INFORMATICA, 2014, Vol. 25, No. 2, 283–298

New Asymmetric Cipher of Non-Commuting Cryptography Class Based on Matrix Power Function

Eligijus SAKALAUSKAS, Aleksejus MIHALKOVICH*
Faculty of Fundamental Sciences, Kaunas University of Technology
Studentų g. 50, LT-51368 Kaunas, Lithuania
e-mail: eligijus.sakalauskas@ktu.lt, aleksejus.michalkovic@stud.ktu.lt

Received: January 2013; accepted: July 2013

Abstract. New asymmetric cipher based on matrix power function is presented. Cipher belongs to the class of recently intensively evolving non-commuting cryptography due to expectation of its resistance to potential quantum cryptanalysis.

The algebraic structures for proposed cipher construction are defined. Security analysis was performed and security parameters are defined. On the base of this research the secure parameters values are determined. The comparison of efficiency of microprocessor realization of proposed algorithm with different security parameters values is presented.

Key words: missing data, restoration, forward–backward parameter estimation, extrapolation.

1. Introduction

One of the first sources declaring non-commuting cryptography was (Sidelnikov *et al.*, 1993). In 200x the state of the art of this perspective field of investigation was presented in seminal book (Myasnikov *et al.*, 2008). In recent time non-commuting cryptographic primitives such as McEliece PKC are considered as a perspective trend of post quantum cryptography (McEliece, 1978). In 2007 authors published a new key agreement protocol based on matrix conjugator search problem in combination with matrix discrete logarithm function (Sakalauskas *et al.*, 2007). This key agreement protocol was named as STR (Sakalauskas, Tvarijonas, Raulynaitis) and was studied in detail in several sources available on web (Ottaviani *et al.*, 2011; Jacobs, 2011; Sracic, 2011). In 2012 it was concluded in Myasnikov and Ushakov (2012), that this algorithm does not provide strong security for quantum computers.

Continuing our research in non-commuting cryptography we present here a new asymmetric cipher based on matrix power function (MPF). MPF was previously used for key agreement protocol (Sakalauskas *et al.*, 2008) and asymmetric cipher construction (Sakalauskas and Luksys, 2007; Sakalauskas and Luksys, 2012).

*Corresponding author.

We expect, that the proposed asymmetric cipher has an effective realization in restricted computational environments as it was shown by Ottaviani *et al.* (2011) for STR key agreement protocol.

2. Preliminaries

Let $\boldsymbol{Z}_n = \{0, 1, \ldots, n-1\}$ be a finite ring of integers where the multiplication and addition are performed modulo n. These operations are associative and commuting and we will take it in mind below by default. It is well known, that if n is prime, then $\boldsymbol{Z}_n$ is a field. Conveniently, we denote a multiplicative group in $\boldsymbol{Z}_n$ consisting of integers relatively prime to n by $\boldsymbol{Z}_n^*$. We denote the order of $\boldsymbol{Z}_n^*$ by $|\boldsymbol{Z}_n^*|$ and it's value is determined by the value of Euler's totient function $\phi(n)$.

Since the group $\boldsymbol{Z}_n^*$ is multiplicative, the powering of its elements can be defined. Referencing to Carmichael's theorem (Carmichael, 1912) we can see, that for any element $g \in \boldsymbol{Z}_n^*$ the power x of an element g^x is in $\boldsymbol{Z}_{\lambda(n)}$, i.e $x \in \boldsymbol{Z}_{\lambda(n)}$, where $\lambda(n)$ is the Carmichael function. This function can be defined as the smallest positive integer λ, which satisfies the identity $g^{\lambda} = 1 \bmod n$ for all g coprime with n. Note, that $\boldsymbol{Z}_{\lambda(n)}$ is determined by the value of n.

At first we consider a general case. Let $\boldsymbol{S}$ be some abstract multiplicative commuting semigroup and assume, that powers of elements of $\boldsymbol{S}$ are in some commuting numerical ring $\boldsymbol{R}$ i.e.

$$\forall g, \quad g^x \in \boldsymbol{S}, \quad x \in \boldsymbol{R}.$$

It is clear, that characterization of $\boldsymbol{R}$ depends on the properties of semigroup $\boldsymbol{S}$ as it was shown in the case of $\boldsymbol{Z}_n^*$. Based on these facts we turn to definition of MPF as an action of $\boldsymbol{M}_{\mathrm{R}} \times \boldsymbol{M}_{\mathrm{R}}$ in $\boldsymbol{M}_{\mathrm{S}}$, where $\boldsymbol{M}_{\mathrm{R}}$ is a matrix ring and $\boldsymbol{M}_{\mathrm{S}}$ is a matrix semigroup defined over $\boldsymbol{R}$ and $\boldsymbol{S}$ respectively.

We define a matrix $Q = \{q_{ij}\}$ in a semigroup $\boldsymbol{M}_{\mathrm{S}}$ and name it as *base matrix*. We also define matrices $X = \{x_{ij}\}$ and $Y = \{y_{ij}\}$ in a ring $\boldsymbol{M}_{\mathrm{R}}$ and name them as *power matrices*. Hence $q_{ij} \in \boldsymbol{S}$, $x_{ij}, y_{ij} \in \boldsymbol{R}$. All of the defined matrices are square of order m.

