysed in [5]. The observation of the further research on non bijective multivariate cryptography a reader can find in [19] (proceedings of the International Conference DIMA 2015 in Belarus), where the new cryptosystems with non bijective multivariate encryption maps on the affine space ${Z_m}^n$ into itself was presented together with some results concerning construction of bijective stable transformations of large order of finite vector spaces. The technique of [13] is based on the usage of the embeddings of projective geometries into corresponding Lie algebra (see [25] and further references).

3 On stable multivariate transformations for the key exchange protocols

It is widely known that Diffie-Hellman key exchange protocol can be formally considered for the generator g of a finite group or semigroup G. Users need a large set $\{g^k | k = 1, 2, \dots\}$ to make it practical. One can see that security of the method depends not only on abstract group or semigroup G but on the way of its representation. If G is a multiplicative group F_p^* of finite field F_p than we have a case of classical Diffie-Hellman algorithm. If we change ${F_p}^*$ for isomorphic group Z_{p-1} then the security will be completely lost. We have a problem of solving linear equation instead of discrete logarithm problem to measure the security level.

Let K be a commutative ring. $S(K^n)$ stands for the Cremona affine semigroup of all polynomial transformation of affine space K^n. Let us consider a multivariate Diffie-Hellman key exchange algorithm for the generator $g(n)$ semigroup G_n of affine Cremona semigroup.

Correspondents (Alice and Bob) agree on this generator $g(n)$ of group of kind

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

acting on the affine space K^n, where $f_i \in K[x_1, x_2, \dots, x_n]$, $i = 1, 2, \dots, n$ are multivariate polynomials. Alice chooses a positive integer k_A as her private key and computes the transformation ${g(n)}^{k_A}$ (multiple iteration of $g(n)$ with itself).

Similarly Bob chooses k_B and gets ${g(n)}^{k_B}$. Correspondents complete the exchange: Alice sends ${g(n)}^{k_A}$ to Bob and receives ${g(n)}^{k_B}$ back from him.

Now Alice and Bob computes independently common key h as $({g(n)}^{k_B})^{k_A}$ and $({g(n)}^{k_A})^{k_B}$ respectively.

So they can use coefficients of multivariate map $h = {g(n)}^{k_B k_A}$ from G_n written in the standard form.

There are obvious problems preventing the implementation of this general method in practice. In case $n = 1$ the degree $\deg(fg)$ of composition fg of elements $f, g \in S(K)$ is simply the product of $\deg(f)$ and $\deg(g)$. Such effect can happen in multidimensional case: $(\deg(g))^x = \deg(g^x) = b$. It causes the reduction of discrete logarithm problem for multivariate polynomials to number theoretical problem. If g is a bijection of degree d and order m then $d^x = b$ in cyclic group Z_m. Similar reduction can appear in case of other degree functions $s(x) = \deg(g^x)$. If $s(x)$ is a linear function than multivariate discrete logarithm problem with base g is reducible to the solution of linear equation. The degenerate case $\deg(g^x) = const$ is an interesting one because in such situation the degree function does not help to investigate multivariate discrete logarithm.

We refer to the sequence of multivariate transformations $f(n) \in S(K^n)$ as stable maps of degree d if $\deg(f(n))$ is a constant $d, d > 2$ and $\deg(f(n)^k) \leq d$ for $k = 1, 2, \ldots$ (see [15]). If τ_n is a bijective affine transformation of K^n, i.e. a bijective transformation of degree 1, then the sequence of stable maps $f(n)$ can be changed for other sequence of stable maps $\tau f(n) \tau^{-1}$ of the same degree d.

The first families of special bijective transformations of K^n of bounded degree were generated by *discrete dynamical systems* defined in [14] in terms of graphs $D(n, K)$. In the paper [16] the fact that each transformation from these families of maps is cubic was proven. In [15] authors notice that this family is stable, the order of its members grow with the increase of parameter n and suggest key exchange protocols with generators from these families. In fact graphs $D(n, K)$ were introduced in [17] in a connection to their cryptographical applications. Graphs $D(n, q) = D(n, F_q)$ appeared even earlier [18], [19] in a connection to their applications to extremal combinatorics.

Other example of stable families of cubic transformations over general commutative ring K is associated with the dynamical systems of other family of algebraic graphs $A(n, K)$ (see [20] and further references). The family of quadratic stable transformations of K^n were introduced in [21], the order of the maps is not yet evaluated.

Recall that the other important property for the generator $g(n)$ in the described above protocol is a large cardinality of $\{g(n)^k | k = 1, 2, \ldots\}$. Let us assume that $g(n)$ are bijections. We say that $g(n)$ is a family of exponential order if the order $|g(n)|$ is at least $a^{\alpha n}$, where $a > 1$ and $\alpha > 0$ are constants. The famous family of linear bijections over F_q of exponential order is formed by Singer cycles $s(n)$, they have order $q^n - 1$.

As it was mentioned in introduction we can use Singer cycles for a creation of nonlinear families of exponential growth which can serve as bases for the described above key exchange protocols in the following way. We say that a family of nonlinear transformations $f(n)$ of affine space K^n is the family of strongly bounded degree if degrees of all functions $f(n)^k$, $k = 1, 2, \ldots$ are bounded above by constant d. It is easy to see that a class of such families is slightly wider than a class of stable transformation. Let $g(n)$ be a family of bijective stable transformations of ${F_q}^n$ of degree t, then $g(n)^{-1} s(n) g(n)$ is a family of exponential order $q^n - 1$ and strongly bounded degree (bounded above by t^2).

The above key exchange protocol can be used to design the following multivariate ElGamal cryptosystem (see [22]). Alice takes generator $g(n)$ of the group G_n together with its inverse $g(n)^{-1}$. She sends the pair $(g(n), g(n)^{-1})$ to Bob. He will work with the plainspace K^n as public user.

At the beginning of each session Alice chooses her private key k_A. She computes $f = g(n)^{k_A}$ and sends it to Bob.

Bob writes his text $(p_1, p_2, \ldots, p_n)$, chooses his private key k_B and creates the ciphertext $f^{k_B}((p_1, p_2, \ldots, p_n)) = $ c.

Additionally he computes the map ${g(n)^{-1}}^{k_B} = h(n)$. He sends the pair $(c_1, c_2, \ldots, c_n), h(n)$ to Alice.

Alice computes $h(n)^{k_A}(\mathrm{c}) = (p_1, p_2, \ldots, p_n)$.

REMARK 1. It is proven (see [22]) that the security level of above multivariate Diffie-Hellman and ElGamal algorithms is the same. It is based on the multivariate discrete logarithm problem.

Solve the equation $g^x = d$, where g and d are elements of special cyclic subgroup G_n of affine Cremona group.

REMARK 2. It is clear, that the algorithm above can be formally considered for the general pair of bijective nonlinear polynomial transformations $g(n)$ and $g(n)^{-1}$ of of free module K^n. But for computational feasibility we will require that $g(n)$ has to be a family of strongly bounded degree. Obviously parameter $|G_n|$ has to grow with the increase of n.

4 On the shifted multivariate ElGamal cryptosystems

ALGORITHM 1.

