Lietuvos matematikos rinkinys
Proc. of the Lithuanian Mathematical Society, Ser. A
DOI: 10.15388/LMR.A.2018.02

ISSN 0132-2818
Vol. **59**, 2018
pages 7–12

# On the associativity property of MPF over $M_{16}$

**Aleksejus Mihalkovich**

*Department of Fundamental Sciences, Kaunas University of Technology*
Studentų str. 48, LT-51367 Kaunas, Lithuania
E-mail: aleksejus.michalkovic@ktu.lt

**Abstract.** The objective of this paper is to find suitable non-commuting algebraic structure to be used as a platform structure in the so-called matrix power function (MPF). We think it is non-trivial and interesting problem could be useful for candidate one-way function (OWF) construction with application in cryptography. Since the cornerstone of OWF construction using non-commuting algebraic structures is the satisfiability of certain associativity conditions, we consider one of the possible choices, i.e. the group $\boldsymbol{M}_{16}$, explore its basic properties and construct templates to use in our future work.

**Keywords:** matrix power function (MPF), one-way function (OWF), non-commuting algebraic structures.

## 1 Introduction

MPF is the function that computes the matrix obtained by powering some given matrix by two numerical matrices: one from the left and the other from the right. It is somewhat similar to the matrix multiplication by two matrices from the left and right, respectively. The matrix that is powered is named the base matrix and the matrices that are powering the base matrix are named power matrices. In general, the base matrix can be defined over the (semi)group $\boldsymbol{S}$ and power matrices, over the (semi)ring $\boldsymbol{R}$. Base matrices are defined in a certain matrix semigroup $\boldsymbol{M_S}$ and power matrices in a certain matrix semiring $\boldsymbol{M_R}$.

$\boldsymbol{S}$ is named a *platform (semi)group*, which according to the MPF definition, is a multiplicative, and $\boldsymbol{R}$ is an *exponent (semi)ring*. So far, all the matrices in the MPF construction were defined over certain commutative algebraic structures, namely, the base matrix $W$ was defined over the commutative numerical (semi)group $\boldsymbol{S}$ and power matrices $X$ and $Y$ over the commutative numerical ring $\boldsymbol{R}$. Formally one-sided MPFs as well as two-sided MPF (or simply MPF for short) can be defined by the following expressions:

$$^{X}W = D_L, (d_L)_{ij} = \prod_{k=1}^{m} w_{kj}^{x_{ik}}; \tag{1}$$

$$W^{Y} = D_R, (d_R)_{ij} = \prod_{k=1}^{m} w_{ik}^{y_{kj}}; \tag{2}$$

$$^{X}W^{Y} = D, d_{ij} = \prod_{l=1}^{m}\prod_{k=1}^{m} w_{lk}^{x_{il}\cdot y_{kj}}. \tag{3}$$

For more information of the MPF and its application we recommend papers [3, 4] and [5]. Here we present the following definition of MPF problem:

**Definition 1.** The MPF problem is to find matrices $X$ and $Y$ in (3), when the matrices $W$ and $D$ are given.

In general, MPF is a function $F(X,Y) : \boldsymbol{M_R} \times \boldsymbol{M_S} \times \boldsymbol{M_R} \to \boldsymbol{M_S}$. Throughout this paper we use the notation $\mathrm{MPF}_{\boldsymbol{S}}^{\boldsymbol{R}}$ to define an MPF over platform semigroup $\boldsymbol{S}$ and exponent semiring $\boldsymbol{R}$ as well as corresponding MPF problem defined over these algebraic structures.

It is important to note that recently a successful attempt to solve an MPF problem using linear algebra has been made in [2]. It was shown, that in case of commuting platform group $\boldsymbol{Z}_n$, where a composite integer $n$ is a product of two primes the corresponding MPF problem is solvable in polynomial time if any of the matrices $X, Y, U, V$ has an inverse. The authors also proposed some improvements to fix the flaws found.

Due to this recent attack we focus our research on exploring non-commuting structures for application to MPF as a platform structure. Here we consider one of the possible choices, i.e. the group $\boldsymbol{M}_{16}$, and discuss its application to cryptography using MPF.

## 2 The definition of the group $\boldsymbol{M}_{16}$ and its basic properties

In their paper the authors of [1] discussed the automatic realization of Galois groups of order 16. They considered ten distinct groups and distinguished seven indecomposable non-commuting groups. One of those seven groups is called *the modular group* $\boldsymbol{M}_{16}$ and will be considered in this paper.