Let matrix $Q = \{q_{ij}\}$ powered by matrix $Y = \{y_{ij}\}$ from the right be a matrix $C = \{c_{ij}\}$, i.e.

$$C = Q^Y, \tag{1}$$

where elements of C are computed by the formula

$$c_{ij} = \prod_{k=1}^{m} q_{ik}^{y_{kj}}. \tag{2}$$

In a similar way by powering matrix Q from the left by matrix $X = \{x_{ij}\}$ we obtain a matrix $D = \{d_{ij}\}$, i.e.

$$D = {}^X Q, \tag{3}$$

where elements of D are computed by the formula

$$d_{ij} = \prod_{k=1}^{m} q_{kj}^{x_{ik}}. \tag{4}$$

Furthermore we can use a combination of both functions to define a *two-sided matrix power function* or MPF by powering matrix Q from the left and right by matrices X and Y respectively. Denoting the result matrix by $E = \{e_{ij}\}$ we have the following MPF definition:

$$E = {}^{X}Q^{Y} \tag{5}$$

where according to (2) and (4) the elements e_{ij} are computed by the formula:

$$\begin{cases} q_{11}^{x_{11}y_{11}} \ldots q_{m1}^{x_{1m}y_{11}} q_{12}^{x_{11}y_{21}} \ldots q_{m2}^{x_{1m}y_{21}} \ldots q_{mm}^{x_{1m}y_{m1}} = e_{11}, \\ q_{11}^{x_{11}y_{12}} \ldots q_{m1}^{x_{1m}y_{12}} q_{12}^{x_{11}y_{22}} \ldots q_{m2}^{x_{1m}y_{22}} \ldots q_{mm}^{x_{1m}y_{m2}} = e_{12}, \\ \quad \vdots \\ q_{11}^{x_{m1}y_{1m}} \ldots q_{m1}^{x_{mm}y_{1m}} q_{12}^{x_{m1}y_{2m}} \ldots q_{m2}^{x_{mm}y_{2m}} \ldots q_{mm}^{x_{mm}y_{mm}} = e_{mm}. \end{cases} \tag{6}$$

It is clear, that the result matrices C, D and E are in $\boldsymbol{M}_{\mathrm{S}}$.

Since the base matrix Q is defined in $\boldsymbol{M}_{\mathrm{S}}$ we name it as a *platform semigroup*, and power matrices X and Y are defined in $\boldsymbol{M}_{\mathrm{R}}$ we name it accordingly as a *power ring*.

Let us now present two lemmas, which indicate important properties of MPF for cryptographic protocols construction (Sakalauskas and Luksys, 2007). We denote the ordinary matrix multiplication in $\boldsymbol{M}_{\mathrm{R}}$ by XY.

Lemma 1. *If* $\boldsymbol{R}$ *is commuting numerical semiring and* $\boldsymbol{S}$ *is commuting semigroup, then MPF defined by* (6) *is an action of* $\boldsymbol{M}_{\mathrm{R}} \times \boldsymbol{M}_{\mathrm{R}}$ *in* $\boldsymbol{M}_{\mathrm{S}}$ *satisfying the following identity*

$$\left({}^{X}Q\right)^{Y} = {}^{X}\left(Q^{Y}\right) = {}^{X}Q^{Y}.$$

Lemma 2. *If* $\boldsymbol{R}$ *is commuting numerical semiring and* $\boldsymbol{S}$ *is commuting semigroup, then MPF defined by* (6) *is an action of* $\boldsymbol{M}_{\mathrm{R}} \times \boldsymbol{M}_{\mathrm{R}}$ *in* $\boldsymbol{M}_{\mathrm{S}}$ *satisfying the following identity*

$${}^{X}\left({}^{U}Q^{V}\right)^{Y} = {}^{(XU)}Q^{(VY)}.$$

The construction of suggested asymmetric cipher is based on the conjecture, that MPF is a candidate one-way function (OWF). This means, that direct MPF value (i.e. matrix E) computation for given instances Q, X and Y in (5) is algorithmically effective while the inverse value computation to find any X and Y for instances Q and E is infeasible. We name the problem of finding matrices X and Y, satisfying equation (5) as *MPF problem*, when Q and E are given.

3. Asymmetric Cipher

Let the sender Bob be willing to encrypt a message M by receiver's Alice's public key, which can be decrypted by Alice's private key. According to the structure of the proposed cipher M is a matrix of order m with entries coded in binary form. This will be explained in example below.

Let Q be a public matrix selected from matrix semigroup $\boldsymbol{M}_{\mathrm{S}}$ and let Z_1 and Z_2 be two public non-commuting matrices selected from matrix ring $\boldsymbol{M}_{\mathrm{R}}$. The necessity of two non-commuting matrices will be explained below. Alice randomly selects non-singular secret matrix X in $\boldsymbol{M}_{\mathrm{R}}$ and computes a secret matrix U as a product of polynomials of Z_1 and Z_2 i.e. $U = \boldsymbol{P}_U(Z_1) \cdot \boldsymbol{P}_U(Z_2)$, when polynomial $\boldsymbol{P}_U()$ is secret and chosen at random. Alice's private key PrK_A is a pair of matrices (X, U), i.e. $PrK_A = (X, U)$. Her public key is a triplet of matrices A_1, A_2 and E, i.e. $PuK_A = (XZ_1X^{-1} = A_1,\ XZ_2X^{-1} = A_2,\ {}^{X}Q^{U} = E)$.

Bob takes Alice's public key PuK_A and performs a following encryption protocol:

1. Bob chooses randomly a non-singular matrix Y in $\boldsymbol{M}_{\mathrm{R}}$.
2. He selects a random secret polynomial $\boldsymbol{P}_V()$ and computes a secret matrix $V = \boldsymbol{P}_V(Z_1) \cdot \boldsymbol{P}_V(Z_2)$. Then he takes matrices A_1 and A_2 and computes a matrix $\boldsymbol{P}_V(A_1) \cdot \boldsymbol{P}_V(A_2) = XVX^{-1} = W$.
3. He raises matrix ${}^{X}Q^{U}$ to the obtained power matrix $W = XVX^{-1}$ on the left and obtains ${}^{XV}Q^{U}$ since $WX = XV$.
4. He raises the result matrix to the power matrix Y on the right and obtains ${}^{XV}Q^{UY} = K$. The obtained matrix K is used as a key to encrypt a message M and compute a ciphertext C.
5. Bob computes the ciphertext $C = K \oplus M$, where $\oplus$ is bitwise sum modulo 2 of all entries of matrices K and M.
6. Bob computes three matrices $(Y^{-1}Z_1Y = B_1,\ Y^{-1}Z_2Y = B_2,\ {}^{V}Q^{Y} = F)$ which we denote by encryptor ε and sends it to Alice together with C.

