



Article

MPF Problem over Modified Medial Semigroup Is NP-Complete

Eligijus Sakalauskas [†]  and Aleksejus Mihalkovich ^{*} 

Department of Applied Mathematics, Kaunas University of Technology, LT-44249 Kaunas, Lithuania; eligijus.sakalauskas@ktu.lt

^{*} Correspondence: aleksejus.michalkovic@ktu.lt; Tel.: +370-600-14070

[†] Current address: Studentu str. 50-324.

Received: 21 September 2018; Accepted: 22 October 2018; Published: 1 November 2018

Abstract: This paper is a continuation of our previous publication of enhanced matrix power function (MPF) as a conjectured one-way function. We are considering a problem introduced in our previous paper and prove that this problem is NP-Complete. The proof is based on the dual interpretation of well known multivariate quadratic (MQ) problem defined over the binary field as a system of MQ equations, and as a general satisfiability (GSAT) problem. Due to this interpretation the necessary constraints to MPF function for cryptographic protocols construction can be added to initial GSAT problem. Then it is proved that obtained GSAT problem is NP-Complete using Schaefer dichotomy theorem. Referencing to this result, GSAT problem by polynomial-time reduction is reduced to the sub-problem of enhanced MPF, hence the latter is NP-Complete as well.

Keywords: cryptography; non-commutative cryptography; one-way functions; NP-Completeness; key agreement protocol

1. Introduction

It is very natural to look for a new conjectured one-way functions (OWFs) for cryptographic applications in connection with new challenges caused by quantum cryptanalysis. This paper is a continuation of research in this field and is dealing with so called matrix power function (MPF). Some cryptographic primitives were built on the basis that MPF is a conjectured OWF in [1–5]. Furthermore, some results were published considering the security of presented primitives in [6–8]. The security of these primitives is based on the complexity of MPF inversion named as MPF problem.

So far, it is thought that OWF security based on the NP-Complete problem is not vulnerable to the quantum cryptanalysis, while the cryptosystems based on conjectured OWFs such as factoring and discrete logarithm problems are vulnerable due to [9]. Therefore, it is very desirable to try to prove NP-Completeness of MPF problem. In [6] the NP-Completeness of a more general problem named as multivariate quadratic power problem is presented. However, the question of NP-Completeness of MPF problem remained open so far.

In [10] our efforts were directed toward the increasing expectable complexity of MPF problem by choosing more complicated algebraic structures for MPF definition but at the same time preserving the necessary properties for the cryptographic primitives construction. In that paper, we presented a key agreement protocol in Section 2, Construction 1 as well as an example of its realization with artificially small parameters in Section 6.

In this paper we present a proof of NP-Completeness of sub-problem of enhanced MPF problem previously considered in [10]. The notion of sub-problem is defined as follows:

Definition 1. *The decision problem P_1 is a sub-problem of problem P_2 if every assignment to input values, which provides the answer YES to problem P_2 , also implies the answer YES to the problem P_1 .*

The proof is based on the duality of multivariate quadratic MQ problem interpretation as a system of MQ equations over $\mathcal{Z}_2 = \{0, 1\}$ [11,12] and according to Schaefer dichotomy theorem [13] as a general satisfiability (GSAT) problem.

The main benefit of such approach is the opportunity to include some constraints to MPF necessary to construct cryptographic primitives as an additional GSAT equations.

The proof is based on proving that this GSAT is NP-Complete and on polynomial-time reduction from GSAT to the sub-problem of enhanced MPF problem.

