UDC 001.8

On the cryptosystems based on two Eulerian transformations defined over the commutative rings Z2s, s>1

Vasyl Ustimenko[1,2]

[1] *Royal Holloway University of London, United Kingdom.*
[2] *Institute of telecommunications and global information space, Kyiv, Ukraine*

E - mail: Vasyl.Ustymenko@rhul.ac.uk

Abstract

We suggest the family of ciphers ${}^sE_n$, $n=2,3,....$ with the space of plaintexts $(Z^*{}_2{}^s)^n$, $s>1$ such that the encryption map is the composition of kind $G=G_1A_1G_2A_2$ where A_i are the affine transformations from $AGL_n(Z_2{}^s)$ preserving the variety $(Z^*{}_2{}^s)^n$.

Eulerian endomorphism G_i , $i=1,2$ of $K[x_1, x_2,...., x_n]$ moves x_i to monomial term $\mu x_1{}^{d(1)}x_2{}^{d(2)}...x_n{}^{d(n)}$, $\mu \epsilon Z^*{}_2{}^s$ and act on $(Z^*{}_2{}^s)^n$ as bijective transformations.

The cipher is converted to a protocol supported cryptosystem. Protocols of Noncommutative Cryptography implemented on the platform of Eulerian endomorphism are used for the delivery of G_i and A_i from Alice to Bob. One can use twisted Diffie Hellman protocols which security rests on the complexity of Conjugacy Power problem or hidden tame homomorphism protocol which security rests of the word decomposition problem. Instead of delivery of G_i Alice and Bob can elaborate these transformations via the inverse twisted Diffie-Hellman protocol implemented on the platform of tame Eulerian transformations of $(Z^*{}_2{}^s)^n$. The cost of single protocol is $O(n^3)$ and the cost of the computation of the reimage of used nonlinear map is $O(n^2)$. So the verification of n^t , $t\geq 1$ signatures takes time $O(n^{t+2})$. Instead of inverse twisted Diffie-Hellman protocol correspondents can use inverse hidden tame homomorphism protocol which rests on the complexity of word decomposition for tame Eulerian transformations. We use natural bijections between $Z^*{}_2{}^s$ and $Z_2{}^{s-1}$, $Z^*{}_2{}^s$ and finite field $F_2{}^{s-1}$ and $Z^*{}_2{}^s$ and Boolean ring B_{s-1} of order 2^{s-1} to modify the family of ciphers or cryptosystems via the change of $AGL_n(Z_2{}^s)$ for the $AGL_n(K)$, where K is one of the rings $Z_2{}^{s-1}$, $F_2{}^{s-1}$ and B_{s-1}. New ciphers are defined via the multiplications of two different commutative rings $Z_2{}^s$ and K. It does not allow to treat them as stream ciphers of multivariate cryptography and use corresponding cryptanalytic technique.

Adversary is not able to use known cryptanalytical methods such as linearisation attacks. We discuss the option of change in the mentioned above elements of $AGL_n(Z_2{}^s)$ or $AGL_n(K)$ for nonlinear multivariate transformation F of $(Z_2{}^s)^n$ or K^n with the symmetric trapdoor accelerator T, i.e. the piece of information such that the knowledge of T allows to compute the value $F(p)$ in arbitrarily chosen $p \epsilon P$ in time $O(n^2)$ and to solve the equation of kind $F(x)=c$ for each c from C in time $O(n^2)$.

Keywords: Symmetric stream ciphers, Digital signatures, Protocol based cryptosystems, Noncommutative Cryptography, Eulerian transformations

Introduction

Quadratic multivariate public keys of Post-Quantum Cryptography can provide ‘’short’’ digital signatures for which the procedure of the verification of signature has complexity $O(n^3)$ where n is the length of hash file of the documents.

There is no a certified standard algorithm from these class. Well known Unbalance Rainbow like Oil and Vinegar algorithm was one of the candidates for NIST standardization but finally was rejected due to cryptanalytic results (see [1], [2] and further references). The research on the construction of new quadratic multivariate public keys and their cryptanalytic investigation is continued [5]- [25].

This paper is dedicated to alternative approach to construct new instruments for digital signatures. We suggest several new protocol based cryptosystems which security rest on the complexity of hard problems of Noncommutative Cryptography (see [3] and further references). The complexity of used protocol is $O(n^3)$. After the execution of $O(1)$ protocols correspondents can use obtained digital signatures scheme as many times as they want. The cost of single signature is $O(n^2)$ where n is the length of the hash file of the document.The complexity of the verification of the signatures of $O(n^t)$ documents is $O(n^{t+2})$.

Section 1 contains some definitions of Multivariate Cryptography and Algebraic Geometry. It contains also descriptions of the semigroup of Eulerian transformations of $K[x_1, x_2,\dots, x_n]$ where K is a commutative ring acting naturally on the variety $\boldsymbol{(K^*)^n}$**.** Some bijective transformations of $\boldsymbol{(K^*)}^n$ induced by Eulerian maps are also presented**.** Some basic protocols of Noncommutative Cryptography are given there, These protocols can be implemented of the platforms of Eulerian transformations.

Section 2 contains the description of ciphers and protocol based cryptosystems which used the compositions of kind E_1AE_2 where E_i , $i=1,2$ are Eulerian endomorphisms of $Z_2^s[x_1, x_1,\dots, x_n]$ and A is the special element of $AGL_n(Z_2^s)$ which preserves the variety $(Z^*{}_2^s)^n$.

In the Section 3 we use fast computable natural bijection between $Z^*{}_2^s$ and one of the ring $K= Z_2^{s-1}$, $K=F_2^{s-1}$ and $K=B_{s-1}$ which is the Boolean ring of order 2^{s-1} **.** We also discuss the idea of change transformation A of degree for nonlinear map F with the trapdoor accelerator which is a piece of information sufficient for the computation of the reimage of F in time $O(n^2)$. Last section is the conclusion.

1. On the algorithms of Noncommutative Cryptography implemented on the platforms of multivariate transformations

1.1. Some definitions

Classical multivariate public rule is a transformation of $\boldsymbol{n}$-dimensional vector space over finite field $\boldsymbol{F_q}$ which move vector $(x_1, x_2, \dots , x_n)$ to the tuple $(g_1(x_1, x_2, \dots , x_n), g_2(x_1, x_2, \dots, x_n), \dots, g_n(x_1, x_2, \dots, x_n))$, where polynomials g_i are given in their standard forms, i.e. lists of monomial terms in the lexicographical order.