To decrypt Bob's message Alice does the following:

1. Using given matrices B_1 and B_2 Alice computes $\boldsymbol{P}_U(B_1) \cdot \boldsymbol{P}_U(B_2) = Y^{-1}UY$, since $U = \boldsymbol{P}_U(Z_1) \cdot \boldsymbol{P}_U(Z_2)$.
2. Alice raises matrix ${}^{V}Q^{Y}$ to the power $Y^{-1}UY$ on the right and then raises the result matrix to the power X on the left and hence obtains a matrix ${}^{XV}Q^{UY}$ which is the same encryption key K.
3. Alice can now decrypt a ciphertext C using encryption key K and relation

$$M = K \oplus C = K \oplus K \oplus M.$$

Note, that neither of matrices used to obtain an encryption key are commuting.

To illustrate the proposed cipher we give a following example:

- Alice and Bob agree on a public group $\boldsymbol{Z}_{15}^{*} = \{1, 2, 4, 7, 8, 11, 13, 14\}$, i.e. the platform group is defined over $\boldsymbol{S} = \boldsymbol{Z}_{15}^{*}$. Since $g^4 = 1$ for all $g \in \boldsymbol{Z}_{15}^{*}$, the power ring is defined over $\boldsymbol{R} = \mathbf{Z}_4$. Note, that all the actions in a platform group are performed modulo 15 and all the actions in a power ring are performed modulo 4.

- Alice and Bob agree on a public base matrix Q and two public non-commuting power matrices Z_1 and Z_2. Let

$$Q = \begin{pmatrix} 2 & 7 & 13 \\ 8 & 2 & 7 \\ 13 & 7 & 8 \end{pmatrix}, \qquad Z_1 = \begin{pmatrix} 3 & 3 & 1 \\ 3 & 2 & 2 \\ 0 & 0 & 3 \end{pmatrix}, \qquad Z_2 = \begin{pmatrix} 3 & 3 & 0 \\ 0 & 1 & 1 \\ 3 & 3 & 3 \end{pmatrix}.$$

- Alice chooses her secret non-singular power matrix

$$X = \begin{pmatrix} 3 & 0 & 3 \\ 3 & 3 & 3 \\ 2 & 3 & 2 \end{pmatrix}.$$

- Alice computes a secret power matrix U using a polynomial $P_U(x) = x^2 + 3x$. Hence

$$U = P_U(Z_1) \cdot P_U(Z_2) = \begin{pmatrix} 3 & 1 & 0 \\ 2 & 3 & 0 \\ 2 & 0 & 2 \end{pmatrix}.$$

- Alice calculates matrix E:

$$E = {}^{X}Q^{U} = \begin{pmatrix} 8 & 11 & 4 \\ 13 & 11 & 4 \\ 8 & 4 & 4 \end{pmatrix}.$$

- Alice calculates power matrices A_1 and A_2:

$$A_1 = XZ_1X^{-1} = \begin{pmatrix} 0 & 3 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix},$$

$$A_2 = XZ_2X^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 1 \\ 3 & 1 & 0 \end{pmatrix}.$$

- Alice has her private key $PrK_A = (X, U)$ and her public key $PuK_A = (A_1, A_2, E)$.

Since $S = \mathbf{Z}_{15}^*$ and operations in $\mathbf{Z}_{15}^*$ are taken modulo 15, the elements of matrix M can be coded by 4 bits and hence $M = \{m_{ij}\}$, where $m_{ij} \in \mathbf{Z}_{16}$.

Let Bob be willing to encrypt a message

$$M = \begin{pmatrix} 10 & 8 & 3 \\ 13 & 2 & 12 \\ 14 & 2 & 3 \end{pmatrix}.$$

Bob takes Alice's public key PuK_A and performs a following encryption protocol:

- He selects a random non-singular power matrix

$$Y = \begin{pmatrix} 0 & 1 & 3 \\ 1 & 2 & 1 \\ 3 & 0 & 2 \end{pmatrix}.$$

- Bob calculates power matrices V and W using a secret polynomial $P_V(x) = 2x^2 + x$. Hence

$$V = P_V(Z_1) \cdot P_V(Z_2) = \begin{pmatrix} 0 & 3 & 2 \\ 1 & 3 & 2 \\ 3 & 1 & 3 \end{pmatrix},$$

$$W = P_V(A_1) \cdot P_V(A_2) = XVX^{-1} = \begin{pmatrix} 2 & 2 & 3 \\ 3 & 1 & 2 \\ 1 & 0 & 3 \end{pmatrix}.$$

- Bob calculates the key matrix

$$K = {}^{W}E^{Y} = {}^{XV}Q^{UY} = \begin{pmatrix} 1 & 2 & 2 \\ 1 & 14 & 14 \\ 14 & 1 & 14 \end{pmatrix}.$$

- Bob calculates the ciphertext

$$C = K \oplus M = \begin{pmatrix} 11 & 10 & 1 \\ 12 & 12 & 2 \\ 0 & 3 & 13 \end{pmatrix}.$$

- Bob computes power matrices B_1, B_2 and the matrix F

$$B_1 = Y^{-1} Z_1 Y = \begin{pmatrix} 1 & 2 & 0 \\ 3 & 2 & 3 \\ 1 & 1 & 1 \end{pmatrix},$$

$$B_2 = Y^{-1} Z_1 Y = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 2 & 1 \\ 2 & 1 & 1 \end{pmatrix},$$

$$F = {}^{V}Q^{Y} = \begin{pmatrix} 11 & 2 & 1 \\ 14 & 1 & 14 \\ 1 & 7 & 14 \end{pmatrix}.$$

- Bob sends $\varepsilon = (B_1, B_2, F)$ and C to Alice.