We say that family of elements $h(n) \in C(K^n)$ of affine Cremona group is of symmetrical bounded degree if sequences $\deg h(n)$ and $\deg h^{-1}(n)$ are bounded by some independent constant.

We refer to a family $g(n) \in C(K^n)$ as a family of strictly bounded degree if integers $\deg(g^k(n))$ are bounded by independent from n and k constants.

We suggested at CECC 2016 the following modification of the algorithm described in previous section. Assume that Alice takes the family of generators $g(n)$ of cyclic groups G_n of large order with its inverse $g(n)^{-1}$ and it is a family of strictly bounded degree. Two other families $h_1(n)$ and $h_2(n)$ are families of symmetrically bounded degree and the sequences of ${h_1}^{-1}(n)$ and ${h_2}^{-1}(n)$ are computable for Alice.

1) Alice chooses large positive integer k_A as her private key.

2) After that she computes $R(n) = g(n)^{k_A} \in C(K^n)$ and its conjugation $Q(n) = h_1(n)R(n){h_1}^{-1}$.

3)Alice computes the transformation $H(n) = h_2(n)g(n)^{-1}h_2(n)^{-1}$.

She sends $G(n)$ and $H(n)$ to Bob.

Bob chooses his private key k_B, writes his plaintext $\mathrm{p} = (p_1, p_2, \ldots, p_n)$, computes $H^{k_B}(n)$ and the ciphertext $\mathrm{c} = Q^{k_B}(n)(\mathrm{p})$ via multiple application (k_B times))of $Q(n)$ to the tuple from K^n.

Bob sends vector c to Alice together with $H' = H^{k_B}$

Alice decrypts via the following steps:

1. She computes g^{-k_B} as ${h_2}^{-1}(n)H'(n)h_2(n)$. Really ${h_2}^{-1}H'h_2 =$ $= {h_2}^{-1}(h_2 g^{-k_B} {h_2}^{-1})h_2$.
2. Alice creates $H_1 = h_1 g^{-k_B} {h_1}^{-1}$.
3. She applies k_A times H_1 to ciphertext and computes the plaintext. In fact $H_1^{k_A}(\mathrm{c}) = \mathrm{p}$.

The shifted algorithm may have better protection against attacks by adversary. One can choose $h_2(n)$ to make the discrete logarithm problem in affine Cremona group with the new base $H(n)$ harder than one in a case of base $g(n)^{-1}$. Additionally the adversary has to compute the inverse of $Q(n)$. The choice of h_2 can change the complexity of this problem without change of the discrete logarithm complexity.

REMARK 1. Alice can work with a stable map $g(n)$ of a large order.

ALTERNATIVE ALGORITHM 2 with active participation of Bob follows.

Let us consider the following scheme.

Alice take maps f and f^{-1} from affine Cremona group. She chooses k_A and sends f^{k_A} and f^{-1} to Bob.

Bob takes k_B and h from $C(K^n)$. He takes plaintext p in K^n and applies $h^{-1}f^{k_A}h$ multiply (k_B times) to form ciphertext c. He computes $g = h^{-1}f^{-k_B}h$ and sends it to Alice.

Alice decrypts via application k_A times transformation g to the ciphertext.

REMARK. Here the shifted discrete logarithm problem appears: Solve for x the equation $h^{-1}f^{-1x}h = g$ with unknown h. Notice that adversary may have a look at pair f^{-1} and f^{k_A} which are elements of the same cyclic group. So he has to solve ${f^{-1}}^x = b$ and find k_A via computation of the order of cyclic group. Adversary takes g^{k_A} and decrypts. So for breaking the algorithm one has to solve standard multivariate discrete logarithm problem and compute the order of cyclic group with generator f^{-1}.

THE MODIFICATION OF ALGORITHM 2.

Let us assume that G is a subgroup of $S(K^n)$ and Alice have a homomorphism μ from semigroup S' into G. We assume that S' is a subsemigroup of $S(R^m)$, where R is a finite commutative ring R.

Alice takes elements f an f' such that $\mu(ff') = e$, where e is an identity map from G. She takes k_A and forms $g_A = \mu(f^{k_A})$ for Bob. We assume that the subsemigroup S' and group G are unknown for Bob, but the information on the μ is given partially: Bob has pairs $(g_i, \tilde{g}_i = \mu((g_i)))$, for invertible elements $g_i \in S$, $i = 1, 2, \ldots, t$. He also receives $f' \in S$.

So Bob takes parameter k_B and chooses $i_1, i_2, \ldots, i_l$ and positive numbers $\alpha_1, \alpha_2, \ldots, \alpha_l$ to form word $h = g_{i_1}^{\alpha_1} g_{i_2}^{\alpha_2} \ldots g_{i_l}^{\alpha_l}$, $i_s \in \{1, 2, \ldots, t\}$, $s = 1, 2, \ldots, l$ and compute $\delta = \mu(h)$ as an element of G and its inverse $\mu(h^{-1})$.

So he computes $\Delta = \delta g_A \delta^{-1}$, writes plaintext p $\in K^n$ and creates the ciphertext c via application of Δ exactly k_B times to p.

Additionally Bob takes $g_B = h{f'}^{k_B}h^{-1}$ of Cremona semigroup $S(R^n)$ written in a standard form and sends it to Alice.

Alice computes group element $H_1 = \mu(g_B)$, $F = {H_1}^{K_A}$ and the plaintext as F(c).

REMARK ON MULTIVARIATE IMPLEMENTATION.

Alice can take multivariate bijective maps $\pi_1 \in C(K^n)$ and $\pi_2 \in C(R^m)$ and work with group $G' = \pi_1 G {\pi_1}^{-1}$ and $S'' = \pi_2 S' \pi_2$. Knowledge of π_1 and π_2 allows her to work with $\eta' : S'' \to G'$ which is a composition of isomorphism of S'' onto S', induced by the conjugation with ${\pi_2}^{-1}$, homomorphism $\eta : S' \to G$

and isomorphism of G and G' (induced by the conjugation with ${\pi_2}^{-1}$. She gives to Bob the following data.

$g = \pi_1(g_A){\pi_1}^{-1}$, $g' = \pi_2(f'){\pi_2}^{-1}$, $s_i = \pi_1(\mu(g_i))$, $i = 1, 2, \ldots, t$ and $r_i = \pi_2(g_i)$.

Adversary has to work with homomorphism between semigroup S_2 generated by r_i and group G_1 generated by s_i. He has to take $< S_2, g' >$ and $< S_1, g >$ and search for appropriate expanded homomorphism η between this objects for which $\eta(g')^x = g^{-1}$ for some parameter x. Notice that g and g' can be outside of S_1 and S_2. This "twisted discrete logarithm problem" can be a difficult task. The problem to compute the value of η in point $\pi_2 g_B \pi_2$ could be a very difficult task because the decomposition of g_B into r_i and g' is unknown for him.

MODIFIED DIFFIE HELLMAN KEY EXCHANGE.

Finally we look at the case of *symmetric use of conjugation* by Alice and Bob. We start with the modification of key exchange algorithm.