2. Matrix Power Function

MPF was first introduced in [4]. To be self-contained, we present here MPF in the following way:

Definition 2. Symbolically MPF corresponds to matrix $W_{m \times m} = \{w_{ij}\}$ powered by matrix $X_{m \times m} = \{x_{ij}\}$ on the left and by matrix $Y_{m \times m} = \{y_{ij}\}$ on the right with MPF value equal to matrix $E_{m \times m} = \{e_{ij}\}$ and is expressed in the following way

$${}^X W^Y = E, e_{ij} = \prod_{k=1}^m \prod_{l=1}^m w_{kl}^{x_{ik} \cdot y_{lj}}. \quad (1)$$

The matrix W that is powered is named the base matrix and the matrices X and Y that are powering the base matrix are named power matrices. In general, we define the base matrix over the multiplicative (semi)group \mathcal{S} and power matrices over some numerical (semi)ring \mathcal{R} . We call semigroup \mathcal{S} a platform (semi)group, which according to the MPF definition, is multiplicative, and \mathcal{R} —an exponent (semi)ring. The appropriate matrix semigroups $\mathcal{M}_{\mathcal{S}}$ and matrix semiring $\mathcal{M}_{\mathcal{R}}$ contain base matrices and power matrices respectively.

The exact MPF definition depends on the type of sets over which matrices are defined.

In [3] authors proved, that if platform semigroup and power semiring are commutative, then the following associative properties of MPF takes place:

Definition 3. MPF is one-side associative, (left-side and right-side associative, respectively) if the following identities hold:

$$\begin{aligned} Y ({}^X W) &= (YX)W = {}^{YX}W; \\ (W^X)^Y &= W^{(XY)} = W^{XY}. \end{aligned} \quad (2)$$

Definition 4. MPF is two-side associative if the following identities hold:

$$({}^X W)^Y = {}^X (W^Y) = {}^X W^Y. \quad (3)$$

In [3] authors proved, that if platform semigroup \mathcal{S} and power semiring \mathcal{R} are commutative, then $\text{MPF}_{\mathcal{S}}^{\mathcal{R}}$ is one and two-side associative.

It follows from Equation (1), that in general, MPF is a function

$$\text{MPF} : \mathcal{M}_{\mathcal{R}} \times \mathcal{M}_{\mathcal{S}} \times \mathcal{M}_{\mathcal{R}} \mapsto \mathcal{M}_{\mathcal{S}}.$$

Definition 5. The direct MPF value computation is to find matrix E , when matrices X, W, Y are given.

Definition 6. The inverse MPF value computation is to find matrices X and Y , when matrices W and E are given.

Definition 7. MPF problem is its inverse value computation.

Definition 8. MPF presented in 1 is a candidate one-way function (OWF) if the following necessary (but not sufficient) conditions are satisfied:

1. The direct MPF value computation is easy;
2. The MPF problem is polynomially equivalent to a certain hard problem with not known polynomial time algorithm.

Assume, that the base matrix W in Expression 1 is defined over a platform semigroup denoted by \mathcal{S} and the power matrices X and Y are defined over a power semiring denoted by \mathcal{R} . We denote the MPF problem defined by these structures by $\text{MPF}_{\mathcal{S}}^{\mathcal{R}}$. Assume, that power matrices X and Y have to satisfy some constrains denoted by \mathcal{C} . In this case we denote the MPF problem by $\text{MPF}_{\mathcal{S}}^{\mathcal{R},\mathcal{C}}$.

To build cryptographic primitives, e.g., key agreement protocol, based on $\text{MPF}_{\mathcal{S}}^{\mathcal{R}}$ the following additional property must be satisfied: square matrices of m -th order X and Y defined over the power semiring \mathcal{R} must be elements of two subsets $\mathcal{M}_{\mathcal{R},1}$ and $\mathcal{M}_{\mathcal{R},2}$ of commuting matrices in $\mathcal{M}_{\mathcal{R}}$ respectively, i.e., for any $U \in \mathcal{M}_{\mathcal{R},1}$ and $V \in \mathcal{M}_{\mathcal{R},1}$ the following identities take place

$$\mathcal{C}: \begin{cases} XU = UX; \\ YV = VY. \end{cases} \quad (4)$$

This defines a constrained MPF that we previously denoted by $\text{MPF}_{\mathcal{S}}^{\mathcal{R},\mathcal{C}}$. Further we will use the single subset of commuting matrices in $\mathcal{M}_{\mathcal{R}}$, namely the subset of circulant matrices i.e., matrices of the following general form [14]:

$$X = \begin{pmatrix} x_1 & x_m & \ddots & \ddots & x_2 \\ x_2 & x_1 & x_m & \ddots & \ddots \\ x_3 & x_2 & x_1 & \ddots & \ddots \\ \ddots & \ddots & \ddots & \ddots & x_m \\ x_m & \ddots & x_3 & x_2 & x_1 \end{pmatrix}. \quad (5)$$