The decryption is as follows:

- Alice computes the power matrix $Y^{-1}UY$ using her polynomial $P_U(x)$

$$Y^{-1}UY = P_U(B_1) \cdot P_U(B_2) = \begin{pmatrix} 0 & 2 & 0 \\ 0 & 1 & 1 \\ 3 & 0 & 3 \end{pmatrix}.$$

- Alice computes the key matrix

$$K = {}^{X}F^{Y^{-1}UY} = {}^{XV}Q^{UY} = \begin{pmatrix} 1 & 2 & 2 \\ 1 & 14 & 14 \\ 14 & 1 & 14 \end{pmatrix}.$$

- Alice decrypts the message

$$M = C \oplus K = \begin{pmatrix} 10 & 8 & 3 \\ 13 & 2 & 12 \\ 14 & 2 & 3 \end{pmatrix}.$$

4. Security Analysis

We will now introduce the matrix discrete logarithm function on the base of convenient discrete logarithm function. Note, that we do not consider both ordinary and matrix discrete logarithm problem (DLP) hard, since we will not use large semigroup $\boldsymbol{S}$ to define platform semigroup $\boldsymbol{M}_{\mathrm{S}}$.

Suppose, that matrix Q is defined over some cyclic group $\boldsymbol{G}$ i.e. $\boldsymbol{S} = \boldsymbol{G}$. Let the generator g of the group $\boldsymbol{G}$ be given. A discrete logarithm ld_g with the base of this generator of Q^Y can be applied to (1) to obtain

$$\mathrm{ld}_g Q^Y = (\mathrm{ld}_g Q)Y = \mathrm{ld}_g C \tag{7}$$

where $\mathrm{ld}_g Q$ and $\mathrm{ld}_g C$ mean, that the discrete logarithm is applied to all entries of matrices Q and C respectively. In the same way we can apply matrix discrete logarithm function to (3) i.e.

$$\mathrm{ld}_g {}^{X}Q = X(\mathrm{ld}_g Q) = \mathrm{ld}_g D. \tag{8}$$

Assume, that matrix $(\mathrm{ld}_g Q)^{-1}$ exists. Then by multiplying both sides of (7) by $(\mathrm{ld}_g Q)^{-1}$ we get

$$Y = (\mathrm{ld}_g Q)^{-1} \cdot \mathrm{ld}_g C.$$

The same is true for (8), i.e

$$X = \mathrm{ld}_g D \cdot (\mathrm{ld}_g Q)^{-1}.$$

Since we can apply matrix discrete logarithm function to (1) and (3) we can also apply it to (5) to get

$$\mathrm{ld}_g\, {}^X Q^Y = X(\mathrm{ld}_g Q)Y = XTY = \mathrm{ld}_g E, \tag{9}$$

where $T = \mathrm{ld}_g Q$.

The way to break the presented asymmetric cipher specification is to find matrices X and Y, when T and $\mathrm{ld}_g E$ are given. This problem is similar to well known NP-complete problem, namely multivariate quadratic (MQ) problem. We name the problem defined by (9) as *matrix MQ problem* (MMQ).

Let us consider the conditions under which the discrete logarithm can be applied to (5).

Let $\boldsymbol{S} = \boldsymbol{Z}_n^*$ be a non-cyclic group with n being a composite integer. According to Chinese remainder theorem, the group $\boldsymbol{Z}_n^*$ is isomorphic to the multiplicative group $\boldsymbol{Z}_p^* \times \boldsymbol{Z}_q^*$. Since $\boldsymbol{Z}_p^*$ and $\boldsymbol{Z}_q^*$ are cyclic groups, the generators of both groups can be found. The multiplicative group $\boldsymbol{Z}_p^* \times \boldsymbol{Z}_q^*$ is then isomorphic to the following direct product of two additive groups $\boldsymbol{Z}_{(p-1)} \times \boldsymbol{Z}_{(q-1)}$ with the isomorphism defined as

$$\varphi : \left(g_p^a, g_q^b\right) \to (a, b), \tag{10}$$

where g_p and g_q are generators of $\boldsymbol{Z}_p^*$ and $\boldsymbol{Z}_q^*$ respectively (Clifford and Preston, 1961). Hence the group $\boldsymbol{Z}_n^*$ is also isomorphic to $\boldsymbol{Z}_{(p-1)} \times \boldsymbol{Z}_{(q-1)}$. We can now use an isomorphism φ from $\boldsymbol{Z}_p^* \times \boldsymbol{Z}_q^*$ to $\boldsymbol{Z}_{(p-1)} \times \boldsymbol{Z}_{(q-1)}$ defined by (10) to find a discrete logarithm of the matrix Q, given that all elements q_{ij} are selected from $\boldsymbol{Z}_n^*$. In this case the complexity of MPF problem is defined by the complexity of several MMQ problems. We think, that we can make a conjecture, that if we prevent the MPF problem transformation to MMQ problem, then the complexity of such MPF problem will be rather higher than complexity of corresponding MMQ problem. The necessary conditions for this will be presented below. These conditions depend on the algebraic structure of S.