The degree of this transformation is the maximal value of $deg(g_i)$. Traditionally public rule has degree 2 or 3. Degree 2 is preferable (RUOV algorithm claimed to provide ‘’the shortest digital signatures’’). Let us consider the following important object of Noncommutative Cryptography. Affine Cremona Semigroup ${}^nCS(K)$ is defined as endomorphism group of polynomial ring $K[x_1, x_2,\dots, x_n]$ over the commutative ring K. It is an important object of Algebraic Geometry (see [4] about mathematics of Luigi Cremona - prominent figure in Algebraic Geometry in XIX). Element of the semigroup $\boldsymbol{\sigma}$ can be given via its values on variables, i. e. as the rule $x_i\rightarrow f_i(x_1, x_2, \dots, x_n)$, $i=1, 2,\dots, n$. This rule induces the map σ': $(a_1, a_2,.., a_n)\rightarrow(f_1(a_1, a_2,.., a_n), f_2(x_1, x_2, \dots, x_n),\dots, f_n(x_1, x_2,\dots, x_n))$ on the free module K^n.

Automorphisms of $K[x_1, x_2,\dots, x_n]$ form *affine Cremona Group* ${}^nCG(K)$. In the case when K is a finite field or arithmetic ring Z_m of residues modulo m elements of affine Cremona Groups or Semigroups are used in algorithms of Multivariate Cryptography. Results about subsemigroups S of ${}^nCS(K)$ (or subgroups of ${}^nCG(K)$ such that computation of the superposition of arbitrary $\boldsymbol{n}$ elements can be completed for polynomial time can be used as so called platforms of Noncommutative Cryptography. One class of such objects is formed by stable subsemigroups of degree k, i. e. subsemigroup $\boldsymbol{S}$ such that the maximal degree of its representative is bounded by the constant k.

We will talk about Multiple Composition Computability (*MCC*) property. In the case of $k=1$ one can take $AGL_n(K)$, stable subsemigroups of degree k in ${}^nCG(K)$ exist for each k, $k=2, 3,\dots$. *Affine Cremona semigroup* ${}^nCS(K)$ does not poses MCC. If one takes $\boldsymbol{n}$ quadratic elements is randomly their product with the probability close to 1 will have degree 2^n. So the computation is not feasible.

EXAMPLE 1. Let us consider the totality ${}^{n}ES(K)$ of endomorphisms of $K[x_1, x_2,..., x_n]$ of kind

$$x_1 \to \mu_1 x_1^{a(1,1)} x_2^{a(1,2)} \dots x_n^{a(1,n)},$$
$$x_2 \to \mu_2 x_1^{a(2,1)} x_2^{a(2,2)} \dots x_n^{a(2,n)}, \quad (1)$$
$$\dots$$
$$x_m \to \mu_n x_1^{a(n,1)} x_2^{a(n,2)} \dots x_n^{a(n,n)}$$

where μ_i are regular elements of finite commutative ring K with the unity.

It is easy to see that the complexity of the composition of two elements of kind (1) is $O(n^3)$.

So the subsemigroup of Eulerian transformations ${}^{n}ES(K)$ poses MCC property**.**Semigroups with MCC property can serve as ‘’platforms’’ for protocols of Noncommutative Cryptography.

1.2. Twisted Diffie-Hellman protocol

Let S be an abstract semigroup which has some invertible elements.Alice and Bob share element $g\epsilon S$ and pair of invertible elements h, h^{-1} from this semigroup. Alice takes positive integers $k(A)$ and $r(A)$ and forms $h^{dr(A)}g^{k(A)}h^{r(A)}= g_A$. Bob takes $k(B)$ and $r(B)$ and forms $h^{-r(B)}g^{k(B)}h^{r(B)}= g_B$. They exchange g_A and g_B and compute collision element X as ${}^{A}g= h^{-r(A)}g_B^{k(A)}h^{r(A)}$ (Alice) and ${}^{B}g= h^{-r(B)}g_A^{k(B)}h^{r(B)}$ (Bob) respectively.

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

1.3. Inverse twisted Diffie-Hellman protocol

Let S be an abstract noncommutative semigroup which has some invertible elements. Alice and Bob share element $g\epsilon S$ and pair of invertible elements h, h^{-1} from this semigroup. Alice knows g^{-1}. Alice takes positive integers $k(A)$ and $d=r(A)$ and forms $h^{-r(A)}g^{-k(A)}h^{r(A)}= g_A$. Bob takes $k(B)$ and $r(B)$ and forms $h^{-r(B)}g^{k(B)}h^{r(B)}= g_B$.

They exchange g_A and g_B and Alice computes $X= h^{-r(A)}(g_B)^{k(A)}\ h^{r(A)}$. Bob computes $Y = h^{-r(B)}(g_A)^{k(B)}\ h^{r(B)}$ (Alice) and ${}^{B}g= h^{-p}g_A^{s}h^{p}$ respectively. It is clear that $Y=X^{-1}$

The security of the scheme rest on the Conjugation Power Problem, adversary has to solve the problem $h^{-x}g^{y}h^{x}= b$.

The complexity of the problem depends heavily on the choice of highly noncommutative platform ***S***. Let us take platform $S={}^{n}ES(K)$.

REMARK. Protocols with the security based on the word decomposition problem, i. e. task to decompose $g\ \epsilon S$ into the word in given generators g_1, g_2, ..., g_t, $t >1$ were presented during my previous talk.

1.4. On some bijective transformation of (K*)n

Let π and δ be two permutations on the set $\{1,2,..., n\}$. Let K be a commutative ring with unity which has nontrivial multiplicative group K^* of order $d =|K^*|>1$ and $n\geq 1$. We define transformation ${}^{A}JG(\pi, \delta)$ of the variety $(K^*)^n$, where A is triangular matrix with positive integer entries $0\leq a(i,j)\leq d$, $i\geq d$ defined by the following closed formula.

$$y_{\pi(1)=\mu 1}x_{\delta(1)}^{a(1,1)}$$
$$y_{\pi(2)=\mu 2}x_{\delta(1)}^{a(2,1)}\ x_{\delta(2)}^{a(2,2)}$$
$$\dots$$
$$y_{\pi(n)=\mu n}x_{\delta(1)}^{a(n,1)}\ x_{\delta(2)}^{a(n,2)} \dots x_{\delta(n)}^{a(n,n)}$$

where $(a(1,1),d)=1$, $(a(2,2),d)=1,\dots,(a(n,n),d)=1$.