The group $\boldsymbol{M}_{16}$ is defined as follows:

$$\boldsymbol{M}_{16} = \left\langle a, x \,\middle|\, a^8 = e, x^2 = e, xax^{-1} = a^5 \right\rangle, \tag{4}$$

where two generators $a$ and $x$ do not commute and $e$ is a neutral element of the group. Note, that the group $\boldsymbol{M}_{16}$ is non-commuting and hence is not isomorphic to the Cartesian product $\boldsymbol{Z}_8 \times \boldsymbol{Z}_2$. In fact $ax = xa^5$ and $a^5x = xa$. These equalities follow directly from definition of $\boldsymbol{M}_{16}$ since $x = x^{-1}$.

Let us write down all the elements of $\boldsymbol{M}_{16}$:

$$\boldsymbol{M}_{16} = \{e, x, a, xa, a^2, xa^2, a^3, xa^3, a^4, xa^4, a^5, xa^5, a^6, xa^6, a^7, xa^7\}. \tag{5}$$

Hence the cardinality of $\boldsymbol{M}_{16}$ is $|\boldsymbol{M}_{16}| = 16$. Note, that any element of the form $a^p x$ is represented by a certain element of the form $xa^p$ depending on the parity of $p$, e.g. $a^6x = xa^6$, $a^7x = xa^3$.

The product of two elements $x^\alpha a^k, x^\beta a^n \in \boldsymbol{M}_{16}$ is calculated as follows:

$$\left(x^\alpha a^k\right) \cdot \left(x^\beta a^n\right) = \begin{cases} x^{\alpha+\beta}a^{k+n}, & \text{if } k \text{ is even;} \\ x^\alpha a^{k+n}, & \text{if } k \text{ is odd and } \beta = 0; \\ x^{\alpha+1}a^{k+n+4}, & \text{if } k \text{ is odd and } \beta = 1. \end{cases} \tag{6}$$

The case of $\beta = 0$ is trivial. If $\beta = 1$, the proof of this formula relies on the identities $a^5x = xa$ and $(a^5)^k = a^{4k}a^k$, resulting in an extra summand of 4 if $k$ is odd.

The formula for calculating the exponent of an arbitrary element can be derived from formula (6) and looks as follows:

$$\left(x^{\alpha}a^{k}\right)^{n} = \begin{cases} a^{nk}, & \text{if } \alpha = 0; \\ x^{n}a^{nk}, & \text{if } \alpha = 1 \text{ and } k \text{ is even}; \\ x^{n}a^{nk+4[\frac{n}{2}]}, & \text{if } \alpha = 1 \text{ and } k \text{ is odd}. \end{cases} \tag{7}$$

The inverse element is defined in the following way:

$$\left(x^{\alpha}a^{k}\right)^{-1} = \begin{cases} a^{-k}, & \text{if } \alpha = 0; \\ xa^{4-k}, & \text{if } \alpha = 1 \text{ and } k \text{ is odd}; \\ xa^{-k}, & \text{if } \alpha = 1 \text{ and } k \text{ is even}, \end{cases} \tag{8}$$

where negative powers of generator $a$ are reduced modulo 8, i.e. $-3 \equiv 5 \mod 8$.

The validity of this formula can be verified by multiplying the corresponding elements in their general form.

By considering the multiplicative orders of the elements of $\boldsymbol{M}_{16}$ we can derive an important cyclic subgroup of multiplicative order 8:

$$\langle xa \rangle = \left\{e, xa, a^2, xa^3, a^4, xa^5, a^6, xa^7\right\}. \tag{9}$$

The group $\boldsymbol{M}_{16}$ also has a subgroup of order 8 generated by $a$. We denote this subgroup by $\langle a \rangle$. It is clear, that each subgroup contains a center $\boldsymbol{C}$ and all other elements have multiplicative order 8. Hence we consider the set

$$\boldsymbol{A} = \langle xa \rangle \cup \langle a \rangle. \tag{10}$$

Note, that the elements of $\boldsymbol{A}$ do not form a multiplicative group since the closure property is not satisfied. However, since we consider the set $\boldsymbol{A}$ as a subset of the group $\boldsymbol{M}_{16}$, the latter fact is of no importance to us.