Let us consider a multiplicative semigroup $\boldsymbol{Z}_n = \{0, 1, \ldots, n-1\}$, where $n = pq$ is a composite integer and p, q are distinct odd primes with $p > q$. Semigroup $\boldsymbol{Z}_n$ contains a subgroup $\boldsymbol{Z}_n^*$ of order $\phi(n) = (p-1)(q-1)$. Let us construct a set $\boldsymbol{Z}_n^\sharp$ being a union of $\boldsymbol{Z}_n^*$ and some ideal $Id_q(\boldsymbol{Z}_n) = \{j = i \cdot q;\ i = 1, \ldots, p-1\}$ in $\boldsymbol{Z}_n$, i.e. $\boldsymbol{Z}_n^* \cup \mathrm{Id}_q(\boldsymbol{Z}_n) = \boldsymbol{Z}_n^\sharp$. It is easy to prove, that $\boldsymbol{Z}_n^\sharp$ is a semigroup under multiplication. Let $\boldsymbol{S} = \boldsymbol{Z}_n^\sharp$ and let $\boldsymbol{C}_1$ and $\boldsymbol{C}_2$ be two cyclic subgroups of $\boldsymbol{Z}_n^*$ having maximal order. Notice, that $\mathrm{Id}_q(\boldsymbol{Z}_n)$ is also a cyclic group of order $|\mathrm{Id}_q(\boldsymbol{Z}_n)| = (p-1)$. Hence the order of generators of $\mathrm{Id}_q(\boldsymbol{Z}_n)$ is $(p-1)$. We propose the elements of the base matrix Q to be chosen as generators in $\boldsymbol{C}_1$, $\boldsymbol{C}_2$ and $\mathrm{Id}_q(\boldsymbol{Z}_n)$.

In the case of cyclic subgroups $\boldsymbol{C}_1$ and $\boldsymbol{C}_2$ their orders and orders of their generators are defined by the Carmichael function $\lambda(n)$. We propose to choose $\boldsymbol{C}_1$ and $\boldsymbol{C}_2$ of maximal orders. In the case of $n = pq$ the Carmichael function is equal to $\lambda(n) = \mathrm{lcm}(p-1, q-1)$ where lcm stands for least common multiple. Since $\lambda(n) < \phi(n)$ if $\gcd(p-1, q-1) \neq 1$, the Carmichael function defines the maximal order of cyclic subgroups $\boldsymbol{C}_1$ and $\boldsymbol{C}_2$. We propose to use a composite integer n satisfying relation:

$$\lambda(n) = p - 1.$$

In this case $|\boldsymbol{C}_1| = |\boldsymbol{C}_2| = |\mathrm{Id}_q(\boldsymbol{Z}_n)| = \lambda(n)$ and hence the elements q_{ij} of matrix Q are of the same order $r = \lambda(n)$ and the power matrices X and Y are in the power ring $\boldsymbol{M}_\mathrm{R}$, where $\boldsymbol{R} = \boldsymbol{Z}_{\lambda(n)}$.

We can prevent the direct application of discrete logarithm function to (13) and related isomorphism by choosing at least one element of the matrix Q from $\mathrm{Id}_q(\boldsymbol{Z}_n)$. Since $\boldsymbol{Z}_n^\sharp$ is a semigroup, it has no isomorphism splitting it to the direct product of several cyclic groups with discrete logarithm function defined. In this case the discrete logarithm of the base matrix Q cannot be defined.

We consider the security of the presented cipher in the sense of Alice's private key PrK_A recovery from her public key PuK_A. This means, that an adversary must find matrices X and U when matrices Q, Z_1, Z_2, A_1, A_2 and E are given. To break the cipher adversary must find any matrices $\tilde{X}$ and $\tilde{U}$ satisfying equations:

$$\tilde{X} Z_1 \tilde{X}^{-1} = A_1, \tag{11}$$

$$\tilde{X} Z_2 \tilde{X}^{-1} = A_2, \tag{12}$$

$$^{\tilde{X}}Q^{\tilde{U}} = E, \tag{13}$$

such that for any matrices $V = P_V(Z_1) \cdot P_V(Z_2)$ and $Y \in \boldsymbol{M}_\mathrm{R}$ the following identity holds

$$^{XV}Q^{UY} = {}^{\tilde{X}V}Q^{\tilde{U}Y}. \tag{14}$$

Let us consider the protocol, suggested in Mihalkovich and Sakalauskas (2012). There only one matrix (we shall denote it by Z) is used for conjugation constrain in stead of matrices Z_1 and Z_2, i.e.

$$XZX^{-1} = A.$$

By powering both sides of Eq. (13) by Z on the right and A on the left and since $U = P_U(Z)$ and $XZ = AX$, we can get the following equation:

$$^{AX}Q^{UZ} = {}^{XZ}Q^{ZU} = {}^{A}E^{Z}.$$

Let us denote $P = {}^{Z}Q^{Z}$ and $H = {}^{A}E^{Z}$, obtaining the following equation:

$$^{X}P^{U} = H. \tag{15}$$

Since all elements of P and H are in $\mathrm{Id}_q(\boldsymbol{Z}_n)$, which is a cyclic group generated by its element g, the discrete logarithm of both sides of Eq. (15) can be taken, then:

$$X(\mathrm{ld}_g P)U = \mathrm{ld}_g H. \tag{16}$$

Note, that in the last equation we did not apply a discrete logarithm to matrix Q (since it is not possible), but nevertheless we obtained an MMQ problem to find unknown matrices X

and U. Hence as we can see the initial MPF problem can be reduced to an MMQ problem even if discrete logarithm of Q cannot be defined. The question is if the solution of Eq. (16) is a way to break the cipher, i.e. if it also satisfies Eq. (13). To give an appropriate answer to this question we must consider two cases:

- Matrix Z is invertible.
- Matrix Z is singular.

If matrix Z is invertible, then raising both sides of Eq. (15) to Z^{-1} on the right and to A^{-1} on the left we get Eq. (13). The inverse of matrix A exists, since it is similar to matrix Z. Hence in this case the solutions of Eq. (16) also satisfy Eq. (13) and an MPF problem can be reduced to an MMQ problem regardless of the choice of a base matrix Q and its discrete logarithm existence.