We refer to ${}^{A}JG(\pi, \delta)$ as Jordan transformations Gauss multiplicative transformation or simply JG element. It is an invertible element of ${}^{n}ES(K)$ with the inverse of kind ${}^{B}JG(\delta, \pi)$ such that $a(i,i)b(i,i)=1 \pmod d$. Notice that in the case $K= Z_m$ straightforward process of computation the inverse of JG element is connected with the factorization problem of integer m. If $n=1$ and m is a product of two large primes p and q the complexity of the problem is used in RSA public key algorithm. The idea to use composition of JG elements or their generalisations with injective maps *of* K^n into K^n was used in [27] ($K=Z_m$) and [26] ($K= F_q$.).

We say that τ is *tame Eulerian element* over the commutative ring K if it is a composition of several Jordan Gauss multiplicative maps over commutative ring or field respectively. It is clear that τ sends variable x_i to a certain monomial term. The decomposition of τ into product of Jordan Gauss transformation allows us to find the solution of equations $\tau(x)=b$ for x from $(Z^*_m)^n$ or $(F*_q)$ ^{m}. So tame Eulerian transformations over Z_m or $F_{q.}$ are special elements of $^nEG(Z_m)$ or $^nEG(F_q)$ respectively.

We refer to elements of $^nES(K)$ as multiplicative Cremona element. Assume that the order of K is constant. As it follows from definition the computation of the value of element from $^nES(K)$ on the given element of K^n is estimated by $O(n^2)$. The product of two multiplicative Cremona elements can be computed in time $O(n^3)$.

We are not discussing here the complexity of computing the inverse for general element g϶ nEG(K) on Turing machine or Quantum computer and problem finding the inverse for tame Eulerian elements.

2. Some ciphers and cryptosystems based on Eulerian transformations over the Z2s

The main idea of constructions of this section is based on the fact that the composition of the general element A of $AGL_n(K)$ and the general element G of $^nEG(K)$ has nonpolynomial density. We can change element A for the general element F of $CG_n(K)$. In the case of $K=Z_2^s$, s>1 we can slightly modify F of kind

$x_i \rightarrow f_i(x_1, x_2,..., x_n)$ and get the bijective transformation $*F$ of the variety $(Z*_2^s)^n$ via the following procedure.

We set the vector $b=(b_1, b_2,...., b_n)$ where $b_i=1$ if $f_i(1, 1, ..., 1)$ *mod* $2=0$ and $b_i=0$ if $f_i(1, 1, ..., 1)$ *mod* $2=1$ and form $*F$ as transformation of $(Z*_2^s)^n$ of kind $x\rightarrow F(x)+b$. It is easy to see that $*F$ is a bijection.

Scheme 1.

If F has a polynomial density or F has a symmetric trapdoor accelerator $\boldsymbol{T}$ then computation of $F(1, 1,...,1)$ can be completed in polynomial time.

Assume that $\boldsymbol{G}$ from $CG_n(K)$ is formed as the composition of $k=O(1)$ Jordan-Gauss transformations $J_1, J_2,..., J_k$ Alice and Bob share the information on $\boldsymbol{T}$ and the decomposition of G into J_i, $i=1,2,..., k$.

They work with the space of plaintext $(Z*_2^s)^n$ and use encryption procedure $x \rightarrow F*(x)=v$, $v\rightarrow G(v)=y$.

The cost of the encryption/decryption procedure is $O(n^2)$.

*Attacks of adversary with interception of multiple pairs of kind plaintext/corresponding ciphertext are unfeasible because of the nonpolynomial density of G(*F)*

We can obfuscate these scheme without theoretical change of encryption procedure via the use of two Eulerian transformations.

Symmetric cipher. Alice and Bob share two tame Eulerian transformations G_1 and G_2 given with their decompositions via Jordan-Gauss generators. They also have invertible affine transformation L from $AGL_n(Z_2^s)$**.** Alice and Bob use (F, T) , they can compute the value of $*F$ in time $O(n^2)$.

They compute inverses $(G_1)^{-1}$ and $(G_2)^{-1}$ of the Eulerian transformations and the matrix L^{-1}. They work with the space of plaintexts $(Z*_2^s)^n$**.**

Encryption procedure has the followings steps.

S1. The transformation of the plaintext $(p_1, p_2,...., p_n)=p$ to the $^1p=G_1(p)=(^1p_1, ^1p_2,...., ^1p_n)$.

S2. The computation of $*F(^1p)= ^2p$.

S3. The computation of $^3p = G_2(^2p)$.

S4. The computation of the ciphertext c as $*L(^3p)$.

Decryption is a consecutive application of operators $*L^{-1}(c)=(^3p)$, $(G_2)^{-1}(^3p)=^2p$, $*F^{-1}(^2p)=^1p$ and the plaintext $p=(^1G)^{-1}(^1p)$**.**

Each procedure Si, $i=1,2, 3,4$ and its inverse have the complexity $O(n^2)$. So we have a symmetric cipher with the complexity $O(n^2)$. We refer to it in the simplest case of $*F϶AGL_n(Z_2^s)$ as Double Eulerian Cipher (*DEC*).

REMARK 1. The encryption map is induced by multivariate transformation E of $(Z_2^s)^n$. It has a linear degree of kind ***an, a>0*** and nonpolynomial density which is the total number of monomial terms in all $\boldsymbol{F(x_i)}$**.** So linearization attacks on this cipher are unfeasible.

Let us convert the Double Eulerian Cipher to the protocol based cryptosystems.

The following definition can be useful.

Let E be a function from the set P onto the set C. We say that the piece of information T is a symmetric trapdoor accelerator if the knowledge of T allows to compute the value $F(p)$ in arbitrarily chosen p ϵ P in time $O(n^2)$ and to solve the equation of kind $F(x)=c$ for each c from C in time $O(n^2)$.