Let us assume that Alice and Bob have group G together with choosen representatives $g \in G$ and $h \in G$. Alice takes two parameters k_A and r_a as her private keys, forms element $g_A = h^{r_A} g^{k_A} h^{-r_A}$ and sends it to Bob. In his turn Bob forms private key as (k_B, r_B), computes $g_B = r_B g^{k_B} h^{-r_B}$ and passes it to Alice. Secondly correspondents Alice and Bob compute the collision element as $h^{r_A} {g_B}^{k_A} h^{-r_A}$ and

$h^{r_B} {g_A}^{k_B} h^{-r_B}$ which is simply $h^{r_A+r_B} g^{k_A k_B} h^{-r_A-r_B}$.

The adversary can look at the equation $h^y g^x h^{-y} = g_A$. We refer to this algorithm as twisted Diffie - Hellman key exchange protocol.

ALGORITHM 3.

Now we introduce symmetric twisted El Gamal multivariate algorithm.

We will use the idea of written above key exchange protocol in the case when G is an affine Cremona group $C(K^n)$ where K is a finite commutative ring. So Alice sends $g^{-1}, h \in S(K^n)$ to together with g_A as above.Bob selects k_B, conjugates g_A with h^{r_B} and applies this map k_B times to his plaintext p $= (p_1, p_2, \ldots, p_n)$. He sends the ciphertext together with his element $g_B = h^{r_B} g^{-1 k_B} h_{-r_B}$ to Alice.

Alice computes $h^{r_A} {g_B}^{k_A} h^{r_A}$, applies this transformation to the ciphertext and gets the plaintext.

ALGORITHM 4.

Let us assume that the homomorphism μ from subsemigroup S of $S(R^n)$ into subgroup G of $C(K^n)$ is given.

Alice will take two noncommutative pairs of elements (g, g') and (h, h') such that $\mu(gg') = e$, $\mu(h, h') = e$ and group elements $\mu(g)$ and $\mu(h)$ have large order. She is keeping semigroup S and G in secret. Notice that she can always change S and G for theirs conjugations with invertible elements $\pi_1 \in C(R^n)$ and $\pi_2 \in C(K^m)$.

Alice chooses integers k_A and α and computes $g_A = \mu(h^\alpha)\mu(g)^{k_A}\mu(h^{-\alpha})$. She sends this element to Bob together with g', h, h' and $\mu(h)$. Bob writes plaintext p $= (p_1, p_2, \ldots, p_n)$ and chooses parameter k_B and β. He uses group element $\Delta =$

$\mu(h^{\beta}{g_A}^{k_B}h^{-\beta})$ and computes Δ(p) = c, which is the ciphertext. Additionally he forms $\delta = h^{\beta}{g'}^{k_B}{h'}^{-\beta}$ and sends it to Alice.

Alice computes Δ^{-1} as $\mu(h^{\alpha}\delta^{k_A}{h'}^{-\alpha})$ and decrypt.

GENERALISATION of algorithm 4.

Alice uses S, G, g and g' as above assume that h_i, h'_i, $i = 1, 2, \ldots, t$ are elements of S such that $\mu(h_i h'_i) = e$. Additionally Alice takes pair $d \in G$, d^{-1} such that $[d\mu(h_i)] = e$ for $i = 1, 2, \ldots, t$. Alice choses integer k_A and sends $g_A = d\mu(g^{k_A})d^{-1}$ to Bob together with elements g', h_i, h'_i and $\mu(h_i)$.

Bob chooses k_B, writes his plaintext p and forms the pair of elements of kind $h = h_{i_1}^{a_1} h_{i_2}^{a_2} \ldots h_{i_t}^{a_t}$, $h' = {h'_{i_1}}^{a_1} {h'_{i_2}}^{a_2} \ldots {h'_{i_t}}^{a_t}$ computes element $g_B = h{g'}^{k_B}h'$ and ciphertext $c = \mu(h){g_A}^{k_B}\mu(h)^{-1}$(p) and sends it to Alice.

Alice decrypts via the application of $d\mu(g_B)^{k_A}d^{-1}$ to ciphertext.

5 On desynchronised El Gamal algorithm over diagram

Let us consider the diagram $G_1 \leftarrow G \rightarrow G_2$, where G, G_1 and G_2 are semigroups, G_1 is a semigroup with unity Assume that arrow with nodes G_1 and G corresponds to homomorphism η_1 from G into G_1, arrow between G and G_2 corresponds to injective homomorphism η_2 from G to G_2. Let is denote $\eta_1(G)$ and $\eta_2(G)$ as H and L. One can work with the extended diagram $G_1 \leftarrow H \leftarrow G \rightarrow L \rightarrow G_2$. Assume that the pair of elements g and g' of elements of G such that $\eta_1(gg') = e$ is given together with automorphisms α and β of G. Additionally we assume that G_1 and G_2 are affine Cremona semigroups of affine spaces K^n and R^m over finite commutative rings K and R. Let us assume that automorphisms ϕ_1, ϕ_2 and ϕ_3 of groups G_1 , G_2 and H are given.

We refer to the given above information as El Gamal commutative diagram data. Public key owner Alice has this information. The transformation semigroups G_1 and G_2 are known publicly. The rest of data Alice has to keep in secrecy.

In further examples we assume that ϕ_1 and ϕ_2 are internal automorphisms of conjugation with an invertible polynomial given in standard form together with its inverse.

Additionally Alice chooses her private key as positive integer k_A, $k_A > 1$. She computes g^{k_A}, $\alpha(g^{k_A})$ and $\beta(g')$). Alice forms $\eta_2(\beta(g'))$ and writes $\phi_2(\eta_2(\beta(g')))$ as multivariate transformation G_2 on R^m:

$x_1 \rightarrow g_1(x_1, x_2, \ldots, x_n)$,
$x_2 \rightarrow g_2(x_1, x_2, \ldots, x_n)$,
$\ldots$
$x_m \rightarrow g_m(x_1, x_2, \ldots, x_m)$.

Alice computes $\phi_3\eta_1(\alpha(g^{k_A})) \in H$ and $G_A = \phi_1(\phi_3(\eta_1(\alpha(g^{k_A}))))$. She has to write G_A as multivariate map on K^n written in a standard form.

Alice sends G and G_A to public user Bob.

THE ENCRYPTION PROCESS: Bob writes his plaintext as element p $= (p_1, p_2, \ldots, p_n) \in K^n$ of affine space K^n. He chooses parameter K_B and computes the ciphertext $c = {G_A}^{k_B}$(p). He forms G^{k_B} and sends it to Alice.

DECRYPTION: Alice computes $F_1 = {\phi_2}^{-1}(G^{k_B}) \in L$, calculates $F_2 = {\eta_2}^{-1}(F_1) \in G$ and gets $F_3 = \beta^{-1}(F_2)$. Secondly she computes $F_4 = {F_3}^{k_A}$, $F_5 = \alpha(F_4)$ and $F_6 = \eta_2(F_5)$, $F_7 = \phi_3(F_6)$ and $F_8 = \phi_1(F_7)$. Alice gets plaintext p as F_8(c).