If matrix Z is singular, then matrices Z^{-1} and A^{-1} do not exist, which makes raising to these powers impossible. However in this case an adversary may calculate a matrix $\tilde{Z} = aZ + bI$, where I is the identity matrix and a and b are coefficients in $\mathbf{Z}_{\lambda(n)}$. Let matrix $\tilde{Z}$ be invertible for some fixed coefficients a and b. Since $\tilde{Z}$ commutes with Z it also commutes with matrix U. Furthermore, it can easily be shown, that $X\tilde{Z} = \tilde{A}X$, where $\tilde{A} = aA + bI$. An adversary can then use matrices $\tilde{A}$ and $\tilde{Z}$ to reduce Eq. (13) to Eq. (16). Hence an MPF problem can be reduced to an MMQ problem in case of a singular matrix Z. We name this attack as the *discrete logarithm attack*.

However if two non-commuting matrices Z_1 and Z_2 are used, then a non-trivial matrix (i.e. matrix not equal to bI) commuting with U cannot be found. In this case the reduction of Eq. (13) is not possible if matrices ${}^{Z_1}Q$ and ${}^{Z_2}Q$ do not have a discrete logarithm. Hence the necessary conditions to avoid discrete logarithm attack are the following:

- The platform matrix semigroup must be defined over $\mathbf{Z}_n^{\sharp}$.
- Matrices Z_1 and Z_2 must be non-commuting.
- Discrete logarithm of matrices Q, ${}^{Z_1}Q$ and ${}^{Z_2}Q$ must not be determined.

5. Security Parameters Definition and Their Secure Values Determination

The suggested protocol has two main security parameters: parameter n defining group $\mathbf{Z}_n^{\sharp}$ and the matrix order m. Since we obtain commutating matrices using polynomials while non-singular matrices X and Y can be chosen freely, then to determine main security parameters we are making reference to the following facts:

- The number of matrices commuting with a public matrix Z_1, defined over a power ring, should be at least 2^{80}. Every commuting matrix should be obtained using polynomials over $\mathbf{R}$ of matrix Z_1. The same should be valid for Z_2.
- The number of matrices conjugating with a public matrix Z_1, defined over a power ring should be at least 2^{80}. The same should be valid for Z_1.

Let us consider commutation and conjugation equations in a ring $\mathbf{Z}_r$, where $r = 2s$ is the value of a Carmichael function $\lambda(n)$ and s is prime. It was shown in Mihalkovich and

Sakalauskas (2012), that these equations can be considered separately in fields $\mathbf{Z}_2$ and $\mathbf{Z}_s$. The number of solutions of commutation and conjugation equations is equal to:

$$N = N_2 N_s,$$

where N_2 and N_s are numbers of solutions of the corresponding equation in fields $\mathbf{Z}_2$ and $\mathbf{Z}_s$.

Let us denote $Z_1 = Z$ for short and consider the commutation equation

$$ZX = XZ, \tag{17}$$

which is defined over the field $\mathbf{Z}_s$. Let us assume, that matrix Z is similar to Jordan matrix, i.e. it can be expressed in the following canonical Jordan form

$$Z = K^{-1} J_Z K \tag{18}$$

where J_Z is a Jordan matrix

$$J_Z = \begin{pmatrix} J_{k_1}(\mu_1) & & & 0 \\ & J_{k_2}(\mu_2) & & \\ & & \ddots & \\ 0 & & & J_{k_l}(\mu_l) \end{pmatrix} \tag{19}$$

$\mu_1, \mu_2, \ldots, \mu_l$ are distinct eigenvalues of Z, $J_{k_i}(\mu_i)$ are Jordan blocks

$$J_{k_i}(\mu_i) = \begin{pmatrix} \mu_i & 1 & & & 0 \\ & \mu_i & 1 & & \\ & & \mu_i & \ddots & \\ & & & \ddots & 1 \\ 0 & & & & \mu_i \end{pmatrix} \tag{20}$$

of order k_i and $k_1 + k_2 + \cdots + k_l = m$. Hence we get the following equation

$$K^{-1} J_Z K X = X K^{-1} J_Z K. \tag{21}$$

We can now multiply (21) by K on the left and by K^{-1} on the right to get

$$J_Z K X K^{-1} = K X K^{-1} J_Z. \tag{22}$$

Let us denote $\tilde{X} = K X K^{-1}$. Thus we get

$$J_Z \tilde{X} = \tilde{X} J_Z. \tag{23}$$

Then all matrices $\tilde{X}$ commuting with J_Z have a following form:

$$\tilde{X} = \begin{pmatrix} R_{k_1} & & & 0 \\ & R_{k_2} & & \\ & & \ddots & \\ 0 & & & R_{k_l} \end{pmatrix} \tag{24}$$

where matrices R_{k_i} have an upper regular form:

$$R_{k_i} = \begin{pmatrix} a_1 & a_2 & \cdots & a_{k_i-1} & a_{k_i} \\ & a_1 & a_2 & \cdots & a_{k_i-1} \\ & & a_1 & \ddots & \cdots \\ & & & \ddots & a_2 \\ 0 & & & & a_1 \end{pmatrix}. \tag{25}$$

We can now see from (25), that the block R_{k_i} has k_i different parameters $a_1, \ldots, a_{k_i}$. Since $|\boldsymbol{Z}_s| = s$ and $k_1 + k_2 + \cdots + k_l = m$ it is clear, that there are s^m different matrices commuting with J_Z. Hence by (24) and (25) we get all possible solutions of Eq. (17) by computing $X = K^{-1}\tilde{X}K$, where matrices $\tilde{X}$ are solutions of Eq. (23). We have proven the following proposition:

Proposition 1. *Let Z be a square matrix of order m defined over a field $\mathbf{Z}_s$. If Z is similar to Jordan matrix* (19)*, then Eq.* (17) *has exactly s^m solutions.*

Note, that not all matrices satisfying Eq. (17) have an inverse because zero value cannot be chosen for diagonal elements. If we omit zero diagonal elements we get exactly $s^{(m-l)}(p-1)^l$ invertible matrices satisfying Eq. (17).