For the encryption map E of the defined above cipher the decomposition of E into he composition of G_1, $*F$, G_2 L and together with the decomposition of each G_i into the product of $O(1)$ Jordan-Gauss transformation.

CRYPTOSYSTEM DEC1. Let us assume that Alice and Bob execute the twisted Diffie-Hellman protocol based on the platform ${}^{n}ES(Z_2^{s})$ two times. They elaborate elements H_i, $i=1,2$ from this semigroup.

Additionally they conduct two sessions the twisted Diffie Hellman protocol based on platform ${}^{n+1}ES(Z_2^{s+1})$ and elaborate the elements ${}^{r}H$, $r=1.2$ from this semigroup.

Alice forms elements G_j, $j=1, 2$ as a products of $O(1)$ Jordan-Gauss elements. She computes and keeps $(G_j)^{-1}$**.**

Assume that H_i are maps of kind (1) with $(\mu_1, \mu_2,\dots, \mu_n)=(\mu_1(i), \mu_2(i),\dots, \mu_n(i))$ and $a(j,k)=a_i(j, k)$ and maps G_i are elements of kind (1) with $(\mu_1, \mu_2,\dots, \mu_n)=(\alpha_1(i), \alpha_2(i), \dots, \alpha_n(i))$ and $a(j,k)=b_i(j, k) \bmod 2^{s-1}$.

Assume that ${}^{r}H$, $r=1, 2$ is element of kind (1) with $(\mu_1, \mu_2,\dots, \mu_n)=({}^{r}\alpha_1, {}^{r}\alpha_2, \dots, {}^{r}\alpha_n)$ and $a(i, k)={}^{r}b(j, k) \bmod 2^{s}$. Let ${}^{r}B=({}^{r}b(i,j))$.

Alice sends parameters $\mu_j(i)\alpha_j(i)$, $j=1, 2, \dots, n$, $i=1,2$ and $a_i(j, k) +_i b_i(j, k) \bmod 2^{s-1}$, $j=1,2,\dots,n$, $k=1,2,\dots,n$, $i=1,2$.

So Bob restores G_1 and G_2**.**

Alice creates invertible matrices M and N with entries from Z_2^{s} . She sends $M+{}^{1}B$ and $N+{}^{2}B$ to Bob. So he restores the matrices M and N.

Finally Alice selects the tuples $(d_1, d_2,\dots, d_n)$ and $(t_1, t_2,\dots, t_n)$ from $(Z_2^{s})^{n}$. She takes $({}^{r}\alpha_1, {}^{r}\alpha_2,\dots, {}^{r}\alpha_n)$ of elements from $Z^*{}_2^{s+1}$.

Alice considers the map $\sigma_s=\sigma$ from Z_2^{s} to $Z^*{}_2^{s+1}$ such that $\sigma(t \bmod 2^{s})$ is $2t+1 \bmod 2^{s+1}$. It is a bijection**.** Let σ^{-1} be the inverse map from $Z^*{}_2^{s+1}$ to Z_2^{s}**.** She forms

$(\sigma^{-1}({}^{1}\alpha_1)+d_1 \bmod 2^{s}, \sigma^{-1}({}^{1}\alpha_2)+d_2 \bmod 2^{s}, \dots, \sigma^{-1}({}^{1}\alpha_n)+d_n \bmod 2^{s})$ from $(Z_2^{s})^{n}$ and sends it to Bob. He restores the tuple $d=(d_1, d_2,\dots, d_n)$. Similarly Alice sends

$(\sigma^{-1}({}^{2}\alpha_1)+t_1 \bmod 2^{s}, \sigma^{-1}({}^{2}\alpha_2)+t_2 \bmod 2^{s}, \dots, \sigma^{-1}({}^{2}\alpha_n)+t_n \bmod 2^{s})$ for the delivery $t=(t_1, t_2,\dots, t_n)$ to Bob.

Alice and Bob share the transformations $F: x\rightarrow xM+d$ and $L:x \rightarrow xN+t$.

Thus Alice has the symmetric trapdoor accelerator T of the described above symmetric cipher for herself. She delivers the partial information on T in the form of the tuple $(G_1, *F, G_2, L)$.

So Bob encrypts the plaintext from $(Z^*{}_2^{s})^{n}$ via the consecutive use of G_1, $*F$**,** G_2 and *****L.

Alice has complete information on the trapdoor T. She converts the ciphertext to the plaintext via the consecutive use of *****L^{-1} , $(G_2)^{-1}$, $*F^{-1}$ and $(G_1)^{-1}$.

REMARK 1. The complexity of the protocol is $O(n^3)$. It is the cost of operation in ${}^{n}ES(Z_2^{s})$ or ${}^{n}ES(Z_2^{s+1})$. The encryption and decryption procedures cost $O(n^2)$.

So encryption of $O(n^{t})$, $t \geq 1$ documents costs $O(n^{t+2})$.

REMARK 2. The security of the cryptosystem rests on the security of the protocol.

Highly nonlinear nature of the encryption and decryption maps which have linear degrees and nonpolynomial density makes unfeasible attacks of adversary with the interception of pairs of kind plaintext/corresponding ciphertext.

The protocol uses Conjugation Power Problem. Adversary has decompose g_A or g_B into the word of kind $h^{y}g^{x} h^{-y}$.

REMARK 3. The following obfuscation is possible. Alice and Bob can use hidden tame homomorphisms protocol with the collision element of kind (1) (see [28]). The security of this protocol rests on the word decomposition problem for element g (g_A or g_B) from ${}^{m}ES(Z_2^{s})$ **(**or ${}^{m}ES(Z_2^{s+1})$, $m>n$, $m=O(n)$. Adversary has to decompose g into the word in the alphabet of known generators $g_1, g_2,\dots, g_l$, $l>1$.

REMARK 4. Alice can use this cryptosystem as instrument for digital signatures.

CRYPTOSYSTEM DEC2.

Let us assume that Alice selects invertible elements g_i and h_i, $i=1, 2$ for two inverse twisted Diffie-Hellman protocols**.** So correspondents use two sessions of this protocol with different generators from the platform ${}^{n}ES(Z_2^{s})$.

Alice gets two output elements X_1 and X_2 while Bob gets their inverses Y_1 and Y_2.