## 3 The application of the group $\boldsymbol{M}_{16}$ to MPF

Using elements of set $\boldsymbol{A}$ we define a matrix $W$ which has the following form:

$$W = \begin{pmatrix} xa^{w_{11}} & a^{w_{12}} & \dots & a^{w_{1,m-1}} & xa^{w_{1m}} \\ a^{w_{21}} & a^{w_{22}} & \dots & a^{w_{2,m-1}} & a^{w_{2m}} \\ \dots & \dots & \dots & \dots & \dots \\ a^{w_{m-1,1}} & a^{w_{m-1,2}} & \dots & a^{w_{m-1,m-1}} & a^{w_{m-1,m}} \\ xa^{w_{m1}} & a^{w_{m2}} & \dots & a^{w_{m,m-1}} & xa^{w_{mm}} \end{pmatrix}. \tag{11}$$

We will call this matrix a *corner matrix* and fix it as a base matrix for MPF function.

It is important to note, that for two arbitrary commuting matrices $X$ and $U$ we have:

$$\begin{gathered} {}^{U}\left({}^{X}W\right) \neq {}^{X}\left({}^{U}W\right) \neq {}^{UX}W \\ \left(W^{X}\right)^{U} \neq \left(W^{U}\right)^{X} \neq W^{XU}. \end{gathered} \tag{12}$$

Furthermore, for two arbitrary matrices $Z$ and $Y$ we have:

$$\left({}^{Z}W\right)^{Y} \neq {}^{Z}\left(W^{Y}\right). \tag{13}$$

Let us consider the key exchange protocol presented in [4]. We present it here in a general form:

1. Two parties Alice and Bob agree on a commutative platform group $\boldsymbol{G}$ with multiplicative order $ord(\boldsymbol{G})$ and a public square matrix $W$ with entries randomly selected from $\boldsymbol{G}$.
2. Alice and Bob agree on two sets of commuting matrices $Mat(L)$ and $Mat(R)$, where $L$ and $R$ are generators of the defined sets. Entries of these matrices are randomly selected from the numerical ring $\boldsymbol{Z}_{ord(\boldsymbol{G})}$.
3. Alice selects two matrices $X \in Mat(L)$ and $Y \in Mat(R)$ as her private key and publishes her public key $A = {}^{X}W^{Y}$.
4. Bob selects two matrices $U \in Mat(L)$ and $V \in Mat(R)$ as his private key and publishes his public key $B = {}^{U}W^{V}$.
5. Using shared information Alice and Bob agree on a common key ${}^{U}A^{V} = {}^{X}B^{Y}$.

Due to recent attack [2] we aim to switch to a non-commutative platform group $\boldsymbol{M}_{16}$. Hence we have to modify the initial protocol so that valid key exchange would be possible.

Note that the MPF defined over $\boldsymbol{M}_{16}$ is nor associative, nor one-way associative in general case as shown above in (12) and (13). Hence we have to define templates for generation of base matrix $W$ and all power matrices $X, Y, U, V$.

We first consider the matrix $W$ and split it to two parts, namely $W_x = \{x^{\alpha_{ij}}\}$ and $W_a = \{a^{k_{ij}}\}$. Note, that due to the properties of $\boldsymbol{M}_{16}$ we have $\alpha_{ij} \in \boldsymbol{Z}_2$ and $k_{ij} \in \boldsymbol{Z}_8$. Furthermore, looking at the structure of the set $\boldsymbol{A}$ defined by (9) and (10) we see, that if $\alpha_{ij} = 1$, then $k$ is odd. Hence we choose the powers $k_{ij}$ of matrix $W_a$ in the following way:

$$k_{ij} = \alpha_{ij} \cdot (2r_{ij} + 1) + (1 - \alpha_{ij}) \cdot s_{ij}, \tag{14}$$

where $r_{ij}$ and $s_{ij}$ are random positive integers less than 4 and 8 respectively. The corner matrix $W = W_x \odot W_a$, where $\odot$ denotes hadamard product of matrices $W_x$ and $W_a$. This template guarantees, that each entry of matrix $W$ $w_{ij} \in \boldsymbol{A}$.

We now consider private keys of both parties, i.e. pairs of matrices $(X, Y)$ and $(U, V)$. Since MPF is associative if the platform (semi)group is commutative, one of possible choices of private keys are matrices with even entries. More specifically, either matrices $X$ and $U$ or $Y$ and $V$ may contain even entries whereas the other pair of commuting matrices may be chosen freely. Hence we define the following template:

**Template 1**.

(a) Choose matrix $X$ with even entries and select matrix $Y$ freely;

(b) Choose matrix $X$ freely and select matrix $Y$ with even entries.

