INFORMATICA, 2017, Vol. 28, No. 3, 517–524

DOI: http://dx.doi.org/10.15388/Informatica.2017.142

Improved Asymmetric Cipher Based on Matrix Power Function Resistant to Linear Algebra Attack

Eligijus SAKALAUSKAS, Aleksejus MIHALKOVICH*

Faculty of Mathematics and Natural Sciences, Department of Applied Mathematics
Kaunas University of Technology, Studentų g. 50-324, Kaunas, Lithuania
e-mail: aleksejus.michalkovic@ktu.lt

Received: May 2016; accepted: August 2017

Abstract. In this paper we consider an improved version of earlier published asymmetric encryption protocol based on matrix power function (MPF). Recently, a linear algebra attack on earlier version of this protocol was found. This attack allows an attacker to break suggested protocol in polynomial time.

Here we show that the improved version of our encryption protocol is not vulnerable to the declared linear attack, while retaining its effective realization in embedded systems.

Key words: cryptography, matrix power function, asymmetric encryption, linear algebra attack.

1. Introduction

Matrix power function (MPF) was first introduced in late 2000's. This function proved to be useful for application in symmetric and asymmetric cryptography, since all actions are performed with small integers. This means that no additional co-processors have to be used to perform actions with large elements as opposed to RSA encryption or elliptic curves cryptography. Examples of these protocols can be found in Sakalauskas and Luksys (2012), Sakalauskas *et al.* (2008), Mihalkovich and Sakalauskas (2012), Sakalauskas and Mihalkovich (2014). The constructed protocols belong to non-commuting cryptography, which currently is of special interest to researchers. However, to our knowledge none of the protocols of this branch have been proven to be based on candidate one-way functions relying on NP-complete problems.

Formally, MPF can be defined as a function of matrix Q as a parameter and matrices (X, Y) as function arguments parameters denoted by $F_Q(X, Y)$ and expressed by the formula

$$F_Q(X, Y) = E$$

where E is a matrix representing the function value. In this paper we mainly focus on papers (Sakalauskas *et al.*, 2008; Mihalkovich and Sakalauskas, 2012; Sakalauskas *et al.*,

*Corresponding author.

2017) and (Liu *et al.*, 2016). In the latter paper authors present an attack based on linear algebra, which can be applied to protocols, presented in Sakalauskas *et al.* (2008) and Mihalkovich and Sakalauskas (2012) to break them in polynomial time. Our aim is to prove that the latest version of the so-called matrix power asymmetric cipher (MPAC), presented in Sakalauskas *et al.* (2017), is resistant to the declared attack, thus repairing the flaw found. Also, due to provable security of the latest version of MPAC protocol, we are making a conjecture that the recovery of decryption key is a hard problem.

2. Our Previous Work

Let us consider a commutative multiplicative semigroup $\boldsymbol{S}$ of multiplicative order t. Hence the powers of elements of $\boldsymbol{S}$ can be defined in a commutative numeric ring $\boldsymbol{Z}_t$, where addition and multiplication are defined modulo t. Previously in Sakalauskas *et al.* (2017) we defined this group as Sylow subgroup $\boldsymbol{\Gamma}_{p,n} \subset \boldsymbol{Z}_n$ of prime multiplicative order p combined with an ideal $\boldsymbol{J}_{p,n}$ given by $\boldsymbol{J}_{p,n} = j\boldsymbol{\Gamma}_{p,n}$, where j is an idempotent of the semigroup $\boldsymbol{Z}_p$. Due to prime multiplicative order p of the platform semigroup $\boldsymbol{\Gamma}^{\sharp}_{p,n} = \boldsymbol{\Gamma}_{p,n} \cup \boldsymbol{J}_{p,n}$, all the powers of elements of this algebraic structure are contained in a power field $\boldsymbol{Z}_p$.

We construct a semigroup of square $m \times m$ matrices with entries defined in semigroup $\boldsymbol{\Gamma}_{p,n}$ and denote it by $\boldsymbol{M}_{\boldsymbol{\Gamma}_{p,n}}$. Analogously we construct a ring of square $m \times m$ matrices $\boldsymbol{M}_{\boldsymbol{Z}_n}$ with entries of these matrices defined in numerical field $\boldsymbol{Z}_p$.

