On the cryptosystems based on two Eulerian transformations defined over the commutative rings \(Z_2^s, s>1\).

Vasyl Ustimenko\(^1,2\)

\(^1\) Royal Holloway University of London, United Kingdom.
\(^2\) Institute of telecommunications and global information space, Kyiv, Ukraine

E-mail: Vasyly.Ustimenko@rhul.ac.uk

Abstract. We suggest the family of ciphers \(E_n, n=2,3,\ldots\) with the space of plaintexts \((Z^*_2)^n\), \(s>1\) such that the encryption map is the composition of kind \(G=G_1G_2A_2\) where \(A_2\) are the affine transformations from \(AGL_n(Z_2^s)\) preserving the variety \((Z^*_2)^n\).

Eulerian endomorphism \(G_i, i=1,2\) of \(K[x_1, x_2,\ldots, x_n]\) moves \(x_i\) to monomial term \(\mu_{x_1^{d(1)}x_2^{d(2)}\ldots x_n^{d(s)}}, \mu \in (Z^*_2)\) and act on \((Z^*_2)^n\) 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 \(A_2\) 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 \(G, A_2\), Alice and Bob can elaborate these transformations via the inverse twisted Diffie-Hellman protocol implemented on the platform of tame Eulerian transformations of \((Z^*_2)^n\). The cost of single protocol is \(O(n^t)\) and the cost of the computation of the reimage of used nonlinear map is \(O(n^t)\). 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 \(Z_2^{\mu(s)}\), \(Z_2^s\) and \(F_2^{\mu(s)}\) and Boolean ring \(B_{\mu(s)}\) of order \(2^{\mu(s)}\) 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 \(Z_2^s, F_2^{\mu(s)}\) and \(B_{\mu(s)}\). 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 \(p \in P\) in time \(O(n^t)\) and to solve the equation of kind \(F(x)=c\) for each \(c\) from \(C\) in time \(O(n^t)\).

Keywords: Symmetric stream ciphers, Digital signatures, Protocol based cryptosystems, Noncommutative Cryptography, Eulerian transformations.
1. 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 $O(n^t)$ 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 $O(n^t)$. 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 2 contains some definitions of Multivariate Cryptography and Algebraic Geometry. It contains also description of the semigroup of Eulerian transformations of $K[x_1,x_2,...,x_n]$ where $K$ is a commutative ring acting naturally on the variety $(K^*)^n$. Some bijective transformations of $(K^*)^n$ induced by Eulerian maps are also presented. Some basic protocols of Noncommutative Cryptography are given there. These protocols can be implemented on the platforms of Eulerian transformations.

Section 3 contains the description of ciphers and protocol based cryptosystems which used the compositions of kind $E_iAE_i$ where $E_i$, $i=1,2$ are Eulerian endomorphisms of $Z_2^+x_1,x_2,...,x_n$ and $A$ is the special element of $AGL_n(Z_2^+)$ which preserves the variety $(Z^t)^n$. In the Section 4 we use fast computable natural bijection between $Z^t$ and one of the ring $K=Z_2^t$, $K=Z_2^{t-d}$ and $K=Z_2^{t-d}$ which is the Boolean ring of order $2^{t-d}$. 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 $O(n^2)$. The last section is the conclusion.