EXAMPLE 1. Let us take the general linear semigroup $M(n+k, F_q)$ of all linear transformations of vector space $V = {F_q}^n$. Let $e_1, e_2, \ldots, e_n, e_{n+1}, e_{n+2}, \ldots, e_{n+t}$ be a standard basis of V. We take subspace $W =< e_1, e_2, \ldots, e_n >$ spanned by listed basic vectors. Let G be a semigroup of all linear transformations τ of V for which W is an invariant subspace and the restriction of τ on W is a bijective map. Let $g \in G$ and g' be an

elements which restrictions on W are Singer cycles C and C'. The restriction of an element from G onto W defines homomorphism μ_1 onto $GL(n, F_q)$. Let μ_2 be the natural embedding of $GL(n, F_q)$ into $GL(n, F_{q^m}) = G_1$, $m \geq 1$. Assume that η_1 is the composition of μ_1 and μ_2. We need also the natural embedding of $M(n+k, F_q)$ into $M(n+k, F_{q^t})$. Its restriction on G will be denoted as η_2.

We take for α and β as in written above algorithm internal automorphism $x \to g_1 x {g_1}^{-1}$ and $x \to g_2 x {g_2}^{-1}$, where g_1 and g_2 are certain invertible elements of G. Alice will apply automorphism ϕ_3 of $H = GL(n, F_q)$, which is a composition of contragradient automorphism $x \to (x^T)^{-1}$, where x^T is a transposed matrix for x with some internal automorphism of H. We choose map ϕ_1 as an internal automorphism of Affine Cremona Semiroup $S({F_{q^m}}^n)$ of kind $x \to hxh^{-1}$, where h is some deformation of invertible stable transformation of degree d_1 given in a standard form. Similarly ϕ_2 is an internal automorphism $x \to jxj^{-1}$ for certain deformation j of invertible stable transformation of degree d_2 from $C({F_{q^t}}^{k+n})$.

REMARK 1. In the case of stable h and j Alice can change them for elements of kind $h' = h^{k_1}$ and $j' = j^{k_2}$ or there deformations of kind $A_1 h' B_1$ and $A_2 j' B_2$, where A_1 and B_1 are bijective affine transformations of vector space ${F_{q^m}}^n$ and A_2 and B_2 are bijective affine transformations of vector space ${F_{q^t}}^{n+k}$.

REMARK 2. Assume that Alice choose k_A such that $(k_A, q^n - 1) = 1$. Then Bob receives two multivariate maps. One of them is the bijective transformation of degree $\leq {d_1}^2$ of vector apace ${F_{q^m}}^n$ and other is a map of degree $\leq {d_2}^2$ of ${F_{q^t}}^{k+n}$, which generates semigroup with at least $q^n - 1$ elements.

REMARK 3. Graphs based constructions of quadratic and cubic stable transformations of affine space K^n over general commutative degree are observed in section 3. Methods of construction of stable transformation of K^n of fixed prescribed degree based on graphs $D(n, K)$ are presented in [24].

6 On explicit constructions of stable quadratic maps of large order

We define Double Schubert Graph $DS(k, K)$ over commutative ring K as incidence structure defined as disjoint union of points from

$PS = \{(x) = (x_1, x_2, \ldots, x_k, x_{1,1}, x_{1,2}, \ldots x_{k,k})| \in (x) \in K^{(k+1)k}\}$ and lines from $LS = \{[y] = [y_1, y_2, \ldots, y_k, y_{1,1}, y_{1,2}, \ldots y_{k,k}]| \in (y) \in K^{(k+1)k}\}$ where (x) is incident to [y] if and only if $x_{i,j} - y_{i,j} = x_i y_j$ for $i = 1, 2, \ldots, k$, $j = 1, 2, \ldots, k$.

It is convenient to assume that indexes of kind i, j are placed in lexicographical order.

REMARK. *The term* Double Schubert Graphs *is chosen because points and lines of $DS(k, F_q)$ can be treated as subspaces of ${F_q}^{2k+1}$ of dimensions $k+1$ and k which form two largest Schubert cells. Recall that the largest Schubert cell is the largest orbit of group of unitriangular matrices acting on the variety of subsets of given dimensions.* (see [25] and further references).

We define the colour of point (x) $= (x_1, x_2, \ldots, x_k, x_{1,1}, x_{1,2}, \ldots x_{k,k})$ from PS as tuple $(x_1, x_2, \ldots, x_k)$ and the colour of line

[y] $= [y_1, y_2, \ldots, y_k, y_{1,1}, y_{1,2}, \ldots y_{k,k}]$ as tuple $(y_1, y_2, \ldots, y_k)$. For each vertex v of $DS(k, K)$ there is a unique neighbour $N_\alpha(\mathrm{v})$ of given colour $\alpha = (a_1, a_2, \ldots, a_k)$, $a_i \in K$, $i = 1, 2, \ldots, k$.

The symbolic colour g from $K[z_1, z_2, \ldots, z_k]^k$ of kind $f_1(z_1, z_2, , \ldots, z_k)$, $f_2(z_1, z_2, \ldots, z_k)$, $\ldots$, $f_k(z_1, z_2, \ldots, z_k)$, where f_i are polynomials from $K[z_1, z_2, \ldots, z_k]$ defines the neighbouring line of point (x) with colour

$(f_1(x_1, x_2, , \ldots, x_k), f_2(x_1, x_2, \ldots, x_k), \ldots, f_k(x_1, x_2, \ldots, x_k)$.

Let us consider a tuple of symbolic colours $(g_1, g_2, \ldots, g_{2t}) \in K[z_1, z_2, \ldots, z_k]^k$ and the map F of PS to itself which sends the point (x) to the end v_{2t} of the chain v_0, v_1, $\ldots$, v_{2t}, where (x) $= \mathrm{v}_0$, $\mathrm{v}_i I \mathrm{v}_{i+1}$, $i = 0, 1, \ldots, 2t-1$ and $\rho(\mathrm{v}_j) = g_j(x_1, x_2, \ldots, x_k)$, $j = 1, 2, \ldots, 2t$. We refer to F as closed point to point computation with the symbolic key $(g_1, g_2, \ldots, g_{2t})$. As it follows from definitions $F = F_{g_1, g_2, \ldots, g_{2t}}$ is a multivariate map of $K^{k(k+1)}$ to itself. When symbolic key is given F can be computed in a standard form via elementary operations of addition and multiplication of the ring $K[x_1, x_2, \ldots, x_k, x_{11}, x_{12}, \ldots, x_{kk}]$. Recall that $(x_1, x_2, \ldots, x_k, x_{11}, x_{12}, \ldots, x_{kk})$ is our plaintext treated as symbolic point of the graph.

We refer for expression $F_{g_1, g_2, \ldots, g_{2t}}$ as automaton presentation of F with the symbolic key $g_1, g_2, \ldots, g_{2t}$. Notice that if g_{2t} is an element of affine Cremona group $C(K^k)$ then $F_{g_1, g_2, \ldots, g_{2t}} \in C(K^{k(k+1)})$ and automaton presentation of its inverse is $F_{g_{2t}^{-1} g_{2t-1}, {g_{2t}}^{-1} g_{2t-2}, \ldots, {g_{2t}}^{-1} g_1, {g_{2t}}^{-1}}$.