The two-sided MPF (or MPF for short) for a fixed parameter matrix $\boldsymbol{M}_{\boldsymbol{\Gamma}_{p,n}}$ is denoted as follows:

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

where matrices $X = \{x_{ij}\}$ and $Y = \{y_{ij}\}$ are defined in a power ring $\boldsymbol{M}_{\boldsymbol{Z}_p}$ and matrix $Q = \{q_{ij}\}$ is defined in a platform semigroup $\boldsymbol{M}_{\boldsymbol{\Gamma}_{p,n}}$. The entries of matrix $e = \{e_{ij}\}$ are calculated in the following way:

$$e_{ij} = \prod_{k=1}^{m}\prod_{l=1}^{m} q_{kl}^{x_{ik}y_{lj}}. \tag{2}$$

We will refer to matrices X and Y as *matrix powers* or *power matrices*, Q as *a base matrix* and E as *a matrix power value*.

The following main properties of MPF were presented and proven in Sakalauskas and Luksys (2012):

$$\left(^{X}Q\right)^{Y} = {}^{X}\left(Q^{Y}\right) = {}^{X}Q^{Y}, \tag{3}$$

$$^{X}\left(^{U}Q^{V}\right)^{Y} = {}^{(XU)}Q^{(VY)} = {}^{XU}Q^{VY}. \tag{4}$$

The idea of using MPF to perform asymmetric key exchange was initially proposed in Sakalauskas *et al.* (2008). The suggested protocol resembles a famous approach of Diffie and Hellman (1976).

According to the initial idea, two protocol parties, called Alice and Bob, agree on the public platform semigroup $\boldsymbol{Z}_p$ hence implying the power ring $\boldsymbol{Z}_{p-1}$. Both parties also agree on two sets of commuting matrices $\langle L\rangle \subset \boldsymbol{M}_{\boldsymbol{Z}_p}$ and $\langle R\rangle \subset \boldsymbol{M}_{\boldsymbol{Z}_p}$ generated by matrices L and R respectively. Furthermore the base matrix $Q \in \boldsymbol{M}_{\boldsymbol{Z}_p}$ is generated and published online.

To perform asymmetric key exchange Alice and Bob select their private keys – pairs of matrices $X \in \langle L\rangle$, $Y \in \langle R\rangle$ for Alice and $U \in \langle L\rangle$, $V \in \langle R\rangle$ for Bob. Their public keys are obtained using MPF, i.e. $A = {}^X Q^Y$ for Alice and $B = {}^U Q^V$ for Bob. Hence we have:

$$PrK_A = (X, Y), \qquad PuK_A = A,$$
$$PrK_B = (U, V), \qquad PuK_B = B,$$

where *PrK* and *PuK* denote private and public key respectively.

Upon exchanging their public keys, Alice and Bob can agree on a common key K calculated as follows:

$$K = {}^X B^Y = {}^{(XU)} Q^{(VY)} = {}^{(UX)} Q^{(YV)} = {}^U A^V,$$

since matrices X, U and Y, V commute.

However, it is shown in Liu *et al.* (2016), that this asymmetric key exchange is vulnerable to a certain linear algebra attack. Furthermore, their idea also holds in case of asymmetric encryption proposed in Mihalkovich and Sakalauskas (2012).

We now recall an improved version of MPAC presented in Sakalauskas *et al.* (2017).

Alice and Bob agree on the public platform semigroup $\boldsymbol{\Gamma}^{\sharp}_{p,n}$ hence implying the power field $\boldsymbol{Z}_p$. Furthermore, the base matrix $Q \in \boldsymbol{M}_{\boldsymbol{\Gamma}_{p,n}}$, as well as two non-commuting power matrices $Z_1, Z_2 \in \boldsymbol{M}_{\boldsymbol{Z}_p}$, are generated and published publicly for both parties to use.

To perform MPAC protocol Alice generates her private and public data using the following steps:

- She randomly selects non-singular secret matrix $X \in \boldsymbol{M}_{\boldsymbol{Z}_p}$;
- Alice selects a random function $u(x_1, x_2)$, where variables are non-commuting and coefficients are in $\boldsymbol{Z}_p$. Using this function Alice calculates matrix $U = u(Z_1, Z_2)$;
- She computes matrices $XZ_1X^{-1} = A_1$, $XZ_2X^{-1} = A_2$, ${}^X Q^U = E$.