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

2.1 Some definitions.

Classical multivariate public rule is a transformation of $n$-dimensional vector space over finite field $F_q$ which move vector $(x_1,x_2, ...,x_n)$ to the tuple $(g_1(x_1,x_2,...,x_n), g_2(x_1,x_2,...,x_n), ..., g_d(x_1,x_2,...,x_n))$, 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 $^\ast CS(K)$ is defined as endomorphism group of polynomial ring $K[x_1, x_2, ..., x_n]$ 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 $\sigma$ can be given via its values on variables, i.e. as the rule $x_i \mapsto f_i(x_1, x_2, ..., x_n)$, $i=1, 2, ..., n$. This rule induces the map $\sigma : (a_1, a_2, ..., a_n) \mapsto (f_1(a_1, a_2, ..., a_n), f_2(x_1, x_2, ..., x_n), ..., f_n(x_1, x_2, ..., x_n))$ on the free module $K^n$. Automorphisms of $K[x_1, x_2, ..., x_n]$ form affine Cremona Group $^\ast CG(K)$. In the case when $K$ is a finite field or arithmetic ring $\mathbb{Z}_m$ of residues modulo $m$ elements of affine Cremona Groups or Semigroups are used in algorithms of Multivariate Cryptography. Results about subsemigroups $S$ of $^\ast CS(K)$ (or subgroups of $^\ast CG(K)$ such that computation of the superposition of arbitrary $n$ elements can be completed for polynomial time can be used as so called platforms of Non-commutative Cryptography. One class of such objects is formed by stable subsemigroups of degree $k$, i.e. subsemigroup $S$ 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 $^\ast CG(K)$ exist for each $k, k=2, 3, ....$. Affine Cremona semigroup $^\ast CS(K)$ does not poses MCC. If one takes $n$ 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 $^\ast ES(K)$ of endomorphisms of $K[x_1, x_2, ..., x_n]$ of kind

$$
\begin{align*}
x_1 &\mapsto M_1 x_1^{a(1,1)} x_2^{a(1,2)} ... x_n^{a(1,n)} , \\
x_2 &\mapsto M_2 x_1^{a(2,1)} x_2^{a(2,2)} ... x_n^{a(2,n)} , \\
\vdots \ &

\end{align*}
$$

(1)

where $M_i$ 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 $^\ast ES(K)$ poses MCC property. Semigroups with MCC property can serve as ’platforms’ for protocols of Non-commutative Cryptography.

### 2.2 Twisted Diffie-Hellman protocol.

Let $S$ be an abstract semigroup which has some invertible elements. Alice and Bob share element $g \in S$ and pair of invertible elements $h, h^{-1}$ from this semigroup. Alice takes positive integers $k(A)$ and $r(A)$ and forms $h^{k(A)} g^{k(A)} h^{-k(A)} = g_3$. Bob takes $k(B)$ and $r(B)$ and forms $h^{r(B)} g^{r(B)} h^{-r(B)} = g_B$. They exchange $g_3$ and $g_B$ and compute collision element $X$ as $g = h^{r(B)} g^{k(A)} h^{-r(B)}$ (Alice) and $g' = h^{k(B)} g^{r(A)} h^{-k(B)}$ (Bob) respectively.
The security of the scheme rest on the Conjugation Power Problem, adversary has to solve the problem \( h^s g^t h^r = b \) where \( b \) coincides with \( g_b \) or \( g_a \). The complexity of the problem depends heavily on the choice of highly noncommutative platform \( S \).

2.3. Inverse twisted Diffie-Hellman protocol.

Let \( S \) be an abstract noncommutative semigroup which has some invertible elements. Alice and Bob share element \( gcS \) and pair of invertible elements \( h, h^{-1} \) from this semigroup. Alice knows \( g^{-1} \). Alice takes positive integers \( k(\mathcal{A}) \) and \( d= r(\mathcal{A}) \) and \( k(\mathcal{B}) \) and \( r(\mathcal{B}) \) and forms \( h^{-r(\mathcal{A})} g^{-k(\mathcal{A})} h^{r(\mathcal{A})} = g_a \). Bob takes \( k(\mathcal{B}) \) and \( r(\mathcal{B}) \) and forms \( h^{-r(\mathcal{B})} g^{-k(\mathcal{B})} h^{r(\mathcal{B})} = g_b \). They exchange \( g_a \) and \( g_b \) and Alice computes \( X = h^{-r(\mathcal{A})}(g_b)^{r(\mathcal{A})} h^{r(\mathcal{A})} \). Bob computes \( Y = h^{-r(\mathcal{B})}(g_a)^{r(\mathcal{B})} h^{r(\mathcal{B})} \). It is clear that \( Y = h^{-r(\mathcal{B})}(g_a)^{r(\mathcal{B})} h^{r(\mathcal{B})} \).