Any circulant matrix X can be represented by its column vector \vec{x} , which transposed form is expressed by the following row vector $\vec{x}^T = (x_1, x_2, \dots, x_m)$. If $\text{MPF}_{\mathcal{S}}^{\mathcal{R},\mathcal{C}}$ satisfies the conditions of Definition 8, then the following secret-key agreement protocol can be executed as proposed in [10]:

Both parties agree on a public information: the modified medial semigroup \mathcal{S} and a public base matrix W with its entries randomly chosen from \mathcal{S} . Alice and Bob can agree on a common key as follows:

1. Alice chooses two secret circulant matrices X and Y at random of size m . Using these matrices she computes the MPF value $A = {}^X W^Y$ and sends it to Bob;
2. Bob chooses two secret circulant matrices U and V at random of size m . Using these matrices he computes the MPF value $B = {}^U W^V$ and sends it to Alice;
3. Alice and Bob compute the same secret key in the following way:

$$K_A = {}^X B^Y = {}^X ({}^U W^V)^Y = {}^U ({}^X W^Y)^V = K_B = K. \quad (6)$$

The Identity (6) is true due to the fact, that circulant matrices are commuting and associativity Conditions (2) and (3).

Remark 1. In general two-sided association Condition (3) will be not necessary, if we agree upon on the order of operations, e.g., from the left to the right.

In our previous research the base matrix W was defined over the multiplicative platform group $\mathcal{Z}_p^* = \{1, 2, \dots, p-1\}$ and power matrices X and Y over the numerical power ring $\mathcal{Z}_{p-1} =$

$\{0, 1, 2, \dots, p-2\}$. This kind of MPF is denoted by $MPF_{Z_p^*}^{Z_{p-1}}$ and constrained version by $MPF_{Z_p^*}^{Z_{p-1}, \mathcal{C}}$. It represents the MPF defined over commutative algebraic structures considered in [1,2,5,7,15].

However, recently a linear algebra attack to the protocol presented in [3] based on $MPF_{Z_p^*}^{Z_{p-1}, \mathcal{C}}$ was found by [16]. This attack to $MPF_{Z_p^*}^{Z_{p-1}, \mathcal{C}}$ problem runs in polynomial time and hence can be used to break the algorithms presented in [1,3]. The authors of [16] also suggested some improvements of our protocols to resist the proposed attack. In [7] we fixed this flaw for the asymmetric encryption protocol, presented in [1].

The intriguing idea was to extend MPF construction to non-commutative algebraic structures, namely \mathcal{S} and \mathcal{R} , hence expecting higher complexity of MPF problem and achieving a higher potential security for the construction of cryptographic primitives. The main problem of this approach was the loss of associativity of MPF, which made its application in cryptography impossible.

This approach was successful and is presented in [10], when platform semigroup \mathcal{S} is a modified medial semigroup and power semiring is a special kind of so called near semiring NSR . In this study as a power semiring we use a semiring of non-negative integers denoted by $\mathcal{N}^0 = \{0, 1, 2, 3, \dots\}$. So we deal with the MPF denoted by $MPF_{\mathcal{S}}^{\mathcal{N}^0}$. If power matrices satisfies commutation Constraints in (4), then we denote corresponding MPF by $MPF_{\mathcal{S}}^{\mathcal{N}^0, \mathcal{C}}$.

In this paper we consider a class of $MPF_{\mathcal{S}}^{\mathcal{N}^0, \mathcal{C}}$ problems when power matrices are circulant matrices over the \mathcal{N}^0 and hence they are commuting and satisfying Conditions (4). Interestingly enough, matrices X and Y are almost never invertible due to the fact, that both fractions and negative numbers are not contained in \mathcal{N}^0 . This is essential to our proof of NP-Completeness of the $MPF_{\mathcal{S}}^{\mathcal{N}^0, \mathcal{C}}$ problem.