The restrictions on degrees and densities of multivariate maps g_i of K^k to K^k and size of parameter t allow to define a polynomial map F of polynomial degree and density.

Let us assume that $g_i = ({h_1}^i, {h_2}^i, \ldots, {h_k}^i)$, $i = 1, 2, \ldots, 2t$ is the symbolic key of the closed point to point computation $F = F(k)$ of the symbolic automaton $DS(k, K)$. We set that $g_0 = ({h_1}^0, {h_2}^0, \ldots, {h_k}^0) = (x_1, x_2, \ldots, x_k)$. We set that ${h_1}^0, {h_2}^0, \ldots, {h_k}^0) = (z_1, z_2, \ldots, z_k)$. Then F is a transformation of kind

$z_1 \to {h_1}^{2t}(z_1, z_2, \ldots, z_k)$, $z_2 \to {h_2}^{2t}(z_1, z_2, \ldots, z_k)$, $\ldots$, $z_k \to {h_k}^{2t}(z_1, z_2, \ldots, z_k))$

$z_{11} \to z_{11} - {h_1}^1 z_1 + {h_1}^1 {h_1}^2 - {h_1}^3 {h_1}^2 + {h_1}^3 {h_1}^4 + \cdots + {h_1}^{2t-1} {h_1}^{2t}$

$z_{12} \to z_{12} - {h_1}^1 z_2 + {h_1}^1 {h_2}^2 - {h_1}^3 {h_2}^2 + {h_1}^3 {h_1}^4 + \cdots + {h_2}^{2t-1} {h_1}^{2t}$

$\ldots$

$z_{kk} \to z_{kk} - {h_k}^1 z_k + {h_k}^1 {h_k}^2 - {h_k}^3 {h_k}^2 + {h_k}^3 {h_k}^4 + \cdots + {h_k}^{2t-1} {h_k}^{2t}$

LEMMA 1.

The degree of F is bounded by a maximum M of $\gamma_{r,s,i}(n) = \deg({h_r}^i) + \deg({h_s}^{i+1})$, $0 \le i \le 2t$, $1 \le r \le k$, $1 \le s \le k$. The density of F is at most *a maximum of* $d(r,s)$*, where* $d(r,s)-1$ *is the sum of parameters* $\mathrm{den}({h_r}^i) \times \mathrm{den}({h_s}^{i+1})$ *for* $i = 0, 1, \ldots, 2t$.

We say that closed point to point computation F is affine if all elements g_i of symbolic key are elements of degree ≤ 1 .

We refer to a subsemigroup G in $S(K^n)$ as semigroup of degree d if the maximal degree for representative g equals d.

Let $AGL_n(K)$ be the group of affine transformations of K^n, i. e. the group of all bijective transformations of degree 1.

Let us consider groups $E_k(K)$ which consists of all transformations $F_{h_1,h_2,\ldots,h_l,g}$ where $\mathrm{deg} h_i \leq 1$ for $i = 1, 2, \ldots, l$, l is an odd number and bijective map g is an element of $AGL_k(K)$. It is clear that $E_n(K)$ is a stable subgroup of degree 2.

REMARK. *Notice that conditions of lemma 1 allow to construct large cyclic groups of stable transformations of prescribed degree d. Such groups can be used in the multivariate El Gamal algorithm and its modifications.*

LEMMA 2. *Let* $K = F_q$ *and* F *be the map of closed point to point computation* $F_{h_1,h_2,\ldots,h_l,h}$ *and* h *is a Singer Cycle from* $GL_k(F_q)$*. Then the order of* F *is* $\geq q^k - 1$.

QUADRATIC MULTIVARIATE CRYPTOSYSTEM.

Let us consider the semigroup $G = E_k(F_q)$ and its embeddings μ_1 and μ_2 into semigroups $E_1 = E_n(F_{q^m})$ and $E_2 = E_n(F_{q^t})$, which are subgroups of Affine Cremona Semigroups G_1 and G_2 of vector spaces ${F_{q^m}}^n$ and ${F_{q^t}}^n$, where $n = k(k+1)$. Let ${\mu_1}'$ and ${\mu_2}'$ are natural embeddings of E_1 into G_1 and E_2 into G_2. We assume that η_i is a composition of μ_i and ${\mu_i}'$ for $i = 1, 2$. They are natural embeddings of G into G_1 and G_2. We can take internal automorphisms α and β of group G of kind $x \to g_i x g_i^{-1}$, $i = 1, 2$. We assume that $g = F$ satisfies to conditions of LEMMA 2 and $\mathrm{deg}(h_i) = 1$ for $i = 1, 2, \ldots, l$. Alice choses identical ϕ_3. Alice takes ϕ_i as maps of kind $x \to \tau_i h x h^{-1} \tau_i^{-1} h^{-1}$, $i = 1, 2$, where $h_i \in E_i$ and τ_i are bijective transformation of degree 1 from G_i. Alice may choose k_A such that $(k_A, q-1) = 1$.

Then maps G and G_A are quadratic maps of order $\geq q^k - 1$.

Let e_i, $i = 1, 2, \ldots, k$, $e_{s,j}$, $s = 1, 2, \ldots, k$, $j = 1, 2, \ldots, k$ are elements of standard basis of $K^{k(k+1)}$ in which all points and lines of $D(k,K)$ are presented.

Let us consider graph homomorphism δ of $DS(n, F_q)$ onto $DS(m, F_q)$ for $m < n$ of "deleting of coordinates of points and lines with indexes $i \geq m+1$ and (s,j) with $s > m+1$ or $j > m+1$ Let us consider elements $F = F_{h_1,h_2,\ldots,h_l,\tau}$ of $E_n(F_q)$ for which $h_1, h_2, \ldots, h_l$, τ preserve $< e_1, e_2, \ldots, e_m >$, as invariant subspace. They form semigroup G of $E_n(K)$. Let us denote via μ the homomorphism of G into $E_m(F_q)$ which sends F into computation F' of $E_m(F_q)$ with symbolic key given by restrictions of h_i, $i = 1, 2, \ldots, l$ and g onto subspace W. Let us assume that we have $g = F$ and g' such that $\mu(gg') = 1$ and the restriction of τ on W is a Singer cycle. We assume that α and β are internal automorphisms of G induced by conjugations with elements of G. Let μ_1 be the embedding of $E_m(F_q)$ into $E_m(F_{q^s})$, $s \geq 1$. We assume that η_1 is the composition of μ and μ_1 and η_2 is an embedding of $E_k(q)$ into $E_k(F_{q^t})$, $t \geq 1$. We take ϕ_3 as internal automorphizm of$E_m(F_q)$, ϕ_1 and ϕ_2 are internal automorphisms of Affine Cremona Semigroups induced by conjugations with elements from $E_m(F_{q^s})$ and $E_k(F_{q^t})$ and affine transformations corresponding vector spaces. Alice takes some positive integer k_A. Choosen data allows her to generate map $G \in E_k(F_{q^t})$ and invertible G_A. Both maps are quadratic stable transformations. The discrete logarithm problem in Affine Cremona Semigroup to solve equation $G^z = H$ for z is hard (semigroup generated by G contains more than $q^m - 1$ elements).