Hence Alice obtained her data: a private key $PrK_A = (X, u(x_1, x_2))$, which she keeps a secret, and a public key $PuK_A = (A_1, A_2, E)$, which is certificated and published online.

To encrypt a secret message M Bob takes Alice's public key PuK_A and performs the following actions:

1. Bob chooses randomly a non-singular matrix $Y \in \boldsymbol{M}_{\boldsymbol{Z}_p}$;
2. He selects a random function $v(x_1, x_2)$, where variables are non-commuting and coefficients are in $\boldsymbol{Z}_p$. Using this function he calculates matrix $V = v(Z_1, Z_2)$. Then Bob takes matrices A_1 and A_2 and computes a matrix $W = v(A_1, A_2) = Xv(Z_1, Z_2)X^{-1} = XVX^{-1}$;

3. He raises matrix ${}^{X}Q^{U}$ to the obtained power matrix W 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, which can then be converted to a bit string;
5. Bob computes the ciphertext C = $K \oplus M$, where $\oplus$ is bitwise sum modulo 2 of all entries of bit stings 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.

Upon receiving the encryptor ε Alice performs the following actions to decrypt Bob's message:

1. She uses matrices B_1 and B_2 and her secret function $u(x_1, x_2)$ to compute $u(B_1, B_2) = Y^{-1}UY$;
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 $K = {}^{XV}Q^{UY}$ and converts it to a bitstring;
3. Alice can now decrypt a ciphertext C using encryption key K and relation

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

The essential modification of the protocol suggested in Mihalkovich and Sakalauskas (2012) is an extra matrix Z_2, which is published as a public parameter. In the next section we will show that this improvement of the initial protocol is enough to protect secret key from linear algebra cryptanalysis.

3. The Analysis Linear Algebra Attack

Let us briefly recall the attack presented in Liu *et al.* (2016).

To break the asymmetric key exchange proposed in Sakalauskas *et al.* (2008) an attacker has to solve the following system of equations:

$$\begin{cases} {}^{X}Q^{Y} = A, \\ XL = LX, \\ YR = RY, \end{cases} \tag{5}$$

where matrices Q, L, R, A are publicly known. Using convenient discrete logarithm function this system can be transformed to the following system:

$$\begin{cases} (ld_g Q)Y = X^{-1} ld_g A, \\ X^{-1}L = LX^{-1}, \\ YR = RY. \end{cases} \tag{6}$$

The latter system can be solved in polynomial time if at least one of matrices X, Y has an inverse. The algorithm for solving system (6) uses Kronecker product of matrices and stacking matrices X, Y into one long vector. Hence an extra restriction on private matrices has to be added. Namely, matrices X, Y, U, V have to be singular.

Another way to avoid revealing of private keys in protocol (Sakalauskas *et al.*, 2008) is to escape the discrete logarithm transformation of system (5). Hence the choice of the platform semigroup is vital to keep the protocol secure. As of now the platform group $\mathbf{\Gamma}^{\sharp}_{p,n}$ seems to be a safe choice to avoid linear algebra attack since, in general, there is no common generator of this semigroup, nor is this semigroup isomorphic to the Cartesian or free product of several cyclic semigroups. For more information on this semigroup the reader can turn to Sakalauskas *et al.* (2017), where the security of MPAC is considered.

In their paper (Liu *et al.*, 2016) have also suggested an idea of using non-commuting (semi)group to define a platform structure, i.e. the entries of base matrix Q should not commute. While this idea is interesting, it has to be thoroughly studied.

Furthermore, in Mihalkovich and Sakalauskas (2012) we presented an asymmetric encryption protocol, which unfortunately is not resistant to linear algebra attack described in Liu *et al.* (2016). The key-point of this attack is eliminating matrix U by replacing it with its polynomial expression. Hence the following system of equations has to be solved:

$$\begin{cases} ZX^{-1} = X^{-1}A, \\ ZY = YB, \\ (ld_g Q) \cdot \sum\limits_{i=0}^{m-1} a_i Z^i = X^{-1} \cdot (ld_g E). \end{cases} \tag{7}$$

The authors of the attack have shown that this can be done in polynomial time.