Alice and Bob also conduct two twisted Diffie-Hellman protocols with the generators from the platform ${}^{n}ES(Z_2^{s+1})$ and elaborate the element ${}^{r}H$**,** $r=1,2$ from this semigroup given by the tuples $({}^{r}\alpha_1, {}^{r}\alpha_2, \dots, {}^{r}\alpha_n)\epsilon(Z^*{}_2^{s+1})^{n}$ and matrices ${}^{r}B$ with entries ${}^{r}b(i,j)$ from Z_2^{s}.

As in the previous cryptosystem Alice forms affine transformations F and L. She delivers them to Bob similarly to the case of cryptosystem 1.

Bob writes his plaintext p and computes ${}^1p=Y_1(p)$,${}^2p=*F({}^1p)$, ${}^3p =Y_2({}^2p)$. and $c =*L({}^3p)$. He sends the ciphertext c to Alice. She computes ${}^3p$ *as* $*L^{-1}(c)$, ${}^2p= X_2({}^3p)$,

${}^1p=*F^{-1}({}^2p)$ and gets p as $X_1({}^1p)$.

REMARK 5. The inverse Diffie-Hellman protocol with the security based on the complexity of Conjugacy Power problem can be changed for the inverse hidden tame homomorphisms protocol with the collision element of kind (1) from the group ${}^nEG(Z_2{}^s)$ (see [28]).

It will be used for elaboration of X_1, X_2, Y_1, Y_2. For the delivery of F and L correspondents will use hidden tame homomorphism protocol mentioned in the Remark 2.

The security of new cryptosystem rests on the word decomposition problem for element g from ${}^mES(Z_2{}^s)$ (or ${}^mES(Z_2{}^{s+1})$, $m>n$, $m=O(n)$).

3. Algebraic system with the binary operations defined in terms of different commutative rings and its applications

We consider some computational relations between $Z_2{}^{s-1}$, $Z*_2{}^s$ and $F_2{}^{s-1}$.

Recall that $Z*_2{}^s$ is the totality of odd residues modulo 2^s.

We already consider the map $\sigma_{s-1}=\sigma$ from $Z_2{}^{s-1}$ to $Z*_2{}^s$ such that $\sigma(t \bmod 2^{s-1})$ is $2t+1 \bmod 2^s$. It is a bijection**.** Let σ^{-1} be the inverse map from $Z*_2{}^s$ to $Z_2{}^{s-1}$.

Notice that elements from $Z_2{}^{s-1}$can be written as $b=e_0+e_1 2+e_2 2^2 +\dots+e_{s-2}2^{s-2} \bmod 2^{s-1}$, where $e_i \epsilon \{0,1\}$. Element of the finite field F_q, $q=2^{s-1}$ can be written as $g(x)=e_0+e_1x+e_2x^2+\dots+e_{s-2}x^{s-2} \bmod p(x)$ where $p(x)$ is the irreducible polynomial of degree s-1. Let π be the map such that $\pi(b)=g(x)$ and π^{-1} is the inverse map from F_q, $q=2^{s-1}$ onto $Z_2{}^{s-1}$.

We consider the map Δ from F_q onto $(F_2)^{s-1}$ sending $g(x)$ to Boolean vector $(e_0, e_1,\dots, e_{s-2})$ which we identify with the element of Boolean ring B_{s-1} of size 2^{s-1}**.**

These bijective maps allow us to identify the set $Z_2{}^{s-1}$ with $Z*_2{}^s$ and with $F_2{}^{s-1}$ and with B_{s-1}**.**

So we can consider the following binary operation defined on the same set $Z_2{}^{s-1}$**.** The list contains the multiplication and addition of residues modulo 2^{s-1} , multiplication and addition of finite field $F_2{}^{s-1}$, multiplication of elements of Boolean ring B_{s-1} and multiplication of odd residues modulo $Z_2{}^s$**.**

Let us consider the map S of $(Z*_2{}^s)^n$ onto $(Z_2{}^{s-1})^n$ which sends $(x_1, x_2,\dots, x_n)$ to $(\sigma^{-1}(x_1), \sigma^{-1}(x_2)) ,\dots.., \sigma^{-1}(x_n))$. We define the map P of $(Z*_2{}^s)^n$ onto $(F_2{}^{s-1})^n$ which sends $(x_1, x_2,\dots,x_n)$ to $(\pi(\sigma^{-1}(x_1)), \pi(\sigma^{-1}(x_2)) ,\dots.., \pi(\sigma^{-1}(x_n))$. Let D be the map of $(Z*_2{}^s)^n$ onto $(B_{s-1})^n$.

Sending $(x_1, x_2,\dots, x_n)$ to $(\Delta(\pi(\sigma^{-1}(x_1)))$, $\Delta(\pi(\sigma^{-1}(x_2))) ,\dots.., \Delta(\pi(\sigma^{-1}(x_n))))$. We assume that S^{-1}, P^{-1} and D^{-1} are inverses of bijective maps S, P and D.

Let us consider several modifications of the Double Eulerian Cipher.

M1. Let $K= Z_2{}^{s-1}$ and ${}^nF$ be the family of polynomial maps of K^n onto K^n**,** i. e ${}^nF(x_i)$ is an element of $K[x_1, x_2,\dots, x_n]$. Assume that ${}^nF$ has a symmetric trapdoor accelerator T.

Alice and Bob share $({}^nF, T)$ together with the element L from $AGL_n(K)$ and Eulerian transformations G_i, $i=1,2$ defined on $(Z_2{}^s)^n$ with their Eulerian inverses $(G_i)^{-1}$ for which $G_i(G_i)^{-1}(x)=x$ for $x \epsilon (Z*_2{}^s)^n$ **.**

Then they can work with the family of ciphers with the space of plaintexts $(Z*_2{}^s)^n$ and use the encryption function $G= G_1S\,{}^nF\,(S^{-1})G_2\,S\,L\,S^{-1}$**.** The knowledge of T and the decomposition of G and G^{-1} into G_i, ${}^nF$,L, S and their inverses allows to encrypt and decrypt in time $O(n^2)$.

M2. Let $K=F_2{}^{s-1}$ and ${}^nF$ be the family of polynomial maps of K^n onto K^n, i. e ${}^nF(x_i)$ is an element of $K[x_1, x_2,\dots, x_n]$. Assume that ${}^nF$ has a symmetric trapdoor accelerator T.