In earlier work, the proof that random generated multivariate quadratic power problem over \mathcal{Z}_n is NP-Complete is presented. This proof is insufficient to prove the NP-Completeness of $MPF_{\mathcal{S}}^{\mathcal{N}^0, \mathcal{C}}$ problem due to fact that we are considering a partial case of this problem. Our multivariate quadratic power system of equations is predetermined by the matrix power equations. Hence this special case is not random generated. Therefore, the aim of this paper is to fill this gap.

In general, it is hard to prove that a problem with arbitrary constraints is NP-Complete (NP-Hard). We present here an approach to prove it based on Schaefer dichotomy theorem [13]. This theorem is formulated for the GSAT problem, represented by arbitrary finite set of Boolean relations (formulas) with respect to the finite set of Boolean variables. The theorem defines six criteria when either GSAT is in P or in NP-Complete complexity class.

In this paper, we construct a certain sub-problem of GSAT problem which is a one-to-one mapping of certain sub-problem of $MPF_{\mathcal{S}}^{\mathcal{N}^0, \mathcal{C}}$ problem. We show, that this GSAT problem satisfies the Schaefer criteria to be NP-Complete. Hence, using polynomial-time reduction, we will prove that decision version of $MPF_{\mathcal{S}}^{\mathcal{N}^0, \mathcal{C}}$ problem is also NP-Complete.

We revise the definition and basic properties of modified medial semigroup in the next section and present the main result in Section 4.

3. Modified Medial Semigroup as Platform Semigroup of MPF

Let us consider medial semigroup $\mathcal{S}_{\mathcal{M}}$, which was previously introduced by [17]. Assume, that the presentation of this semigroup consists of two generators a and b and a relation $R_{\mathcal{M}}$ written in the following way:

$$\mathcal{S}_{\mathcal{M}} = \langle a, b | R_{\mathcal{M}} \rangle; \tag{7}$$

$$R_{\mathcal{M}} : \omega_1 a b \omega_2 = \omega_1 b a \omega_2. \tag{8}$$

where ω_1 and ω_2 are arbitrary non-empty words in $\mathcal{S}_{\mathcal{M}}$, written in terms of generators a and b .

Let us now present an important identity, which is useful to us for application of medial semigroup $\mathcal{S}_{\mathcal{M}}$ to MPF:

$$(\omega_1 \omega_2)^e = \omega_1^e \omega_2^e. \tag{9}$$

This identity is based on the Relation (8) and is valid for all words $\omega_1, \omega_2 \in \mathcal{S}_{\mathcal{M}}$ and any exponent $e \in \mathcal{N}^0$.

To prevent the growth of powers of generators when exponentiation takes place we introduce a modified medial semigroup \mathcal{S} with two extra relations R_1 and R_2 in the following general form:

$$\begin{aligned} R_1 &: ba^{p+2}b^{p+1} = ba^2b; \\ R_2 &: ab^{p+2}b^{p+1} = ab^2a. \end{aligned} \tag{10}$$

Thus, modified medial semigroup \mathcal{S} has the following presentation:

$$\mathcal{S} = \langle a, b | R_{\mathcal{M}}, R_1, R_2 \rangle, \tag{11}$$

with relations $R_{\mathcal{M}}, R_1$ and R_2 defined above.

Note, that we define \mathcal{S} as a multiplicative, non-commuting, non-cancellative and infinite semigroup which is a non-symmetric algebraic structure.

Remark 2. The modified medial semigroup is well defined if relations R_1 and R_2 are symmetric, i.e., they link both generators in such a way, that the order of generators is symmetric and exponents of each generator add up to the same number. In our case the sum of exponents of generators a and b on the left side of R_1 and R_2 in Relations (10) equals $p + 2$ and on the right side it equals 2.

Remark 3. In our previous paper we considered a special case of $p = 3$.