It has been proven in Gantmacher (1966), that for matrix Z satisfying Proposition 1 every commuting matrix can be expressed as a polynomial of Z. The degree of polynomial is equal to m since there are m linearly independent matrices commuting with Z. Since matrices Z_1 and Z_2 have to be non-commuting we suggest, that these matrices should be similar to Jordan matrices (19) with distinct orders of Jordan blocks (20).

It can now easily be shown, that the number of solutions of (17) defined over a ring $\mathbf{Z}_s$ is r^m. Furthermore $s^{(m-l)}\phi^l(r)$ of these solutions are invertible.

The conjugation equations (11) and (12) can be considered in a similar way. Each of these equation has $s^{(m-l)}\phi^l(r)$ solutions if matrices $Z_s = Z \bmod s$ and $Z_2 = Z \bmod 2$ are similar to Jordan matrices (19).

Keeping this in mind the choice of parameters is as follows:

1. Since the platform matrix semigroup has to be defined over a non-cyclic semigroup $\boldsymbol{Z}_n^\sharp$ we choose $n = 3p$ which yields $\lambda(n) = p - 1$ and $\lambda(n) = 2(p-1)$. We suggest a prime number $p = 2q + 1$, where q is also prime. This yields $\lambda(n) = 2q$. The ideal of the group $\boldsymbol{Z}_n$ is $\mathrm{Id}_3(\boldsymbol{Z}_n) = \{3i;\ i = 1, 2, \ldots, 2q\}$ and $\boldsymbol{Z}_n^\sharp = \boldsymbol{Z}_n^* \cup \mathrm{Id}_3(\boldsymbol{Z}_n)$. Hence $\boldsymbol{S} = \boldsymbol{Z}_n^\sharp$ and $\boldsymbol{R} = \boldsymbol{Z}_{2q}$.

Table 1
Comparison of key lengths and of total count of bits for data storage.

n	m	$\lambda(n)$	Key length in bits		Memory requirements	Elementary operations
			Private key	Public key		
15	42	4	3612	14 112	32 380	12 296 844
21	33	6	3366	11 979	28 845	4670 721
33	25	10	2600	8750	24 665	1530 625
69	19	22	1900	6137	42 345	507 205
141	15	46	1440	4500	150 924	195 525

2. Since discrete logarithm of matrices Q, ${}^{Z_1}Q$ and ${}^{Z_2}Q$ must not exist we suggest, that one element of matrix Q should be chosen as a generator of $\mathrm{Id}_3(\boldsymbol{Z}_n)$ and all the other elements should be chosen as generators maximal order subgroups of $\boldsymbol{Z}_n^*$.
3. Since we consider Eqs. (11), (12) and (17) defined over a ring $\boldsymbol{Z}_{2q}$ and matrices Z_1 and Z_2 have to be non-commuting we must at least two distinct eigenvalues to construct Jordan matrices J_{Z_1} and J_{Z_2}. According to our conjectured requirement the number $r^{(m-2)}(q-1)^2$ must be greater than or equal to 2^{80}. Since $q-1=\frac{n-9}{6}$ and $r=\frac{n-3}{3}$ we get

$$m > \left\lceil \frac{82\ln 2 + 2(\ln(n-3) - \ln(n-9))}{\ln(n-3) - \ln(3)} \right\rceil,$$

where $\lceil\,\rceil$ is the ceiling function.
4. According to obtained security parameters estimates the following information should be stored for cipher protocol realization:
   - Multiplication and exponential tables to perform elementary operations with matrices in $\boldsymbol{M}_\mathrm{S}$.
   - Addition and multiplication tables to perform elementary operations with matrices in $\boldsymbol{M}_\mathrm{R}$.
   - Public matrix $Q \in \boldsymbol{M}_\mathrm{S}$.
   - Public non-commuting matrices $Z_1, Z_2 \in \boldsymbol{M}_\mathrm{R}$.
   - Private matrix $X \in \boldsymbol{M}_\mathrm{R}$ and a set of coefficients defined in $\boldsymbol{R}$ (private key).
   - Public matrices ${}^{X}Q^{U} \in \boldsymbol{M}_\mathrm{S}$ and $XZ_1X^{-1}, XZ_2X^{-1} \in \boldsymbol{M}_\mathrm{R}$ (public key).

Since addition and multiplication of two matrix elements are commuting, it is not necessary to store all elements of these tables. Hence we can store $\frac{(n-3)(n-2)}{2}$ elements for actions in $\boldsymbol{Z}_n^\sharp$ and $\frac{\lambda(n)(\lambda(n)+1)}{2}$ elements for actions in $\boldsymbol{Z}_{2q}$. The exponential table consists of $(n-3)\cdot\lambda(n)$ elements. Each matrix consists of m^2 elements and each element consists of $\lceil\log_2 n\rceil$ or $\lceil\log_2 \lambda(n)\rceil$ bits depending on a ring. Let us consider the first five suitable values of n: 15, 21, 33, 69 and 141. The results are shown in Table 1.

We can see from Table 1, that memory requirements are the lowest if $n=33$. After that memory requirements tend to increase. However, if we consider private and public keys lengths, we can see, that as parameter n increases, the keys tend to shorten. This means, that parameter n must be chosen taking into consideration memory requirements.

According to results presented in paper of Mihalkovich and Sakalauskas (2013) accepted for publication describing the algorithm presented in Mihalkovich and Sakalauskas (2012) the encryption time is less than of other known algorithm. The computational time estimation was performed with El-Gamal-2048 and ECC-521 encryption algorithms. Obtained results showed, that proposed algorithm in the case of $n = 33$ operates at least 8.6 times faster than these known existing algorithms. Furthermore, experimental results showed, that computational time tends to decrease when parameter n increases.