However, in Sakalauskas and Mihalkovich (2014) and Sakalauskas *et al.* (2017) we have improved our protocol by choosing a safer platform semigroup and adding an extra public parameter, namely a power matrix Z_2. The latter improvement is useful since the matrix U can now be calculated using an abstract random function $u(x_1, x_2)$. This comes from the structure of public data, namely matrices A_1, A_2, B_1, B_2 of both parties of the protocol, since

$$XZ_1X^{-1} = A_1, XZ_2X^{-1} = A_2,$$
$$Y^{-1}Z_1Y = B_1, Y^{-1}Z_2Y = B_2$$

and hence

$$u(B_1, B_2) = Y^{-1}u(Z_1, Z_2)Y = Y^{-1}UY,$$
$$v(A_1, A_2) = Xv(Z_1, Z_2)X^{-1} = XVX^{-1}$$

regardless of functions $u(x_1, x_2)$ and $v(x_1, x_2)$ respectively. An important moment here is the arbitrary structure of these private functions, i.e. these functions can be obtained using any combination of additions and multiplications of scalar non-commuting variables x_1, x_2. For more clarity let us present several examples of these functions:

$$x_1x_2 + 2x_2x_1; \; 3x_1x_2x_1 + x_1 + 2x_2 + x_2x_1; \; \big(x_1^2 + 3x_1 + 2\big)\big(x_2^3 - 2x_2^2 - 1\big).$$

As we can see the exact expressions of private functions are limited only by imagination of Alice and Bob and play no part in the execution of the MPAC protocol. However, on the attacker's side this unknown structure of private functions is an obstacle, which keeps him from eliminating matrix U. Furthermore, the length of coefficients vector in now unbounded since the space of all possible private functions is infinite, i.e. functions like $x_1x_2x_1$, $x_2x_1x_2$, $x_1x_2^2x_1^3x_2^4x_1$ as well as their combinations are a legitimate choice.

Note that the suggestion of using singular matrices X, Y, U, V as private key is not valid in case of MPAC protocol due to conjugation constrains, i.e. matrices X and Y have to be invertible. Hence the security of MPAC protocol now relies on the correct choice of platform semigroup and the unknown structure of the private functions $u(x_1, x_2)$ and $v(x_1, x_2)$ respectively.

4. Conclusions

In our paper we presented an analysis of a certain attack suggested in Liu *et al.* (2016). While avoidance of this attack for asymmetric key exchange was suggested by authors themselves, the case of asymmetric encryption is more complicated. The essence of linear algebra attack on the early version of MPAC is elimination of the private matrix U due to its polynomial structure, which is publicly known.

We also analysed the resistance to this attack of improved version of Matrix Power Asymmetric Cipher (MPAC) suggested in Sakalauskas *et al.* (2017). Based on performed analysis we can see that the security of this protocol relies on the following facts:

- An attacker has to solve the so-called MPF problem with conjugation constraints;
- By choosing a platform semigroup $\mathbf{\Gamma}^{\sharp}_{p,n}$ the transformation of MPF problem using discrete logarithm function can be avoided;
- By adding an extra matrix Z_2 as a public parameter matrices U and V can be calculated using arbitrary random functions. The space of these functions is unbounded.

So far we do not know the methods of the solution of systems defined by initial MPF equations, since they are not custom systems of algebraic equations. It is rather a system of power equations, where unknown variables are the powers of certain elements in semigroup. Furthermore, the unknown structure of private function is an extra factor, which has to be considered as well.

References

Diffie, W., Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6), 644–654.

Liu, J., Zhang, H., Jia, J. (2016). A linear algebra attack on the non-commuting cryptography class based on matrix power function. In: *International Conference on Information Security and Cryptology*. Springer, Cham, pp. 343–354.

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

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., Mihalkovich, A. (2014). New asymmetric cipher of non-commuting cryptography class based on matrix power function. *Informatica*, 25(2), 283–298.

Sakalauskas, E., Listopadskis, N., Tvarijonas, P. (2008). Key agreement protocol (KAP) based on matrix power function. In: *Advanced Studies in Software and Knowledge Engineering*. Institute of Information Theories and Applications FOI ITHEA, pp 92–96.

Sakalauskas, E., Mihalkovich, A., Venčkauskas, A. (2017). Improved asymmetric cipher based on matrix power function with provable security. *Symmetry*, 9(1), 9. doi:10.3390/sym9010009.

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 received PhD degree from Kaunas University of Technology in 2015. Currently he is a lecturer in Department of Applied Mathematics in Kaunas University of Technology. The main research interest is connected with non-commutative cryptography.