Lietuvos matematikos rinkinys
Proc. of the Lithuanian Mathematical Society, Ser. A
Vol. **53**, 2012, 72–77

ISSN 0132-2818
www.mii.lt/LMR/

Asymmetric cipher based on MPF and its security parameters evaluation

Aleksėjus Mihalkovič, Eligijus Sakalauskas

Kaunas University of Technology, Fundamentaliųjų mokslų fakultetas
Studentų str. 48, LT-51368 Kaunas
E-mail: aleksejus.michalkovic@stud.ktu.lt, eligijus.sakalauskas@ktu.lt

Abstract. The new asymmetric cipher algorithm based on matrix power function and matrix conjugation is presented. This algorithm is some alternative between known algorithms based on conjugacy problem, see e.g. Ko–Lee et al. and Anshel–Anshel–Goldfeld algorithm based on commutator concept. The security parameters are defined and their values are determined.

Keywords: asymmetric cyphering, matrix power function, one-way function.

1 Intoduction

One of the well known problems used in non-commuting cryptography is the conjugator search problem (CSP) in some non-commuting group $\boldsymbol{G}$. The problem is to find any element x satisfying equation $h = x^{-1}gx$, where h and g are public elements in $\boldsymbol{G}$. Two different approaches to CSP based encryption schemes were suggested. The first one is called the Ko–Lee et al. scheme (see [3]). It uses commuting subgroups concept, i.e. secret elements are chosen from two mutually commuting subgroups. Another approach called Anshel–Anshel–Goldfeld algorithm was suggested in [1]. This scheme uses the commutator concept for obtaining a shared key. It was shown by Spilrain and Ushakov in [6], that instead of solving CSP an adversary can try to solve a much easier decomposition problem. Hence the Anchel–Anchel–Goldfeld scheme is reckoned being more advanced. But nevertheless this scheme has a disadvantage, since it is using tuples of generators of private keys and hence is increasing memory requirements.

In this paper we suggest a new asymmetric encryption scheme, which is some alternative to the schemes mentioned above. Our scheme is based on matrix power function (see [4, 5]) and additional constraint of it's arguments, namely the conjugation equation. We reduce memory requirements for key storage.

2 MPF definition and properties

Matrix power function (MPF) was first introduced in [4]. This function is defined for square $m \times m$ matrix arguments X and Y and is denoted by

$$F_Q(X, Y) = {}^X Q^Y = E \tag{1}$$

where Q is a base $m \times m$ matrix and E is an MPF value $m \times m$ matrix with elements, defined by the system of equations:

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

To define MPF completely we assume that matrix Q is defined over a *platform group* $\boldsymbol{Z}_n^* = \{a\colon a \leqslant n,\ \gcd(a,n) = 1\}$. Then matrices X and Y must be chosen from matrix group over a *power ring* $\boldsymbol{Z}_r = \{0, 1, \dots, r-1\}$ as powers of elements of matrix Q. All the actions in groups $\boldsymbol{Z}_n^*$ and $\boldsymbol{Z}_r$ are performed modulo n and r respectively. It is shown in [5], that MPF is associative and the left-right actions identity ${}^X({}^UQ^V)^Y = {}^{(XU)}Q^{(VY)}$ holds.

In this paper we consider a non-cyclic platform group $\boldsymbol{Z}_n^*$, where a composite n can be expressed as $n = pq$ and p, q are prime factors. This yields a power ring $\boldsymbol{Z}_{\lambda(n)}$, where $\lambda(n)$ is the*Carmichael function*. This function is defined as the smallest positive integer t such that $a^t \bmod n \equiv 1$ for all a coprime with n. The choice of a power ring $\boldsymbol{Z}_{\lambda(n)}$ is obvious, since for all $a \in \boldsymbol{Z}_n^*$, $a^{\lambda(n)} = 1$, which means, that all powers can be reduced modulo $\lambda(n)$. If $n = pq$, then $\lambda(n) = lcm(p-1, q-1)$, where *lcm* stands for least common multiple.