The security of the scheme rest on the Conjugation Power Problem, adversary has to solve the problem \( h^s g^t h^r = b \).

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

REMARK. Protocols with the security based on the word decomposition problem, i.e. task to decompose \( g e \) into the word in given generators \( g_1, g_2, \ldots, g_t \) were presented during my previous talk.

2.4. On some bijective transformation of \((K^\ast)^m\).

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

\[
\begin{align*}
\gamma_{a(1,1)} &= a(1,1)X_{a(1,1)}^{0} \\
\gamma_{a(2,1)} &= a(2,1)X_{a(2,1)}^{0} \\
\vdots
\gamma_{a(n,1)} &= a(n,1)X_{a(n,1)}^{0} \\
\gamma_{a(2,2)} &= a(2,2)X_{a(2,2)}^{0} \\
\vdots
\gamma_{a(n,n)} &= a(n,n)X_{a(n,n)}^{0} \\
\end{align*}
\]

where \( (a(1,1), d) = 1, (a(2,2), d) = 1, \ldots, (a(n,n), d) = 1 \). We refer to \( ^{\ast}JG(\pi, \delta) \) as Jordan transformations Gauss multiplicative transformation or simply \( JG \) element. It is an invertible element of \( ^{\ast}ES(K) \) with the inverse of kind \( ^{\ast}JG(\delta, \pi) \) such that \( a(i,j)b(i,j) = 1 \pmod{d} \). Notice that in the case \( K = \mathbb{Z}_m \) 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 \( K^\ast \) into \( K^\ast \) was used in [27] \( (K=\mathbb{Z}_m) \) and [26] \( (K=F_q) \).

We say that \( \tau \) 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 \( \tau \) sends variable \( x \) to a certain monomial term. The decomposition of \( \tau \) into product of Jordan Gauss transformation allows us to find the
solution of equations $\tau(x) = b$ for $x$ from $(\mathbb{Z}_n^*)^n$ or $(F^*)^m$. So tame Eulerian transformations over $\mathbb{Z}_n$ or $F_q$ are special elements of $^*E\mathbb{G}(\mathbb{Z}_n)$ or $^*E\mathbb{G}(F_q)$ respectively.

We refer to elements of $^*E\mathbb{G}(K)$ 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 $^*E\mathbb{G}(K)$ 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 $g\in ^*E\mathbb{G}(K)$ on Turing machine or Quantum computer and problem finding the inverse for tame Eulerian elements.

### 3. Some ciphers and cryptosystems based on Eulerian transformations over the $\mathbb{Z}_2^s$

The main idea of constructions of this section is based on the fact that the composition of the general element $A$ of $\text{AGL}_n(K)$ and the general element $G$ of $^*E\mathbb{G}(K)$ has nonpolynomial density. We can change element $A$ for the general element $F$ of $\text{CG}_d(K)$. In the case of $K=\mathbb{Z}_2$, $s>1$ we can slightly modify $F$ of kind $x_i \rightarrow f(x_i, x_2, \ldots, x_s)$ and get the bijective transformation $^*F$ of the variety $(\mathbb{Z}_2^n)^s$ via the following procedure.

We set the vector $b=(b_1, b_2, \ldots, b_s)$ where $b_i=1$ if $f_i(1, 1, \ldots, 1) \equiv 0 \pmod{2}$ and $b_i=0$ if $f_i(1, 1, \ldots, 1) \equiv 1 \pmod{2}$ and form $^*F$ as transformation of $(\mathbb{Z}_2^n)^s$ 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 $T$ then computation of $F(1, 1, \ldots, 1)$ can be completed in polynomial time.

Assume that $G$ from $\text{CG}_d(K)$ is formed as the composition of $k=O(1)$ Jordan-Gauss transformations $J_1, J_2, \ldots, J_k$.

Alice and Bob share the information on $T$ and the decomposition of $G$ into $J_i, i=1, 2, \ldots, k$.

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

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 infeasible because of the nonpolynomial density of $G(^*F)$.