However, this trivial approach has a fundamental flaw, i.e. it eliminates all non-commuting elements and hence endangers the security of key exchange.

To define suitable templates we consider the following assumptions:

- We perform actions left-to-right, i.e. public keys are $A = ({}^{X}W)^{Y}$ for Alice and $B = ({}^{U}W)^{V}$ for Bob;

- The entries of public key matrices are commutative.

An important aspect to note is the fact, that we aim to remove non-commuting elements after performing actions, not before it as in the case of Template 1. Two other templates are possible:

**Template 2**. Choose matrix $X$ in such a way, that $x_{i1} + x_{im} \equiv 0 \mod 2$. Select commuting matrix $Y$ freely.

**Template 3**.

1. Select $X$ in such a way, that $X + T \equiv O \mod 2$, where $T$ is an arbitrary fixed matrix and $O$ is a zero matrix.
2. Choose matrix $Y$ in such a way, that $y_{1j} + y_{mj} \equiv 0 \mod 2$.

Both of these templates can be successfully implemented using polynomials, i.e. for an arbitrary fixed matrix $T$ any odd power of this matrix satisfies Template 3.1 as well as commuting with $T$ itself. Alternatively any linear combination of odd powers can be used. Furthermore, since $2T \equiv O \mod 2$ any powers of this matrix may be considered as well.

Another fact to notice is that for an arbitrary fixed matrix $Z$ satisfying Template 2 the polynomial $P_n(Z) = 2c_0I + c_1Z + c_2Z^2 + \cdots + c_nZ^n$ preserves the desired property. The same is true for Template 3.2.

Hence we make the following modifications of the initial key exchange protocol

- On step 1 of the initial protocol Alice and Bob agree on the group $\boldsymbol{M}_{16}$, which implies the numerical power ring $\boldsymbol{Z}_8$. Parties also agree on a corner matrix $W$.
- On step 2 both parties agree on a Templates 2 or 3 and public matrices $M_L$ and $M_R$ satisfying the chosen template. Private key matrices are calculated using polynomials as specified above.
- On steps 3 and 4 parties calculate public key matrices and the common key by performing operations left-to-right.

## 4 Discussions

The future work involves a more detailed study of the latter templates, i.e. exploring the structure of public keys and the common key. Furthermore, it remains an open problem if the both Templates 2 and 3 provide the same security for key exchange protocol considered in this paper.

## References

[1] H. Grundman and T. Smith. Automatic realizability of galois groups of order 16. *Proc. Am. Math. Soc.*, **124**(9):2631–2640, 1996.

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

[3] A. Mihalkovich and E. Sakalauskas. Asymmetric cipher based on MPF and its security parameters evaluation. *Liet. matem. rink. Proc. LMS, Ser. A*, **53**:72–77, 2012.

[4] E. Sakalauskas and K. Luksys. The matrix power function and its application to block cipher s–box construction. *Int. J. Inn. Comp., Inf. Cont. (IJICIC)*, **8**(4), 2012.

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

REZIUMĖ

**Apie MLF, apibrėžtos virš $M_{16}$, asociatyvumo savybę**

*A. Mihalkovich*

Šio straipsnio tikslas yra rasti tinkamą nekomutatyvią algebrinę struktūrą, kurią galima būtų panaudoti kaip platforminę struktūrą matricinio laipsnio funkcijai apibrėžti. Mes manome, jog šis netrivialus ir įdomus uždavinys gali būti naudingas vienkryptei funkcijai, kuri turėtų praktinį taikymą kriptografijoje, apibrėžti. Kadangi pagrindinis sunkumas taikant nekomutatyvias struktūras vienkryptei funkcijai apibrėžti yra tam tikrų sąlygų asociatyvumui užtikrinti tenkinimas, mes nagrinėjame vieną iš galimų pasirinkimų, t.y. grupę $\boldsymbol{M}_{16}$, tiriame jos pagrindines savybes ir apibrėžiame šablonus, su kuriais dirbsime ateityje.

*Raktiniai žodžiai*: matricinio laipsnio funkcija, vienkryptė funkcija, nekomutatyvios algebrinės struktūros.