Semigroups $\mathcal{S}_{\mathcal{M}}$ and \mathcal{S} are made monoids by introducing an empty word as a multiplicatively neutral element, denoted by 1. Then conveniently, the following identities hold for all $\omega \in \mathcal{S}_{\mathcal{M}}$:

$$\omega 1 = 1\omega = \omega, \omega^0 = 1, 0 \in \mathcal{N}^0. \tag{12}$$

The normal form for the words in $\mathcal{S}_{\mathcal{M}}$ was also defined in the following way:

Definition 9. The normal form $\omega_{\mathcal{M},nf}$ of any word ω_0 in semigroup $\mathcal{S}_{\mathcal{M}}$ is expressed as follows:

$$\omega_{\mathcal{M},nf} = \max_{\alpha_a, \beta_b} b^{\beta_b} a^{r_a} b^{s_b} a^{\alpha_a} = b^{\beta} a^{i_a} b^{j_b} a^{\alpha}, \tag{13}$$

where $\alpha, \beta \in \{0, 1\}$ and $\alpha_a, \beta_b, r_a, s_b, i_a, j_b \in \mathcal{N}$.

To obtain the normal form for the word ω we consider its first and last literals. Using Relation (9) we can determine the values of α and β . For example the normal form for the word $b^7 a^8 b^2 a^6$ is $ba^{13} b^8 a$. The word $b^6 a^7 b^3 a^7$ has the same normal form and hence we consider all these words equivalent. The normal form for the word $a^7 b^8 a^2 b^6$ is $b^0 a^9 b^{14} a^0$. Hence in the last case we have $\alpha = 0$ and $\beta = 0$. Evidently for the normal form of the word $a^5 b^7 a^3$ we have $\alpha = 1$ and $\beta = 0$ whereas in case of the word $b^5 a^7 b^3$ we have $\alpha = 0$ and $\beta = 1$. In fact, the normal forms for the presented words are $b^0 a^7 b^7 a$ and $ba^7 b^7 a^0$ respectively. We generally omit zeroth powers when writing normal forms.

On the base of $\omega_{\mathcal{M},nf}$ the normal form in \mathcal{S} is defined as follows:

Definition 10. The normal form ω_{nf} of any word ω_0 in semigroup \mathcal{S} is expressed by the following expression:

$$\omega_{nf} = \min_{i_a, j_b} \max_{\beta, \alpha} b^{\beta} a^{i_a} b^{j_b} a^{\alpha}. \tag{14}$$

Let T be an additive non-commuting semigroup consisting of the tuples (β, i, j, α) , where $\alpha, \beta \in \{0, 1\} \subset \mathcal{N}^0$ and $i, j \in \mathcal{N}^0$, with the following addition operation:

$$(\beta_1, i_1, j_1, \alpha_1) + (\beta_2, i_2, j_2, \alpha_2) =$$

$$= (\beta_1, i_1 + \alpha_1 + i_2, j_1 + \beta_2 + j_2, \alpha_2),$$

then there is an isomorphism $\varphi : \mathcal{S}_{\mathcal{M},nf} \mapsto T$, which can be expressed by the following relation for any word ω_{nf}

$$\varphi(\omega_{nf}) = \varphi(b^\beta a^i b^j a^\alpha) = (\beta, i, j, \alpha). \tag{15}$$

Hence, using our notation, we defined $\text{MPF}_S^{\mathcal{N}^0}$, where \mathcal{S} is modified medial semigroup. It is important to note, that $\text{MPF}_S^{\mathcal{N}^0}$ satisfies associativity conditions in Definitions (2) and (3) due to the properties of medial semigroup.

Adding the commutation Constraints (4) to the power matrices X and Y defined over \mathcal{N}^0 , constrained $\text{MPF}_S^{\mathcal{N}^0}$ problem we denoted by $\text{MPF}_S^{\mathcal{N}^0, \mathcal{C}}$.

In the next section we prove, that $\text{MPF}_S^{\mathcal{N}^0, \mathcal{C}}$ problem is NP-Complete.