We 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 $\text{AGL}_n(\mathbb{Z}_2)$. 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 $(\mathbb{Z}_2^n)^s$.

Encryption procedure has the following steps.
S1. The transformation of the plaintext \((p_1, p_2, ..., p_n)=p\) to the \(^{t}p=G(t)p=(^{t}p_1, ^{t}p_2, ..., ^{t}p_n)\).

S2. The computation of \(*F(^{t}p)=^{t}p\).

S3. The computation of \(^{t}p=G(^{t}p)\).

S4. The computation of the ciphertext \(c\) as \(*L(^{t}p)\).

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

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

**Remark 1.** The encryption map is induced by multivariate transformation \(E\) of \((Z^n)^n\). It has a linear degree of kind \(an, a>0\) and nonpolynomial density which is the total number of monomial terms in all \(F(x)\). 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 \(p \in P\) in time \(O(n^2)\) and to solve the equation of kind \(F(x)=c\) for each \(c \in C\) in time \(O(n^2)\).

For the encryption map \(E\) of the defined above cipher the decomposition of \(E\) into the 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 \(*ES(Z^n)\) 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 \(*ES(Z^n)\) and elaborate the elements \(H, r=1, 2\) 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 \(H\) are maps of kind \((1)\) with \((m_1, m_2, ..., m_n)=(m(i)), (z_1, z_2, ..., z_n)=(z(i))\) and \(a(j,k)=a, (j, k)\) and maps \(G\) are elements of kind \((1)\) with \((m_1, m_2, ..., m_n)=(m(i)), (z_1, z_2, ..., z_n)=(z(i)), \) and \(a(j,k)=b, (j, k)\) mod \(2^t\).

Assume that \(H, r=1, 2\) is element of kind \((1)\) with \((m_1, m_2, ..., m_n)=\left(\alpha_1, \alpha_2, ..., \alpha_n\right)\) and \(a(i, k)=b(i, k)\) mod \(2^t\). Let \(B=(b(i, j))\).

Alice sends parameters \(m(i), z(i), j=1, 2, ..., n, i=1, 2\) and \(a(j, k)+b(i, j)\) mod \(2^t\), \(j=1, 2, ..., n, k=1, 2, ..., n, i=1, 2\).

So Bob restores \(G_1\) and \(G_2\).

Alice creates invertible matrices \(M, N\) with entries from \(Z^n\). She sends \(M+B\) and \(N+B\) to Bob. So he restores the matrices \(M, N\).

Finally Alice selects the tuples \((d_1, d_2, ..., d_n)\) and \((t_1, t_2, ..., t_n)\) from \((Z^n)^n\). She takes \(\left(\alpha_1, \alpha_2, ..., \alpha_n\right)\) of elements from \(Z^n\).

Alice considers the map \(\sigma: \sigma(z)\) from \(Z^n\) to \(Z^{n+1}_2\) such that \(\sigma(t \mod 2^t)\) is \(2t+1 \mod 2^t\). It is a bijection. Let \(\sigma^{-1}\) be the inverse map from \(Z^{n+1}_2\) to \(Z^n\). She forms \(\sigma^{-1}(\alpha_1)+d_1 \mod 2^t, \sigma^{-1}(\alpha_2)+d_2 \mod 2^t, ..., \sigma^{-1}(\alpha_n)+d_n \mod 2^t\) and sends it to Bob. He restores the tuple \(d=(d_1, d_2, ..., d_n)\). Similarly Alice sends
(σ^i(2a_1)+t_1 \mod 2^i, \sigma^i(2a_2)+t_2 \mod 2^i, ..., \sigma^i(2a_n)+t_n \mod 2^i) for the delivery \( t=(t_1, t_2, ..., t_n) \) to Bob.

Alice and Bob share the transformations \( F: x \mapsto xM+d \) and \( Lx \mapsto xN+t \).

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 \( (G_i, \#F, G_2, L) \).

So Bob encrypts from \((Z^*;\epsilon)^n\) via the consecutive use of \( G_i, \#F, G_2 \) 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 \( (G_i)^{-1} \).