3 Asymmetric cypher

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 calculation for instances Q, X and Y, when MPF system of equations (2) is supplemented with additional matrix conjugacy equation, is easy, while MPF inversion operation is hard. We will demonstrate how the sender (Bob) can encrypt a message, which can then be decrypted by the receiver (Alice).

Let Q be a public matrix selected over platform group and let A be a public matrix, selected over power ring. Alice has her private key – a pair of matrices $(X, U) = PrK_A$, where X is a randomly selected non-singular matrix and matrix U is a polynomial of A i.e. $U = P_U(A)$. Her public key is $PuK_A = \{{}^XQ^U, XAX^{-1}\}$. Alice uses her private key to decrypt Bob's message. Bob encrypts a message M by using Alice's PuK_A and performing following actions:

1. Bob chooses randomly a non-singular matrix Y and computes $Y^{-1}AY$;
2. Bob selects a random matrix $V = P_V(A)$ and computes ${}^VQ^Y$. His public key is $PuK_B = \{{}^VQ^Y, Y^{-1}AY\}$;
3. Bob uses Alice's public key to compute the following matrices:
   - Bob computes $XVX^{-1} = P_V(XAX^{-1})$;
   - Raises matrix ${}^XQ^U$ to the power XVX^{-1} on the left and obtains ${}^{XV}Q^U$;
   - Raises the result matrix to the power Y on the right and obtains ${}^{XV}Q^{UY}$, which is his encryption key matrix K_B;

   Since the elements of matrix K_B are random and uniformly distributed, Bob can now use an obtained key $K_B = {}^{XV}Q^{UY}$ to encrypt a message M.

4. The ciphertext is $C = K_B \oplus M$, where $\oplus$ stands for XOR operation. Bob sends $(C; PuK_B)$ to Alice.

To decrypt Bob's message Alice does the following:

1. Using matrix $Y^{-1}AY$ and polynomial $P_U(A)$ Alice computes $Y^{-1}UY = P_U(Y^{-1}AY)$;
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 her decryption key $K_A = {}^{XV}Q^{UY}$;
3. Since $K_A = K_B$ Alice can now decrypt a message using her decryption key K_A and a relation $M = K_A \oplus C$.

Note that only matrices U and V are commuting. This is the main advantage of the suggested protocol as compared with the protocols based on CSP. Note also, that, since Alice and Bob choose their matrices U and V as polynomials of A, only the coefficients of polynomials must be stored. This shortens private key lengths.

4 Security parameters values determination

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

1. The number of matrices, commuting with a public matrix A, defined over a power ring, should be at least 2^{80}. Every commuting matrix should be obtained using polynomials of matrix A;
2. The number of matrices, conjugating with a public matrix A, defined over a power ring, should be at least 2^{80}.

If these requirements are satisfied, then total scan of matrices X and Y is infeasible.

We start with the proof of an important proposition, which will prove useful for evaluation of security parameters. We denote the idempotents of the group $\boldsymbol{Z}_{pq}$ by 1_p and 1_q, i.e. $1_p \bmod p = 1$, $1_p \bmod q = 0$ and $1_q \bmod p = 0$, $1_q \bmod q = 1$. The existence and uniqueness of these elements follow from the extended Euclidian algorithm. If $A = \{a_{ij}\}$ and $a_{ij} \in \boldsymbol{Z}_{pq}$, then we define $A_p = \{a_{ij}\} \bmod p$, $A_q = \{a_{ij}\} \bmod q$. Note, that according to Chinese Remainder Theorem (CRT) $a_{ij} = [a_{ij} \bmod p] \cdot 1_p + [a_{ij} \bmod q] \cdot 1_q$.