4. Proof of NP-Completeness

Let us consider the following binary matrix equation:

$$XQY = A, \tag{16}$$

where all matrices Q, A, X and Y are defined over the field $\mathcal{Z}_2 = \{0, 1\}$ with multiplication operation denoted by \wedge (logical AND) and addition operation by \oplus (logical XOR). This equation corresponds to binary matrix multivariate quadratic (BMMQ) equation and associated problem to BMMQ problem.

Definition 11. *The binary matrix MQ (BMMQ) problem is to find matrices X and Y in Equation (16), when matrices Q and A are given.*

Remark 4. *Throughout this paper we assume, that matrix Q is well-balanced, i.e., the quantity of 1's is close to $m^2/2$. Furthermore all the 1's are distributed uniformly in the rows and columns of matrix Q .*

If at least one of square matrices X or Y is invertible, then BMMQ Problem (16) is solvable in polynomial time due to one the following transformations:

$$\begin{aligned} XQ \oplus AY^{-1} &= 0; \\ QY \oplus X^{-1}A &= 0, \end{aligned} \tag{17}$$

since XOR operation is inverse to itself.

It is clear, that both transformations represent the system of m^2 homogeneous linear equations with $2 m^2$ unknown variables.

However, if both binary matrices X and Y are singular, then Transformations (17) are not possible and hence the initial Problem (16) bears a resemblance to the well known multivariate quadratic (MQ) problem. It is known, that random generated MQ problem is NP-Complete over any field [11,12].

Hence, we define the following problem:

Definition 12. *The singular binary matrix MQ problem (SBMMQ) is to solve BMMQ problem, when matrices X and Y in Equation (16) are singular.*

It is important to note, that we are interested in this particular problem, since in case of $\text{MPF}_S^{\mathcal{N}^0, \mathcal{C}}$ power matrices are defined over the semiring \mathcal{N}^0 and hence any randomly chosen power matrix is not invertible with overwhelming probability. Here and onwards we say that a random event happens with overwhelming probability if its probability of failure is negligible.

We begin from the complexity consideration of CSBMMQ problem.

Our proof is based on Schaefer dichotomy theorem [13]. Let us define a set of Boolean relations $\{r_1, r_2, \dots, r_M\}$ with variables defined by two vectors $\vec{x}^T = (x_1, x_2, \dots, x_m)$ and $\vec{y}^T = (y_1, y_2, \dots, y_m)$. Then the following generalized satisfiability problem GSAT can be formulated:

$$\begin{cases} r_1(\vec{x}, \vec{y}) = 1; \\ r_2(\vec{x}, \vec{y}) = 1; \\ \dots \\ r_M(\vec{x}, \vec{y}) = 1, \end{cases} \tag{18}$$

where 1 is a true value assignment to the relations.

Definition 13. The decision GSAT problem is to answer YES/NO to the question: are there any assignment to the variables \vec{x} and \vec{y} that all Boolean relations in Problem (18) are true?

Theorem 1. (Schaefer dichotomy theorem [13]). If at least one of the following criteria is satisfied, then the satisfiability problem GSAT is in P, otherwise it is NP-Complete :

- (a) Every relation in S is satisfied when all the variables are 0 (0-valid clause);
- (b) Every relation in S is satisfied when all the variables are 1 (1-valid clause);
- (c) Every relation in S is definable by a CNF formula in which each conjunct has at most one negated variable (dual Horn clause);
- (d) Every relation in S is definable by a CNF formula in which each conjunct has at most one unnegated variable (Horn clause);
- (e) Every relation in S is definable by a CNF formula having at most two literals in each conjunct (bijunctive clause);
- (f) Every relation in S is the set of solutions of a system of linear equation over the two element field $\{0, 1\}$ (affine clause).