**REMARK 1**. The complexity of the protocol is \( O(n^3) \). It is the cost of operation in \( "ES(Z^*_{\epsilon})" \) or \( "ES(Z^*_{\epsilon}r)" \). The encryption and decryption procedures cost \( O(n^2) \).

So encryption of \( O(n^3) \), \( t \geq 1 \) 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 \( g_2 \) or \( g_n \) into the word of kind \( h^i g^j h^i \).

**REMARK 3**. The following obfuscation is possible. Alice and Bob can use hidden tame homomorphisms protocol with the collision element of kind \( (1, 2) \) (see [28]). The security of this protocol rests on the word decomposition problem for element \( g \) from \( "ES(Z^*_{\epsilon})" \) or \( "ES(Z^*_{\epsilon}r)" \), \( m \geq n, m=O(n) \). Adversary has to decompose \( g \) into the word in the alphabet of known generators \( g_1, g_2, ..., g_s, l>L \).

**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 \( "ES(Z^*_{\epsilon})" \).

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 \( "ES(Z^*_{\epsilon}r)" \) and elaborate the element \( H_r, r=1,2 \) from this semigroup given by the tuples \( (\epsilon a_1, \epsilon a_2, ..., \epsilon a_n) \) and matrices \( B \) with entries \( h(i,j) \) from \( Z^*_{\epsilon}r \).

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 \( \hat{p}=Y_1(p), \hat{p}=F^r(p), \hat{p}=Y_2^r(p), c = \#L^r(p) \). He sends the ciphertext \( c \) to Alice. She computes \( p \) as \( \#L^{-1}(c) \). \( \hat{p}=X_2^r(p), \hat{p}=F^r(p) \) and gets \( p \) as \( X_2^r(p) \).

**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 \( (1, 2) \) from the group \( "EG(Z^*_{\epsilon})" \) (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 \( "ES(Z^*_{\epsilon})" \) (or \( "ES(Z^*_{\epsilon}r)" \), \( m \geq n, m=O(n) \)).
4. Algebraic system with the binary operations defined in terms of different commutative rings and its applications

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

Recall that $\mathbb{Z}_2^*$ is the totality of odd residues modulo $2^1$.

We already consider the map $\sigma_i = \sigma$ from $\mathbb{Z}_2^{-1}$ to $\mathbb{Z}_2^*$, such that $\sigma(t \mod 2^{-1})$ is $2t+1 \mod 2^1$. It is a bijection. Let $\sigma^i$ be the inverse map from $\mathbb{Z}_2^*$ to $\mathbb{Z}_2^{-1}$.

Notice that elements from $\mathbb{Z}_2^*$ can be written as $b = e_0 + e_12 + e_22^2 + ... + e_i2^{i-1} \mod 2^{i-1}$, where $e_i \in \{0,1\}$. Element of the finite field $F_q$, $q=2^{i-1}$ can be written as $g(x) = e_0 + e_1x + e_2x^2 + ... + e_i2^{i-2} \mod 2^{i-1}$, where $p(x)$ is the irreducible polynomial of degree $i-1$. Let $\pi$ be the map such that $\pi(b) = g(x)$ and $\pi^i$ is the inverse map from $F_q$ $q=2^{i-1}$ onto $\mathbb{Z}_2^{-1}$.

We consider the map $\Delta$ from $F_q$ onto $(F_2^{-1})^i$ sending $g(x)$ to Boolean vector $(e_0, e_1, ..., e_i)$ which we identify with the element of Boolean ring $B_i$ of size $2^{-i}$.

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

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

Let us consider the map $S$ of $(Z_2^*)^n$ onto $(Z_2^{-1})^n$ which sends $(x_1, x_2, ..., x_n)$ to $(\sigma_1^{-1}(x_1), \sigma_2^{-1}(x_2), ..., \sigma_n^{-1}(x_n))$. We define the map $P$ of $(Z_2^*)^n$ onto $(F_2^{-1})^n$ which sends $(x_1, x_2, ..., x_n)$ to $(\pi(\sigma_1^{-1}(x_1)), \pi(\sigma_2^{-1}(x_2)), ..., \pi(\sigma_n^{-1}(x_n)))$. Let $D$ be the map of $(Z_2^*)^n$ onto $(B_i)^n$.