REMARK ON FURTHER INCREASE OF SECURITY.

In case of long usage of unchanged parameter k_A the adversary can find the quadratic inverse of G_A via linearisation attacks, but it is not yet a break of the cryptosystems, because of complexity of finding k_B. Notice that Alice always can change G_A for its conjugation with deformated stable element of affine group with degree d to make linearisation algorithm to invert map of degree $2d^2$ unfeasible. Alternatively one can use the following idea.

Let $g = g_l$ be the image of h under the canonical homomorphism μ of H into G_l. Notice that the order of g_l grows with increase of parameter l.

7 On generalised twisted discrete logarithm

Let S be a semigroup with subgroups A and B such that $[A.B] =< e >$. So $ab = ba$ for $a \in A$, $b \in B$.

Assume that Alice and Bob use the triple S, A, B and $g \in G$. So Alice takes her private key as positive integer k_A and group element $a \in A$. She forms $ag^{k_A}a^{-1}$ and sends it to Bob. In his turn Bob chooses k_B and $b \in B$ to create $bg^k_Bb^{-1}$ for Alice. Secondly Alice transforms received $bg^{k_B}b^{-1}$ into $abg^{k_B}k_Ab^{-1}a^{-1}$ and Bob forms the collision element as $bag^{k_A}k_Ba^{-1}b^{-1}$.

We refer to this key exchange algorithm as *generalised twisted Diffie Hellman protocol*.

Let us consider the following variant of desynchronised El Gamal algorithm with the triple S, A, B and homomorphism $\phi : S \to G$, where G is a group acting on the set M. Assume that Alice has knowledge on ϕ, but public user Bob knows only the restriction of ϕ on the group B

Alice takes pair g and g' such that $\phi(gg') = e$. She chooses parameters k_A and $a \in A$, $h \in A$ and sends $g_A = ag^{K_A}a^{-1}$ to Bob together with $g_1 = hg'h^{-1}$.

Bob takes $b \in B$ and computes $\phi(b) = b'$. He chooses parameter k_B and forms $b'{g_A}^{k_B}{b'}^{-1} = g_B$ and $b{g_1}^{k_B}b^{-1} = g_2$.

Finally he takes his plaintext $m \in M$ and forms ciphertext c $= g_B(m)$ and sends it to Alice together with g_2.

Alice computes $g_3 = ah^{-1}{g_2}^{k_A}ha^{-1}$ and its image $\delta = \phi(g_3)$ and computes plaintext as δ(c).

EXAMPLE 1.

Let us consider the vector space $V = {F_q}^{n+r}$ with the basis

$< e_1, e_2, \ldots, e_n, e_{n+1}, \ldots, e_{n+r} >$ and singular linear transformations g, such that it has an invariant subspace $W =< e_1, e_2, \ldots, e_n >$ and the restriction of g on W is the Singer cycle C' with the inverse C. So $CC' = e$ and orders of C and C' equal to q^{n-1}. Let G be a group of stable transformations of V of degree

d with invariant subspace W, $\tilde{b}$ is a restriction of $b \in G$ on W. Alice takes two elements a and $h = a^s$ from G and positive integer k_A. She takes the bijective affine transformation T of V for which W is not an invariant subspace together with affine bijections T_1 on W.

She chooses $a \in G$ and forms $g_A = T_1 \tilde{a^r} C^{k_A} \tilde{a}^{-r} {T_1}^{-1}$ and $g' = T\tilde{a^s} g \tilde{a^{-s}} T^{-1}$. So she sends these two transformations of degree $\leq d^2$ to Bob together with elements $b_1 = T_1 \tilde{a^r} {T_1}^{-1}$ and $b_2 = T a^r T^{-1}$.

So Bob writes plaintext p $= (p_1, p_2, \ldots, p_n)$, takes parameter k_B and s_B.

He computes the value of ${b_1}^{s_B} {g_A}^{K_B} {b_1}^{-s_B}$ in the point p as ciphertext c.

Additionally Bob computes ${b_2}^{s_B} {g'}^{k_B} {b_2}^{-s_B}$ and sends it to Alice together with the ciphertext c.

8 On the implemented twisted El Gamal multivariate cryptosystem

We implemented the following cryptosystem.

Alice takes the family of graphs $DS(n, F_q)$ and constant m. She uses canonical homomorphism μ of graph $DS(n, F_q)$ onto $DS(n-m, F_q)$ which sends point $(x_1, x_2, \ldots, x_n)$ to $(x_1, x_2, \ldots, x_{n-m})$ and line $[y_1, y_2, \ldots, y_n]$ to $[y_1, y_2, \ldots, y_{n-m}]$.

She chooses even parameter t and string A of linear maps L^1, L^2, $\ldots$, L^t of vector space ${F_q}^n$ to itself such that the subspace W spanned by $e_1, e_2, \ldots, e_{n-m}$ is invariant subspace for each L^i, $i = 1, 2, \ldots, t$ and the restriction of L_t on W is a Singer cycle. She takes a symbolic computation with symbolic key A and gets the polynomial map G. If L_{2t} is singular linear map then G is not a bijection. Notice that subspace U spanned by elements e_1, e_2, $\ldots$, e_{n-m}, e_{ij}, $i = 1, 2, \ldots, n-m$, $j = 1, 2, \ldots, n-m$ is an invariant subspace for G.

Similarly Alice uses graph $DS(n, F_q)$, symbolic key $L'^1, L'^2, \ldots, L'^t$ and constract the map G^1 such that the restriction of GG^1 on U is an identity map.

Secondly Alice takes other even parameter t_1 and string A_1 of linear maps M_1, M_2, $\ldots$, M_{t_1} such that W is invariant subspace for each M_i and the restriction of M_{t_1} on W is a Singer cycle. She takes a symbolic computation with A_1 as a key and forms map H of large order $(\geq q^n - 1)$ with invariant subspace U. Let G' and H' be restrictions of G and H on the vector space U.

Additionaly Alice uses symbolic automata corresponding to graphs $DS(n, F_q)$ and $DS(n-m, F_q)$ with strings B_1 and B_2 of linear maps of length t_3 and t_4 and forms transformation D_1 and D_2 of vector spaces $V_1 = {F_q}^{n(n+1)}$ and $V_2 = {F_q}^{(n-m)(n-m+1)}$. She takes also bijective affine maps τ_1 and τ_2 on V_1 and V_2.

Finally Alice takes triple of positive integer parameters k_A, r_A and r from open interval $(1, q^n - 1)$. She form the following maps in their standard forms G_A which is the composition of τ_2, D_2, H'^{r_A}, $6'^{r_A}$, H'^{-r_A}, ${D_2}^{-1}$, ${\tau_2}^{-1}$. Notice that G_A is a bijective transformation of U. Alice computes G_1 as $\tau_1 D_1 H^r G^1 H^{-r} {D_1}^{-1} {\tau_1}^{-1}$.