As it was mentioned above, to satisfy the commutation Conditions (4), matrices X and Y are chosen to be circulant. Then matrix Equation (16) can be transformed to the following system of equations:

$$\begin{cases} \vec{x}^T Q_{11} \vec{y} = a_{11}; \\ \vec{x}^T Q_{12} \vec{y} = a_{12}; \\ \dots \\ \vec{x}^T Q_{mm} \vec{y} = a_{mm}, \end{cases} \tag{19}$$

where vectors \vec{x}^T and \vec{y}^T are row vectors of the first row and first column of matrix Q respectively, and matrices $Q_{11}, Q_{12}, \dots, Q_{mm}$ are obtained by cyclic permutations of matrix Q. For example, $Q_{11} = Q$ and $Q_{12} = (\vec{q}_2 \ \vec{q}_3 \ \dots \ \vec{q}_m \ \vec{q}_1)$, where the vector \vec{q}_j denotes the j-th column of matrix Q. All matrices Q_{ij} are obtained from the initial matrix by performing shifts of rows and/or columns.

The latter system consist of m^2 quadratic equations with $2m$ variables being a components of vectors \vec{x} and \vec{y} . System (19) is a special type of random generated MQ problem over \mathbb{Z}_2 defined by special type of matrices $Q_{11}, Q_{12}, \dots, Q_{mm}$, generated by deterministic permutations of random generated matrix Q in Equation (16). Every equation in System (19) represents a Boolean relation written in terms of logical operations AND and XOR.

To choose a suitable GSAT problem to prove NP-Completeness of the initial $MPF_S^{\wedge^0, \mathcal{C}}$ problem the set of logical Relations (18) must be supplemented by logical relations defining the singularity constraints of matrices X and Y. Since System (19) is defined over $\mathbb{Z}_2 = \{0, 1\}$, these constraints can be expressed by the following Boolean relations:

$$\begin{aligned} \det X &= 0; \\ \det Y &= 0, \end{aligned} \tag{20}$$

where 0 is a false value assignment to the relations. The actual expressions of (20) are determined by the format of matrices X and Y . Hence, here and onwards we consider square matrices of m -th order X and Y with even values of determinants.

Definition 14. The constrained singular binary matrix MQ problem (CSBMMQ) is to solve SBMMQ problem, when matrices X and Y in Equation (16) are singular and hence satisfy Conditions (4) and (16) while also satisfying Condition (20).

Theorem 2. Decision CSBMMQ problem is NP-Complete.

Proof. To prove the theorem, we use the Schaefer dichotomy theorem. System of binary Equation (19) and Relations (20) represent the system of generalized satisfiability relations in Problem (18) and corresponds to GSAT problem with $M = m^2 + 2$. Then to prove NP-Completeness of CSBMMQ we need to verify inconsistency of Schaefer criteria (a)–(f).

The first two criteria (a) and (b) are not satisfied due to the fact, that we are choosing matrix Q at random and hence the satisfiability of these criteria has a negligible probability.

To verify Schaefer criteria (c)–(e) we denote three pairs of vectors satisfying Equations (19) and (20) by (\vec{x}_1, \vec{y}_1) , (\vec{x}_2, \vec{y}_2) and (\vec{x}_3, \vec{y}_3) . Note, that we generate circulant matrices from selected vectors to check the validity of Equation (20). Schaefer criteria (c)–(e) can be reformulated as follows [18]:

- (c') For all pairs (\vec{x}_1, \vec{y}_1) and (\vec{x}_2, \vec{y}_2) , satisfying System (19) and Equation (20), the pair $(\vec{x}_1 \vee \vec{x}_2, \vec{y}_1 \vee \vec{y}_2)$ is a solution of System (19) and Equation (20);
- (d') For all pairs (\vec{x}_1, \vec{y}_1) and (\vec{x}_2, \vec{y}_2) , satisfying System (19) and Equation (20), the pair $(\vec{x}_1 \wedge \vec{x}_2, \vec{y}_1 \wedge \vec{y}_2)$ is a solution of System (19) and Equation (20);
- (e') For all pairs (\vec{x}_1, \vec{y}_1) , (\vec{x}_2, \vec{y}_2) and (\vec{x}_3, \vec{y}_3) , satisfying System (19) and Equation (20), the pair $((\vec{x}_1 \vee \vec{x}_2) \wedge (\vec{x}_1 \vee \vec{x}_3) \wedge (\vec{x}_2 \vee \vec{x}_3), (\vec{y}_1 \vee \vec{y}_2) \wedge (\vec{y}_1 \vee \vec{y}_3) \wedge (\vec{y}_2 \vee \vec{y}_3))$ is a solution of System (19) and Equation (20).