Sending $(x_1, x_2, ..., x_n)$ to $(\Delta(\pi(\sigma_1^{-1}(x_1))), \Delta(\pi(\sigma_2^{-1}(x_2))), ..., \Delta(\pi(\sigma_n^{-1}(x_n))))$ we assume that $S^i$, $P^i$ and $D^i$ are inverses of bijective maps $S$, $P$ and $D$.

Let us consider several modifications of the Double Eulerian Cipher.

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

Alice and Bob share $(^*F, T)$ together with the element $L$ from AGLn($K$) and Eulerian transformations $G_n$ $i = 1, 2$ defined on $(Z_2^n)^i$ with their Eulerian inverses $(G_i)^{-1}$ for which $G_i(G_i^{-1}(x)) = x$ for $x \in (Z_2^n)^i$.

Then they can work with the family of ciphers with the space of plaintexts $(Z_2^n)^n$ and use the encryption function $G = G_1S^*^nF(S)^iG_2S$ $L S L^{-1}$. The knowledge of $T$ and the decomposition of $G$ and $G^{-1}$ into $G_i, ^*F, L, S$ and their inverses allows to encrypt and decrypt in time $O(n^2)$.

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

Alice and Bob share $(^*F, T)$ together with LAGLn($K$) and Eulerian transformations $G_n$ $i = 1, 2$ defined on $(Z_2^n)^i$ with their Eulerian inverses $(G_i)^{-1}$ for which $G_i(G_i^{-1}(x)) = x$ for $x \in (Z_2^n)^i$.

Then they can work with the family of ciphers with the space of plaintexts $(Z_2^n)^n$ and use the encryption function $G = G_1P^*^nF(P)^iG_2P L(P)^{-1}$. The knowledge of $T$ and the decomposition of $G$ and $G^{-1}$ into $G_i, ^*F, L, P$ and their inverses allows to encrypt and decrypt in time $O(n^2)$. 
M3. Let $K=B_{n,i}$ and $^*F$ be the family of polynomial maps of $K^n$ onto $K^n$, i.e. $^*F(x_i)$ is an element of $K[x_1,x_2,...,x_n]$. Assume that $^*F$ has a symmetric trapdoor accelerator $T$. Alice and Bob share $(^*F, T)$, $L_{AGL_n}(K)$, and Eulerian transformations $G_i, i=1,2$ defined on $(Z_{q^i})^n$ with their Eulerian inverses $(G_i)^{-1}$ for which $G_i(G_i)^{-1}(x)=x$ for $x \in (Z_{q^i})^n$.

Then they can work with the family of ciphers with the space of plaintexts $(Z_{q^i})^n$ and use the encryption function $G=F_{i\rightarrow 2}^G((D^{-1})_{i\rightarrow 2}^{1} \rightarrow D(1))$. The knowledge of $T$ and the decomposition of $G$ and $G^{-1}$ into $\psi$, $^*F, P, L$ 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 $K=Z_{q^i}$, $K=Z_{q^{i+1}}$ or $K=B_{n,i}$. 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 $ADEC_i(K)$ and $ADEC_i(K)$.

If Alice and Bob use $ADEC_i(K)$ they use twisted Diffie-Hellman protocol based on the platform $EG(Z_{q^i})$. 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 $EG(Z_{q^i})$ 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 $(a_1, a_2, ..., a_n)$ with the coordinates from $Z_{q^i}$ and matrix $B=(b(i,j))$ with the entries from $Z_{q^{i+1}}$.