Alice and Bob share $({}^nF, T)$ together with $L \epsilon AGL_n(K)$ and Eulerian transformations G_i, $i=1,2$ defined on $(Z_2{}^s)^n$ with their Eulerian inverses $(G_i)^{-1}$ for which $G_i(G_i)^{-1}(x)=x$ for $x \epsilon (Z*_2{}^s)^n$ **.**

Then they can work with the family of ciphers with the space of plaintexts $(Z*_2{}^s)^n$ and use the encryption function $G= G_1P\,{}^nF\,(P^{-1})\,G_2\,P\,L(P^{-1})$. The knowledge of T and the decomposition of G and G^{-1} into G_i, ${}^nF$, L, P and their inverses allows to encrypt and decrypt in time $O(n^2)$.

M3. Let $K=B_{s-1}$ and ${}^nF$ be the family of polynomial maps of K^n onto K^n, i. e ${}^nF(x_i)$ is an element of $K[x_1, x_2,\dots, x_n]$. Assume that ${}^nF$ has a symmetric trapdoor accelerator T**,** Alice and Bob share $({}^nF, T)$, $L \epsilon AGL_n(K)$ and Eulerian transformations G_i, $i=1,2$ defined on $(Z_2{}^s)^n$ with their Eulerian inverses $(G_i)^{-1}$ for which $G_i(G_i)^{-1}(x)=x$ for $x \epsilon (Z^*{}_2{}^s)^n$ **.**

Then they can work with the family of ciphers with the space of plaintexts $(Z^*{}_2{}^s)^n$ and use the encryption function $G= G_1D^nF (D^{-1}) G_2 D\ L(D^{-1})$. The knowledge of T and the decomposition of G and G^{-1} into $\psi_{i,}$ ${}^nF$, P, L and their inverses allows to encrypt and decrypt in time $O(n^2)$.

Some examples of systems of kind M_i, $i=1,2$ with the nonlinear symmetric trapdoor accelerators are given in the paper [35]. In some cases the conversion of these ciphers into protocol bases cryptosystem is also presented there.

Below we consider the case of scheme M_i when F is simply an element of $AGL_n(K)$ where $K=Z_2{}^{s-1}$, $K=Z_2{}^{s-1}$ or $K=B_{s-1}$. Its representation in a standard form is a symmetric trapdoor accelerator . In this case we refer to the cipher as Affine Double Eulerian cipher over K *(ADEC(K))*.

In each case of M_i we can convert the affine Double Eulerian cipher over the commutative ring K into two distinct cryptosystems $ADEC_1(K)$ and $ADEC_2(K)$.

If Alice and Bob use $ADEC_1(K)$ they use twisted Diffie-Hellman protocol based on the platform $EG(Z_2{}^s)$. Two sessions of the protocol Alice uses for the delivery of G_1 and G_2 to Bob. Alice and Bob use other two session of this protocol with the same platform $EG(Z_2{}^s)$ for the delivery of created by Alice two affine transformations of kind $x\rightarrow xM+d$ from $AGL_n(K)$.

Assume that the collision element is given by the tuple $(\alpha_1, \alpha_2,\dots, \alpha_n)$ with the coordinates from $Z^*{}_2{}^s$ and matrix $B=(b(i, j))$ with the entries from $Z_2{}^{s-1}$ **.**

In the case of M_1 Alice simply sends $M+B$ and the tuple $(d_1, d_2, ..., d_n)+(\sigma^{-1} (\alpha_1), \sigma^{-1} (\alpha_2),\dots, \sigma^{-1}(\alpha_n))$ to Bob. He restores the affine transformation A.

In the case of M_2 Alice sends the matrix $M+(\pi(b(i,j))$ and the tuple $(d_1, d_2, ..., d_n)+(\pi(\sigma^{-1} (\alpha_1), \pi(\sigma^{-1} (\alpha_2), ..., \pi(\sigma^{-1} (\alpha_n))$ to Bob. He restore M and the tuple d.

In the case of M_3 Alice sends the matrix $M+(\Delta(\pi(b(i,j)))$ and the tuple$(d_1, d_2, ..., d_n)+(\Delta(\pi(\sigma^{-1} (\alpha_1)), \Delta(\pi(\sigma^{-1}(\alpha_2)), ..., \Delta(\pi(\sigma^{-1}(\alpha_n))$. Bob restores the transformation A from $AGL_{n-1}(B_{s-1})$.

In $ADEC_2$ Alice and Bob conduct the inverse twisted Diffie-Hellman protocol within the platform ${}^nEG(Z_2{}^s)$ twice and elaborate mutually inverse maps X_i, Y_i, $i=1, 2$ such that $X_iY_i\ (x)=x$ for each x in $(Z^*{}_2{}^s)\ {}^n$. They used twisted Diffie-Hellman algorithm for the delivery of affine transformation A from $AGL_n(K)$ similarly to the case of $ADEC_{1.}$

So in the case of M_1 Bob uses $E_B = Y_1S\ F(S^{-1})Y_2\ S\ L\ S^{-1}$ together with the decomposition into Y_i, F, L and S for the encryption of plaintext p from $(Z^*{}_2{}^{s-1})\ {}^n$**.**

Alice decrypts it with her transformation $S\ L^{-1}\ S^{-1}\ X_2SA^{-1}S^{-1}X_1=E_A$.

Symmetrically Alice encrypts with her transformation E_A and Bob decrypts with his E_B**.**

In the cases of M_2 and M_3 correspondents has to change the map S for P and D respectively.

REMARK 6.

In the algorithm $ADEC_1(K)$ there is an option to change twisted Diffie-Hellman protocols for the hidden Tahoma protocols with outputs from ${}^nES(Z_2{}^s)$ (see [28]).

In the case of $ADEC_2(K)$ one can change each inverse twisted Diffie-Hellman protocol for the two inverse hidden tame homomorphism protocols with the outputs in ${}^nEG(Z_2{}^s)$. It will be used for elaboration of X_1, X_2, Y_1, Y_2. The third protocol with the security based on the complexity of Conjugacy Power problem can be changed for the hidden tame homomorphisms protocol with the collision element of kind (1) from the semigroup ${}^nES(Z_2{}^s)$ (see [28]). It will be used for the delivery of affine transformations F and L.