Proposition 1. *If $A_pB_p = C_p$ and $A_qB_q = C_q$, then matrices A, B and C satisfy identity $AB = C$.*

Proof.

$$AB = (A_p1_p + A_q1_q)(B_p1_p + B_q1_q) = A_pB_p1_p + A_pB_q1_p1_q + A_qB_p1_q1_p + A_qB_q1_q = A_pB_p1_p + A_qB_q1_q,$$

since $1_p1_q = 0$. Since $A_pB_p = C_p$ and $A_qB_q = C_q$, we get $AB = C$

Hence the following corollaries are true:

Corollary 1. *If $A_pB_p = B_pA_p$ and $A_qB_q = B_qA_q$, then matrices A and B are commuting i.e. $AB = BA$.*

Corollary 2. $A^{-1} = A_p^{-1}1_p + A_q^{-1}1_q$.

Let us denote $r = \lambda(n)$ and assume that $r = 2s$ where s is prime. We can now evaluate the number of solutions of commutation and conjugation equations, defined over a ring $\boldsymbol{Z}_r$ using field theory and Proposition 1. We start with the commutation equation

$$AX = XA, \tag{3}$$

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

$$A = K^{-1}J_AK \tag{4}$$

where J_A is a Jordan matrix

$$J_A = \begin{pmatrix} \mu & 1 & 0 & \dots & 0 & 0 \\ 0 & \mu & 1 & \dots & 0 & 0 \\ 0 & 0 & \mu & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \mu & 1 \\ 0 & 0 & 0 & \dots & 0 & \mu \end{pmatrix} \tag{5}$$

and μ is an eigenvalue of A. Then all matrices, commuting with J_A, have a following form (called the regular upper form):

$$\begin{pmatrix} a_1 & a_2 & \dots & a_{m-1} & a_m \\ 0 & a_1 & \dots & a_{m-2} & a_{m-1} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_1 & a_2 \\ 0 & 0 & \dots & 0 & a_1 \end{pmatrix} \tag{6}$$

We can now see from (6), that there are m different parameters $a_1, a_2, \dots, a_m$. Since the order of the field $\boldsymbol{Z}_p$ $|\boldsymbol{Z}_p| = p$, it is clear, that there are p^m different matrices, commuting with J_A. Hence we get all possible solutions of equation (3) by computing $X = K^{-1}\widetilde{X}K$, where matrices $\widetilde{X}$ have the form (6). We have proven the following proposition:

Proposition 2. *Let A be a square matrix of order m defined over a field $\boldsymbol{Z}_p$. If A is similar to Jordan matrix* (5)*, then equation* (3) *has exactly p^m solutions.*

We denote the set of matrices, commuting with A (i.e. solutions of equation (3)), by $\boldsymbol{Com}(A)$ and the number of these matrices by $|\boldsymbol{Com}(A)|$. Note, that not all matrices of $\boldsymbol{Com}(A)$ have an inverse, because zero value cannot be chosen for diagonal elements. If we omit zero diagonal elements, we get exactly $p^{m-1}(p-1)$ invertible matrices, satisfying equation (3). We denote the set of these matrices by $\boldsymbol{Com}^*(A)$. It has been proven, that for matrix A, satisfying proposition (2), every commuting matrix can be expressed as a polynomial of A [2]. The degree of polynomial is equal to $m-1$, since there are m linearly independent matrices, commuting with A. The following corollaries of Proposition 1 give us the evaluation of number of solutions of equation (3), defined over a ring $\boldsymbol{Z}_r$:

Corollary 3. *If* $|\boldsymbol{Com}(A_2)| = N_2$ *and* $|\boldsymbol{Com}(A_s)| = N_s$*, then* $|\boldsymbol{Com}(A)| = N_2 N_s$.

Corollary 4. *If* A_2 *and* A_s *are similar to Jordan matrix* (5) *in fields* $\boldsymbol{Z}_2$ *and* $\boldsymbol{Z}_s$ *respectively, then* $|\boldsymbol{Com}(A)| = r^m$*. Furthermore,* $|\boldsymbol{Com}^*(A)| = r^{m-1}(s-1)$.