She sends standard forms of G_A and G_1 to Bob together with $H_2 = \tau_2 D_2 H' {D_2}^{-1} {\tau_2}^{-1}$ and $H^1 = \tau_1 D_1 H {D_1}^{-1} {\tau_1}^{-1}$ and $G_2 = \tau_1 D_1 H^r G^1 H^{-r} {D_1}^{-1} {\tau_1}^{-1}$.

Bob chooses parameters k_B and r_B. He writes plaintext p $\in U$. Computes $H^{1^{r_B}} G_A H^{1^{-r_B}}$ and applies it k_B times to the plaintext. Bob sends resulting vector as ciphertext to Alice together with $G_3 = H_1^{r_B} {G_2}^{k_B} H_1^{-r_B}$. Alice is able to decrypt according to described above general algorithm. So she transforms $G_3 = \tau_1 D_1 H^{r+r_B} {G^1}^{k_B} H^{-r-r_B} {D_1}^{-1} {\tau_1}^{-1}$ to $G_4 = H^{r_B} {G^1}^{k_B} H^{-r_B}$, computes $\mu(G_4)$ and $G_5 = H'^{r_A} \mu(G_4)^{k_A} H'^{-r_A}$. Alice applies $G_5 = \tau_2 D_2 G_4 {D_2}^{-1} {\tau_2}^{-1}$ to the ciphertext and reads the plaintext p.

REMARK. *All maps G_A, G_1, H_1, H_2 and G_3 are quadratic transformations.*

9 On cubical multivariate El Gamal type cryptosystem with hidden decomposition of group element

EXAMPLE 2. Let K be a commutative ring. We define $A(n, K)$ as bipartite graph with the point set $P = K^n$ and line set $L = K^n$ (two copies of a Cartesian power of K are used).

We will use brackets and parenthesis to distinguish tuples from P and L. So (p) $= (p_1, p_2, \ldots, p_n) \in P_n$ and [l] $= l_1, l_2, \ldots, l_n) \in L_n$. The incidence relation $I = A(n, K)$ (or corresponding bipartite graph I) is given by condition pIl if and only if the equations of the following kind hold.

$p_2 - l_2 = l_1 p_1$
$p_3 - l_3 = p_1 l_2$
$p_4 - l_4 = l_1 p_3$
$p_5 - l_5 = p_1 l_4$
$\ldots$
$p_n - l_n = p_1 l_{n-1}$ for odd n
$p_n - l_n = l_1 p_{n-1}$ for even n

Let us consider the case of finite commutative ring K, $|K| = m$.

As it instantly follows from definition the order of our bipartite graph $A(n, K)$ is $2m^n$. The graph is m-regular. Really, the neighbour of given point p is given by above equations, where parameters $p_1, p_2, \ldots, p_n$ are fixed elements of the ring and symbols $l_1, l_2, \ldots, l_n$ are variables. It is easy to see that the value for l_1 could be freely chosen. This choice uniformly establishes values for $l_2, l_3 \ldots, l_n$. So each point has precisely m neighbours. In similar way we observe the neighbourhood of the line, which also contains m neighbours. We introduce the colour ρ(p) of the point p and the colour ρ(l) of line l as parameter p_1 and l_1 respectively. Graphs $A(n, K)$ with colouring ρ belong to class of linguistic graphs defined in [14]. In the case of linguistic graph Γ the path consisting of its vertices v_0, v_1, v_2, $\ldots$, v_k is uniquely defined by initial vertex v_0 and colours $\rho(v_i)$, $i = 1, 2, \ldots, k$ of other vertices from the path.

So the following symbolic computation can be defined. Take the symbolic point x $= (x_1, x_2, \ldots, x_n)$ where x_i are variables and symbolic key which is a string of polynomials $f_1(x)$, $f_2(x)$, $\ldots$, $f_s(x)$ from $K[x]$. Form the path of vertices $v_0 =$ x, v_1 such that $v_0 I v_1$ and $\rho(v_1) = f_1(x_1)$, v_2 such that $v_1 I v_2$ and $\rho(v_2) = f_2(x_1)$, $\ldots$, v_s such that $v_{s-1} I v_s$ and $\rho(v_s) = f_s(x_1)$. We use term *symbolic point to point computation* in the case of even k and talk on *symbolic point to* *line* computation in the case of odd k. We notice that the computation of each coordinate of v_i via variables $x_1, x_2, \ldots, x_n$ and polynomials $f_1(x)$, $f_2(x)$, $\ldots$, $f_i(x)$ needs only arithmetical operations of addition and multiplication. Final vertex v_s (point or line) has coordinates $(h_1(x_1), h_2(x_1, x_2), h_3(x_1, x_2, x_3), \ldots, h_n(x_1, x_2, \ldots, x_n))$, where $h_1(x_1) = f_s(x_1)$.

Assume that the equation of kind $f_s(x) = b$ has exactly one solution. Then the map $H : x_i \to h(x_1, x_2, \ldots, x_i)$, $i = 1, 2, \ldots, n$ is a bijective map.

In the case of finite parameter s and finite densities of $f_i(x)$, $i = 1, 2, \ldots, s$ the map H also have finite density. If all parameters $\deg(f_i(x))$ are finite then the map H has a linear degree in variable n. Let consider the totality $G(n, K)$ of point to point computations with the symbolic key of kind $f_i(x) = x + a_i$, $i = 1, 2, \ldots, s$, where parameter s is even. We can prove that $G(n, K)$ is a stable group of degree 3.

We have a natural homomorphism $G(n+1, K)$ onto $G(n, K)$ induced by the homomorphism δ from $A(n+1, K)$ onto $A(n, K)$ sending point $(x_1, x_2, \ldots, x_n, x_{n+1})$ to $(x_1, x_2, \ldots, x_n)$ and line $[x_1, x_2, \ldots, x_n, x_{n+1}]$ to $[x_1, x_2, \ldots, x_n]$. It means that there is a well defined projective limit $A(K)$ of graphs $A(n, K)$ when $n \to \infty$. Let $\delta_{n,t}$, $n > t$ be a canonical homomorphism of $A(n, K)$ onto $A(t, K)$ corresponding to procedure of deleting of coordinates withindexes $t+1, t+2, \ldots, n$. This map defines the canonical homomorphism $\eta(n, t)$ of group $G(n, K)$ onto $G(t, K)$.

Alice takes the sequence of transformations $g_n \in G(n, K)$ of increasing order with the grows of n. The existence of such sequences is stated in [20]. together with several other sequences of elements u_1, u_2, $\ldots$, u_r from the group $G(n, K)$. Alice can easily generate ${g_n}^{-1}$, and ${u_i}^{-1}$, $i = 1, 2, \ldots, r$. She takes $l = n-t$, where t is some constants and computes values w_i and ${w_i}^{-1}$ of $\eta(n, l)$ from (u^i) and ${u_i}^{-1}$. Alice will use affine transformations τ_1 and τ_2 of free modules K^n and K^l. She takes positive integer k_A and prepares the following data for public user Bob. She computes $g_A = \tau_2\eta(n, l)((g_n))^{k_A}{\tau_2}^{-1}$ and $d_i = \tau_2 w_i {\tau_2}^{-1}$, $i = 1, 2, \ldots, r$. Alice creates $g' = \tau_1({g_n}^{-1}){\tau_1}^{-1}$ and $v_i = \tau_1(u_i){\tau_1}^{-1}$, $i = 1, 2, \ldots, r$. Bob gets d_i and v_i together with their inverses.