In the case of $M_1$, Alice simply sends $M+B$ and the tuple $(d_1, d_2, ..., d_n)+(\sigma^{-1}(a_1), \sigma^{-1}(a_2), ..., \sigma^{-1}(a_n))$ 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 $(d_1, d_2, ..., d_n)+(\pi(\sigma^{-1}(a_1), \pi(\sigma^{-1}(a_2), ..., \pi(\sigma^{-1}(a_n)))$ 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 $(d_1, d_2, ..., d_n)+(\Delta(\pi(\sigma^{-1}(a_1)), \Delta(\pi(\sigma^{-1}(a_2)), ..., \Delta(\pi(\sigma^{-1}(a_n)))$ to Bob. He restore the transformation $A$ from $AGL_n(B_{n,i})$.

In $ADEC_2$ Alice and Bob conduct the inverse twisted Diffie-Hellman protocol within the platform $EG(Z_{q^i})$ twice and elaborate mutually inverse maps $X_i, Y_i, i=1,2$ such that $XY_i(x)=x$ for each $x$ in $(Z_{q^i})^n$. 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 $E_B = Y_i S F(S^{-1}) Y_i S L S^{-1}$ together with the decomposition into $Y_i, F, L$ and $S$ for the encryption of plaintext $p$ from $(Z_{q^i})^n$.

Alice decrypts it with her transformation $SL^{-1} S^{-1} X_i S^{-1} S^{-1} X_i^{-1}=E_a$. 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 $ADEC_i(K)$ there is an option to change twisted Diffie-Hellman protocols for the hidden Tahoma protocols with outputs from $^*ES(Z_s^2)$ (see [28]).

In the case of $ADEC_3(K)$ one can change each inverse twisted Diffie-Hellman protocol for the two inverse hidden tame homomorphism protocols with the outputs in $^*EG(Z_s^2)$. 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 $^*ES(Z_s^2)$ (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 $^*ES(Z_s^2)$.

REMARK 7.

Let $K$ be one of the commutative rings $Z_s^t, Z_s^{t-1}, F_s^{t-1}$ and $B_{s-1}$, assume that $^s\psi : K'^{n} \rightarrow K'^{n}$ be one of the maps $I$ (identity map), $S, P, D$ correspondingly.

Assume that $K$ and $Q$ are distinct elements of the set $\{Z_s^t, Z_s^{t-1}, F_s^{t-1}, B_{s-1}\}$ we can consider the cipher $DEC(K, Q)$ with the space of plaintexts $(Z_s^t)^n$ with the encryption procedure defined as the consecutive application of $G_1, ^s\psi, F_K, ^s\psi^{-1}G_2, ^s\psi, L_0, ^s\psi^{-1}$

where $F_k$ and $L_k$ are elements of $AGL_n(K)$ for $K$ of cardinality $2^{s-n-1}$ and $F_k = F^s$, $L_k = L^s$ for $F, L \in AGL_n(K)$ if $K = Z_s^t$.

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.

5. Conclusions.

Quadratic multivariate public rules can be used for the verification of the signature in time $O(n^2)$ 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 $Z_s^t\{x_1, x_2, \ldots, x_s\}$ acting naturally on the variety $(Z_s^t)^n, s > 1$.

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 $G$ and affine transformation $A$ from $AGL_n(Z_s^t)$ 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 $(\mathbb{Z}_2^s)^n$ where each column of the matrix $M$ has an odd number of odd residues modulo $2^i$ and all coordinates of the tuple $b$ are even residues.

Eulerian endomorphism $G_i$, $i=1,2$ has to act on $(\mathbb{Z}_2^s)^n$ as bijective transformations. Bob will use the map $F = G_1G_2A_1A_2$.

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 $(\mathbb{Z}_2^s)^n$ 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 $\mathbb{Z}_2^s$ and $\mathbb{Z}_2^{s-1}$, $\mathbb{Z}_2^{s-1}$ and finite field $F_2^{s-1}$ and $\mathbb{Z}_2^{s-1}$ 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 $AGL(\mathbb{Z}_2^s)$ for the $AGL(K)$, where $K$ is one of the rings $\mathbb{Z}_2^{s-1}$, $F_2^{s-1}$ and $B_{s-1}$.

New ciphers are defined via the algebraic systems with the operations of multiplications of two different commutative rings $\mathbb{Z}_2^s$ 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**


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