The conjugation equation i.e.

$$X^{-1}AX = B, \tag{7}$$

defined over the field $\boldsymbol{Z}_p$, can be considered in a similar way. It can be shown, that the conjugation equation is equivalent to commutation equation in the field $\boldsymbol{Z}_p$, if we consider only invertible matrices. Hence equation (7) has $p^{m-1}(p-1)$ solutions if defined over a field $\boldsymbol{Z}_p$ and $r^{m-1}(s-1)$ solutions if defined over a ring $\boldsymbol{Z}_r$.

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

1. For the platform group definition we seek to minimize the group order and to maximize the maximal orders of group elements. In this case the optimal solution is to choose $n = 3p$ with a prime number $p = 2s + 1$, where s is also prime. This yields $r = 2s$;
2. Since we consider equations (3) and (7) defined over a power ring $\boldsymbol{Z}_r$, the number $r^{m-1}(s-1)$ must be greater than or equal to 2^{80}. Since $s-1 = \frac{n-9}{6}$ and $r = \frac{n-3}{3}$ we obtain the following result:

$$m \geqslant \left\lceil \frac{81 \ln 2 + \ln(n-3) - \ln(n-9)}{\ln(n-3) - \ln(3)} \right\rceil$$

   where $\lceil\rceil$ is the ceiling function.
3. Since we want to make this ciphering algorithm usable in systems with limited resources, we must choose parameters values reducing memory and computation resources. We have chosen $n = 33$, since in this case the total amount of bits to store information is the smallest. This yields $m = 25$ and $\lambda(n) = 10$. Total amount of bits used to store information is 17840 bits which is approximately 2.2 kilobytes.

References

[1] I. Anshel, M. Anshel and D. Goldfeld. An algebraic method for public-key cryptography. *Math. Res. Lett.*, **6**:287–291, 1999. Available from Internet: http://mrlonline.org/mrl/1999-006-003/1999-006-003-003.pdf.

[2] F. Gantmacher. *The Theory of Matrices.* Nauka, Moscow, 1966.

[3] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. Kang and C. Park. New public-key cryptosystem using braid groups. *Lecture Notes in Computer Science*, **1880/2000**:166–183, 2000.

[4] E. Sakalauskas and K. Luksys. Matrix power s-box construction. *Crypt. ePrint Arch.*, (2007/214), 2007. Available from Internet: http://eprint.iacr.org/2007/214.pdf.

[5] E. Sakalauskas and K. Luksys. Matrix power function and its application to block cipher s-box construction. *Int. J. Inn. Comp., Inf. Contr.*, **8**(4):2655–2664, 2012.

[6] V. Spilrain and A. Ushakov. The conjugacy search problem in public key cryptography: unnecessary and insufficient. *Appl. Alg. Eng.*, **17**(3-4):285–289, 2006. Available from Internet: http://arxiv.org/pdf/math.GR/0411644.pdf.

REZIUMĖ

MLF paremtas asimetrinis šifras ir jo saugumo parametrų įvertinimas
A. Mihalkovich, E. Sakalauskas

Straipsnyje pristatomas naujas asimetrinio šifravimo algoritmas, kuris remiasi matricinio laipsnio funkcija bei matricų jungtinumo lygtimi. Šis algoritmas yra tam tikra alternatyva žinomiems algoritmams, kurie yra paremti jungtinumo uždaviniu, pvz. Ko–Lee algoritmui, ir Anshel–Anshel–Goldfeld algoritmui, kuris remiasi komutatoriaus idėja. Apibrėžiami saugumo parametrai bei nustatomos šių parametrų reikšmės.

Raktiniai žodžiai: asimetrinis šifravimas, matricinio laipsnio funkcija, vienkryptė funkcija.