After these changes we get cryptosystems which security rests on the word decomposition problem for elements of ${}^nES(Z_2{}^s)$.

REMARK 7.

Let K be one of the commutative rings $Z_2{}^s$ **,** $Z_2{}^{s-1}$ **,** $F_2{}^{s-1}$ and B_{s-1} , assume that ${}^K\psi : K^n\rightarrow K^n$ be one of the maps I (identity map), S, P, D correspondingly.

Assume that K and Q are distinct elements of the set **{** $Z_2{}^s$ **,** $Z_2{}^{s-1}$ **,** $F_2{}^{s-1}$, B_{s-1}**}** we can consider the cipher $DEC(K, Q)$ with the space of plaintexts **(**$Z^*{}_2{}^s$ $)^n$ with the encryption procedure defined as the consecutive application of $G_{1,}$ ${}^K\psi$ **,** F_K, ${}^K\psi^{-1}$ G_2 **,** ${}^Q\psi$, $L_{Q,,}$ ${}^Q\psi^{-1}$

where F_K and L_K are elements of $AGL_n(K)$ for K of cardinality 2^{s-1} and $F_K=F^*$, $L_K=L^*$ for F,L $\epsilon AGL_n(K)$ if $K= Z_2{}^s$ **.**

The cipher $DEC(K, Q)$ can be converted to protocol based cryptosystems $ADEC_i(K, Q)$, $i=1,2$ similarly to the considered above cases M1, M2 and M3.

Conclusions

Quadratic multivariate public rules can be used for the verification of the signature in time $O(n^3)$ where n is the size of the hash file of the document. The search for such public key is continue.

We are working on alternative method of the use of asymmetric protocol based cryptosystem to sign the document. We suggest some protocols of Noncommutative Cryptography implemented on the platform of Eulerian transformations of $Z*_2^s[x_1, x_2,..., x_n]$ acting naturally on the variety $(Z*_2^s)^n$, $s >1$.

The density of Eulerian transformation, i.e the number of all monomial terms in the standard form is ***n*.** Degree of general Eulerian transformation is a linear function in variable n. The composition of Eulerian transformation G_1 and affine transformation A from $AGL_n(Z_2^s)$ has a linear degree and density $O(n^2\ )$. The composition of kind $F=G_1AG_2$ where G_2 is another Eulerian transformation is *different.* Substitution of the polynomials of density n to each variable of monomial terms leads to effect of nonpolynomial density of F. So the standard form of F is not computable in polynomial time.

We can use four sessions of one of the protocols of Noncommutative Cryptography for the safe delivery of Eulerian maps G_1, G_2 and A_1, A_2 from Alice to her partner Bob. Alternatively G_i, $i=1,2$ can be elaborated via the protocol of inverse type.

Selected affine transformations A_i send x to the element of kind $xM+b$ from $(Z*_2^s)^n$ where each column of the matrix M has an odd number of odd residues modulo 2^s and all coordinates of the tuple b are even residues.

Eulerian endomorphism G_i , $i=1,2$ has to act on $(Z*_2^s)^n$ as bijective transformations. Bob will use the map $F=G_1A_1G_2A_2$.

The knowledge of the decomposition of F into G_1, G_2 and A_i, $i=1,2$ allows Bob to compute the value of F on the tuple from $(Z*_2^s)^n$ in time $O(n^2)$. Additional information on the decomposition of each Eulerian transformation into $O(1)$ Jordan -Gauss elements allows Alice to compute the reimage of F.

Attacks of adversary via the interceptions of hash value of documents and corresponding reimages are unfeasible because of the nonpolynomial density of ***F*.** So adversary has to concentrate on the attempts to break the protocol with the security based on the complexity of Conjugacy Power Problem or Word decomposition problems for the platforms of Eulerian transformations. Reader can find recent cryptanalytical studies of Noncommutative Cryptography in papers [29]-[34].

We note that known cryptanalytical tools are not applicable for the investigation of proposed cryptosystem. Some methods to make protocol based digital signatutes with Eulerian transformations in the case of general commutative ring K with unity are considered in [36]. Examples of the change of affine transformation A for the nonlinear map with the trapdoor accelerator are described in [35].

In the Section 4 we use natural bijections between $Z*_2^s$ and Z_2^{s-1}, $Z*_2^s$ and finite field F_2^{s-1} and $Z*_2^s$ and Boolean ring B_{s-1} of order 2^{s-1} to modify the family of ciphers or cryptosystems from the Section 3 via the change of $AGL_n(Z*_2^s)$ for the $AGL(K)$, where K is one of the rings

Z_2^{s-1}, F_2^{s-1} and B_{s-1}. New ciphers are defined via the algebraic systems with the operations of multiplications of two different commutative rings Z_2^s and K and the operation of addition in ***K*.** It does not allow to treat them as stream ciphers of multivariate cryptography over the single commutative ring. That is why the adversary is not able to use known cryptanalytical methods such as linearisation attacks.

Funding Information. This research is supported by British Academy Fellowship for Researchers under Risk 2022 and partially supported by British Academy award LTRSF\100333.

References

[1] Ward Beullens, Improved Cryptanalysis of UOV and Rainbow, In Eurocrypt 2021, Part 1, pp. 348-373.

[2] Anne Canteaut, François-Xavier Standaert (Eds.), Eurocrypt 2021, LNCS 12696, 40th Annual In-ternational Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croa-tia, October 17–21, 2021, Proceedings, Part I, Springer, 2021, 839p.

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

[4] M. Noether, Luigi Cremona, Mathematische Annalen, 59 (1904), pp. 1-19.

[5] Jintai Ding, Joshua Deaton, Vishakha, and Bo-Yin Yang, The Nested Subset Differential Attack,A Practical Direct Attack Against LUOV Which Forges a Signature Within 210 Minutes, In Eurocrypt 2021, Part 1, pp. 329-347.

[6] V. Ustimenko, On Extremal Algebraic Graphs and Multivariate Cryptosystems, IACR e-print archive, 2022/1537.

[7] Ding and A. Petzoldt, "Current State of Multivariate Cryptography," in IEEE Security & Privacy, vol. 15, no. 4, pp. 28-36, 2017, doi: 10.1109/MSP.2017.3151328.