Note, however, that the suggested algorithm requires calculating a polynomial for matrices Z_1 and Z_2, whereas the algorithm presented in Mihalkovich and Sakalauskas (2012) uses only one matrix Z as an argument of a polynomial to be computed. Since most of computational time is used on calculating polynomials, the proposed algorithm in the case of $n = 33$ is 4.6 times faster than the traditional encryption algorithms mentioned above.

Concerning the effective realization of the proposed algorithm in computation restricted embedded systems we can make a conclusion, that $n = 69$ can be recommended, since this value provides a good compromise between the storage memory and computational time consumption.

6. Conclusions

The cryptanalysis of proposed cipher according to potential attacks is performed. According to this cryptanalysis the security parameters are defined. The estimation of security parameters values is obtained. According to these estimations the set of suitable security parameters values is presented.

Proposed cipher can be used in embedded systems having restricted computational resources. It is shown, that security parameters values can be chosen either minimizing the number of computation operations or minimizing program storage.

References

Carmichael, R.D. (1912). On composite numbers P which satisfy the Fermat congruence. *The American Mathematical Monthly*, 19(2), 363–385.

Clifford, A.H., Preston, G.B. (1961). *The Algebraic Theory of Semigroups*, Vol. I. American Mathematical Society, Rhode Island.

Gantmacher, F. (1966). *The Theory of Matrices*. Nauka, Moskow (in Russian).

Jacobs, K. (2011). *A survey of modern mathematical cryptology*. Available at: `http://trace.tennessee.edu/utk_chanhonoproj/1406`.

McEliece, R.J. (1978). *A Public-Key Cryptosystem Based on Algebraic Coding Theory*. DSN progress report, pp. 42-44.

Mihalkovich, A., Sakalauskas, E. (2012). Asymmetric cipher based on MPF and its security parameters evaluation. In: *Proceedings of the Lithuanian Mathematical Society, Ser. A*, *Lietuvos Matematikos Rinkinys*, Vol. 53, pp. 72–77.

Mihalkovich, A., Sakalauskas, E. (2013). New asymmetric cipher based on matrix power function and its implementation in microprocessors efficiency investigation. *Electronics and Electrical Engineering* (in press).

Myasnikov, A., Ushakov, A. (2012) *Quantum algorithm for the discrete Logarithm problem for matrices over finite Group rings*. Available at: `http://eprint.iacr.org/2012/574.pdf`.

Myasnikov, A., Shpilrain, V., Ushakov, A. (2008). *Group-Based Cryptography*. Birkhäuser, Switzerland.

Ottaviani, V., Zanoni, A., Regoli, M. (2011). *Conjugation as public key agreement protocol in mobile cryptography*. Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5741660&isnumber=5741585.

Sakalauskas, E., Luksys, K. (2007) *Matrix power s-box construction*. Available at: http://eprint.iacr.org/2007/214.pdf.

Sakalauskas, E., Luksys, K. (2012) Matrix power function and its application to block cipher s-box construction. *International Journal of Innovative Computing*, 8(4), 2655–2664.

Sakalauskas, E., Tvarijonas, P., Raulynaitis, A. (2007) Key agreement protocol (KAP) using conjugacy and discrete logarithm problems in group representation level. *Informatica*, 18, 115–124.

Sakalauskas, E., Listopadskis, N., Tvarijonas, P. (2008). Key agreement protocol (KAP) based on matrix power function. *Advanced Studies in Software and Knowledge Engineering*, ITHEA, 4(2), 92–96.

Sidelnikov, V., Cherepnev, M., Yaschenko, V. (1993). Systems of open distribution of keys on the basis of non-commutative semigroups. In: *Doklady Mathematics*, Russian Academy of Sciences, 48(2), 384–386.

Sracic, M. (2011). *Quantum circuits for matrix multiplication*. Available at: http://www.math.ksu.edu/reu/sumar/Quantum Algorithms.pdf.

E. Sakalauskas received PhD degree from Kaunas Polytechnical Institute in 1983. Currently he is a professor in Department of Applied Mathematics in Kaunas University of Technology. The scope of scientific interests is system theory, identification and cryptography. Over 50 papers were published in these fields.

In recent time his research interests are focused in cryptography. Some results were obtained in the following fields: one way functions construction based on the hard problems in non-commutative algebraic structures. Using this approach two new candidate one-way functions were proposed. Two such functions were proposed: one based on matrix discrete logarithm problem together with conjugation problem and other on matrix power function. On this base several original cryptographic protocols were proposed. The main trend of investigations is concentrated on post-quantum cryptographic systems construction potentially being resistant to quantum cryptanalysis. The main research results in cryptography were published in 17 papers.

A. Mihalkovich is a research assistant at Applied Mathematics Department of Kaunas University of Technology. The main research interest is connected with non-commutative cryptography.

Naujas asimetrinio šifravimo algoritmas paremtas MLF, priklausantis nekomutatyviosios kriptografijos rūšiai

Eligijus SAKALAUSKAS, Aleksėjus MICHALKOVIČ

Straipsnyje pateikiamas naujas asimetrinio šifravimo algoritmas, paremtas matricinio laipsnio funkcija (MLF). Šifras priklauso besivystančiai nekomutatyviosios kriptografijos rūšiai. Tikimasi, kad šis algoritmas yra atsparus patencialiai kvantinei kriptoanalizei.

Straipsnyje apibrėžiamos algebrinės struktūros, naudojamos šifravimo algoritmui konstruoti. Atlikta saugumo analizė bei apibrėžti saugumo parametrai. Remiantis šiais tyrimais, nustatytos saugios parametrų reikšmės. Pateikamas pasiūlyto algoritmo su skirtingomis saugumo parametrų reikšmėmis realizavimo mikroprocesoriuose efektyvumo palyginimas.