ALGORITHM.

Bob writes plaintext p $= (p_1, p_2, \ldots, p_l)$ and selects positive parameter k_B, string $j_1, j_2, \ldots, j_s$ such that $j_k \in \{1, 2, \ldots, r\}$ and j_k differs from j_{k-1} and j_{k+1}. He takes integer parameter α_1, α_2, $\ldots$, α_s and form element $b = d_{j_1}^{\alpha_1} d_{j_2}^{\alpha_2} \ldots d_{j_s}^{\alpha_s}$ together with b^{-1}. Bob computes bg_Ab^{-1} and applies it k_B times to p, Resulting tuple c $= (c_1, c_2, \ldots, c_l)$ is the ciphertext. Additionally Bob computes $v = v_{j_1}^{\alpha_1} v_{j_2}^{\alpha_2} \ldots v_{j_s}^{\alpha_s}$ and sends to Alice element $g_B = v{g'}^{k_B}v^{-1}$ together with the ciphertext c.

Decryption process is the following. Alice computes $g_1 = {\tau_1}^{-1}g_B\tau_1$. She gets $g_2 = \eta(n, l)(g_1)$ and $g_3 = {g_3}^{k_A}$. Alice applies $g_4 = \tau_2 g_3 {\tau_2}^{-1}$ to the ciphertext. Result of this application is the plaintext.

REMARK. The adversary has to find parameter k_A via studies of g_A and g' from different transformation groups. Additionally he has to compute the value on g_B of partially defined homomorphism δ from the subgroup of $C(K^n)$ generated by v_1, v_2, $\ldots$, v_r, g' onto subgroup of $C(K^m)$ generated by d_1, d_2,

..., d_r and g_A which sends u_i to w_i, $i = 1, 2, \ldots, r$. Adversary can try to find decomposition of g_B into generators v_i and g' of special " central" form $a{g'}^k a^{-1}$, $a \in < v_1, v_2, \ldots, v_k >$. After that adversary can compute $\delta(a)$ and study options of $\delta(g') = (g_A)^t$ with various parameters t.

1. J. Ding, J. E. Gower, D. S. Schmidt, *Multivariate Public Key Cryptosystems.* Springer, Advances in Information Security, V. 25, 2006.
2. A. Cossidente, M. J. de Ressmine, *Remarks on Singer Cycle Groups and Their Normalizers, Designs, Codes and Cryptography*, 32, 97-102, 2004.
3. W. Kantor, *Linear groups containing a Singer cycle*, J. of Algebra 62, 1982, 232-234.
4. L. Babai, *Graph Isomorphism in Quasipolinomial Time*, arXive: 1512 03547v1 [cs. DS], 11 Dec 2015.
5. A. Kipnis, A. Shamir, *Cryptanalisis of the Oil and Vinegar Signature Scheme*, Advances in Cryptology - Crypto 96, Lecture Notes in Computer Science, V. 1462, 1996, P. 257–266.
6. Jacques Patarin, Louis Goubin, *Trapdoor one-way permutations and multivariate polynominals*, ICICS 1997, 356-368.
7. Jacques Patarin, Louis Goubin, *Asymmetric cryptography with S-Boxes*, ICICS 1997, 369-380.
8. Jacques Patarin, *Asymmetric Cryptography with a Hidden Monomial*, CRYPTO 1996: 45-60.
9. Louis Goubin, Jacques Patarin, Bo-Yin Yang, *Multivariate Cryptography. Encyclopedia of Cryptography and Security*, (2nd Ed.) 2011, 824-828.
10. J. Porras, J. Baena, J. Ding *New Candidates for Multivariate Trapdoor Functions*, Revista Colombiana de Matematicas 49(1):57-76 (November 2015).
11. V. A. Ustimenko, *Explicit constructions of extremal graphs and new multivariate cryptosystems*, Studia Scientiarum Mathematicarum Hungarica, Special issue "Proceedings of The Central European Conference, 2014, Budapest", volume 52, issue, June 2015, pp. 185-204.
12. V. Ustimenko, *On Multivariate Cryptosystems Based on Computable Maps with Invertible Decompositions*, Annales of UMCS. Informatica. V. 14. 2014 (Special issue "Proceedings of International Conference Cryptography and Security Systems). P. 7-18.
13. V. Ustimenko, *On Shubert cells in grassmanians and new algorithm of multivariatecryptography*, Proceedings of Institute of Mathematics, Minsk, 2015, pp 137-148.
14. V. Ustimenko, *Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography*, Journal of Mathematical Sciences, Springer, vol.140, N3 (2007) pp. 412-434.
15. V. Ustimenko, A. Wroblewska, *On the key exchange with nonlinear polynomial maps of stable degree*, Annalles UMCS Informatica AI XI, 2 (2011), 81-93.
16. A. Wroblewska, *On some properties of graph based public keys*, Albanian Journal of Mathematics, Volume 2, Number 3, 2008, 229-234, NATO Advanced Studies Institute: "New challenges in digital communications".
17. V. Ustimenko, *Coordinatisation of Trees and their Quotients*, In the "Voronoj's Impact on Modern Science", Kiev, Institute of Mathematics, 1998, vol. 2, 125-152.
18. V. Ustimenko, F. Lazebnik, *Some Algebraic Constractions of Dense Graphs of Large Girth and of Large Size*, DIMACS series in Discrete Mathematics and Theoretical Computer Science , v. 10, (1993) 75 - 93.
19. F. Lazebnik, V. A. Ustimenko and A. J. Woldar, *New Series of Dense Graphs of High Girth*, Bull (New Series) of AMS, v.32, N1, (1995), 73-79.

20. V 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, Vol. 427, Springer, January , 2013, 257-285.
21. V. Ustimenko, A. Wroblewska,*Dynamical systems as the main instrument for the constructions of new quadratic families and their usage in cryptography*, Annales UMCS Informatica AI, ISSN 1732-1360, vol.12, N3 (2012), 65-74.
22. M. Klisowski, *Zwikszenie bezpieczestwa kryptograficznych algorytmw wielu zmiennych bazujcych na algebraicznej teorii grafw*, PhD thesis, Czstochowa, 2014.
23. V. Ustimenko, M. Klisowski, *Graph based cubical multivariate maps and their cryptographical applications*, in Advances on Superelliptic curves and their Applications, IOS Press, NATO Science for Peace and Security series D: Information and Communication Security, vol 41, 2015 , pp. 305 -327.
24. V. Ustimenko, A. Wroblewska. *On new examples of families of multivariate stable maps and their cryptographical applications*. Annales UMCS, Informatica, 14(1):1935, 2014.
25. V. Ustimenko, A. Woldar, *A geometric approach to orbital recognition in Chevalley-type coherent configurations and association schemes*, Australasian Journal of Combinatorics, Volume 67(2) (2017), Pages 166-202.