[8] Smith-Tone, D. (2022), 2F - A New Method for Constructing Efficient Multivariate Encryption Schemes, Proceedings of PQCrypto 2022: The Thirteenth International Conference on Post-Quantum Cryptography, virtual, DC, US.

[9] Daniel Smith Tone, New Practical Multivariate Signatures from a Nonlinear Modifier, IACR e-print archive, 2021/419.

[10] Daniel Smith-Tone and Cristina Tone, A Nonlinear Multivariate Cryptosystem Based on a Random Linear Code, https://eprint.iacr.org/2019/1355.pdf

[11] Jayashree, Dey, Ratna Dutta, Progress in Multivariate Cryptography: Systematic Review, Challenges, and Research Directions, ACM Computing Survey, volume 55, issue 12,No.246, pp 1-34, https://doi.org/10.1145/3571071.

[12] Ikematsu, Y. , Perlner, R. , Smith-Tone, D. , Takagi, T. and Vates, J. (2018), HFERP -- A New Multivariate Encryption Scheme, PQCrypto 2018: The Ninth International Conference on Post-Quantum Cryptography, Fort Lauderdale, FL, US, [online], https://doi.org/10.1007/978-3-319-79063-3_19, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=925152.

[13] Cabarcas Felipe, Cabarcas Daniel, and Baena John. 2019. Efficient public-key operation in multivariate schemes. Advances in Mathematics of Communications 13, 2 (2019), 343.

[14] Cartor Ryann and Smith-Tone Daniel. 2018. EFLASH: A new multivariate encryption scheme. In Proceedings of the International Conference on Selected Areas in Cryptog-raphy. Springer, 281–299.

[15] Casanova Antoine, Faugère Jean-Charles, Macario-Rat Gilles, Patarin Jacques, Perret Lu-dovic, and Ryckeghem Jocelyn. 2017. Gemss: A great multivariate short signa-ture. Submission to NIST (2017).y. Springer, Singapore, 209–229.

[16] Chen Jiahui, Ning Jianting, Ling Jie, Lau Terry Shue Chien, and Wang Yacheng. 2020. A new encryption scheme for multivariate quadratic systems. Theoretical Computer Sci-ence 809 (2020), 372–383.

[17] Chen Ming-Shing, Hülsing Andreas, Rijneveld Joost, Samardjiska Simona, and Schwabe Peter. 2018. SOFIA: MQ-based signatures in the QROM. In Proceedings of the IACR Inter-national Workshop on Public Key Cryptography. Springer, 3–33.

[18] Ding Jintai, Perlner Ray, Petzoldt Albrecht, and Smith-Tone Daniel. 2018. Improved crypta-nalysis of hfev-via projection. In Proceedings of the International Conference on Post-Quantum Cryptography. Springer, 375–395.

[19] Ding Jintai, Petzoldt Albrecht, and Schmidt Dieter S.. 2020. Multivariate Public Key Cryp-tosystems, Second Edition. Advances in Information Security. Springer

[20] Ding Jintai, Zhang Zheng, Deaton Joshua, Schmidt Kurt, and Vishakha F.. 2019. New at-tacks on lifted unbalanced oil vinegar. In Proceedings of the 2nd NIST PQC Standardiza-tion Conference.

[21] Ding Jintai, Zhang Zheng, Deaton Joshua, and Wang Lih-Chung. 2020. A complete crypta-nalysis of the post-quantum multivariate signature scheme Himq-3. In Proceedings of the International Conference on Information and Communications Security.

[22] Dung H. Duong, Ha T. N. Tran, Willy Susilo, and Le Van Luyen. 2021. An efficient multi-variate threshold ring signature scheme. Computer Standards & Interfaces 74.

[23] Jean-Charles Faugère, Gilles Macario-Rat, Jacques Patarin, and Ludovic Perret. 2022. A new perturbation for multivariate public key schemes such as HFE and UOV. Cryptology ePrint Archive (2022).

[24] V. Ustimenko, T. Chojecki, M. Klisowski, On the implementations of new graph based cubic Multivariate Public Keys, Proceedings of the 18th Conference on Computer Science and Intelligence Systems, ACSIS, Vol. 35, pp. 1179-1184

[25] Vasyl Ustimenko, Aneta Wróblewska, Extremal algebraic graphs, quadratic multivariate public keys and temporal rules, FedCSIS 2023: 1173-1178.

[26] V. Ustimenko, On new multivariate cryptosystems based on hidden Eulerian equations over finite fields, IACR e-print archive.2017/093(PDF)

[27] V. A. Ustimenko. On new multivariate cryptosystems based on hidden Eulerian equations, Dopovidi of National Academy of Science of Ukraine N5, 2017.

[28] V. Ustimenko, On Eulerian semigroups of multivariate transformations and their cryptographic applications. European Journal of Mathematics 9, 93 (2023).

[29] Myasnikov A., Roman'kov V. A linear decomposition attack // Groups, Complexity, Cryptology. 2015. Vol. 7. P. 81–94.

[30] Roman'kov V. A. A nonlinear decomposition attack. Groups, Complexity, Cryptology. 2017. Vol. 8, No. 2. P. 197–207.

[31] Romankov V. Two general schemes of algebraic cryptography. Groups, Complexity, Cryptology. 2018. Vol. 10, No. 2. P. 83–98.

[32] Roman'kov V. An improved version of the AAG cryptographic protocol. Groups, Complexity, Cryptology. 2019. Vol. 11, No. 1. 1 2.

[33] Tsaban B. Polynomial time solutions of computational problems in noncommutative algebraic cryptography. Journal of Cryptology. 2015. Vol. 28, No. 3. P. 601–622.

[34] Ben-Zvi A., Kalka A., Tsaban B. Cryptanalysis via algebraic spans. Advances in Cryptology – CRYPTO 2018 / eds.: H. Shachan, A. Boldyreva. Berlin: Springer, 2018. P. 1–20. (LNCS; vol. 109991).

[35] Vasyl Ustimenko, On historical Multivariate Cryptosystems and their restorations as instruments of Post-Quantum Cryptography, IACR e-print Archive 2024/091.

[36] Vasyl Ustimenko, On short digital signatures with Eulerian transformations, IACR e-print Archive 2024/001.