Remark 5. All logical operations in criteria (c')–(e') are performed component-wise.

Then applying criterion (c') to the single equation in System (19) in vector form and assigning arbitrary values to the vectors (\vec{x}_1, \vec{y}_1) , (\vec{x}_2, \vec{y}_2) we obtain the corresponding values b_{ij} satisfying the following equation in every case

$$(\vec{x}_1 \vee \vec{x}_2)^T Q_{ij} (\vec{y}_1 \vee \vec{y}_2) = b_{ij}.$$

Evidently, in most cases $b_{ij} \neq a_{ij}$. Note, however, that for this criterion to be valid the identity $b_{ij} = a_{ij}$ has to hold for all $i, j = 1, 2, \dots, m$. Hence, dual Horn clause in System (19) is not satisfied and criterion (c') is inconsistent.

Analogously, verifying Horn clause we obtain

$$(\vec{x}_1 \wedge \vec{x}_2)^T Q_{ij} (\vec{y}_1 \wedge \vec{y}_2) = c_{ij},$$

where $c_{ij} \neq a_{ij}$. Hence, Horn clause in System (19) is not satisfied for all $i, j = 1, 2, \dots, m$ and criterion (d') is inconsistent.

Inconsistency of criterion (e') follows directly from the latter three expressions. Note, that the key point which allows us to claim the desired result is Remark 5 since no distributive law can be applied to the latter two expressions.

Criterion (f) is not satisfied since, in general, relations in System (19) are non-linear.

So, CSBMMQ problem is NP-Complete. \square

Remark 6. Two additional Relations (20) are needed to ensure that matrices X and Y are singular and hence to ensure the inconsistency of Schaefer criteria.

Now we turn to constrained singular matrix multivariate quadratic (CSMMQ) problem defined over the semiring of integers \mathcal{N}_0 which we denote by $CSMMQ_{\mathcal{N}_0}$. This means that Equation (16) and corresponding Conditions (19) and (20) are defined over \mathcal{N}_0 .

Theorem 3. CSBMMQ problem is a sub-problem of $CSMMQ_{\mathcal{N}_0}$.

Proof. Let us consider all matrices in Equation (16) defined over \mathcal{N}_0 . Then they can be rewritten in the following way:

$$\begin{aligned} X &= 2U + X'; \\ Y &= 2V + Y'; \\ Q &= 2P + Q'; \\ A &= 2T + A'. \end{aligned}$$

By substituting these expressions in Equation (16) we obtain the following result:

$$(2U + X') (2P + Q') (2V + Y') = 2T + A'$$

and hence

$$X'Q'Y' \equiv A' \pmod{2}.$$

Let us consider the following decision problem: does there exist assignments to matrices X and Y defined over the semiring \mathcal{N}_0 satisfying Equation (16), which adding commutation constraints corresponds to Relations (19), (20) and is a $CSMMQ_{\mathcal{N}_0}$ problem? Assume, that we have an answer YES to decision $CSMMQ_{\mathcal{N}_0}$ problem. Due to penultimate equation, it implies the answer YES to CSBMMQ problem.

In computational $CSMMQ_{\mathcal{N}_0}$ version its transformation to CSBMMQ requires the reduction of the solution modulo 2. This is done in polynomial time.

We proved, that CSBMMQ problem is a sub-problem of $CSMMQ_{\mathcal{N}_0}$ problem, when semiring \mathcal{N}_0 is homomorphically mapped to the field \mathbb{Z}_2 . \square

Since Theorem 3 is valid, every solution of $CSMMQ_{\mathcal{N}_0}$ problem has to satisfy CSBMMQ problem as well. Clearly, this problem is non-trivial and was proven to be NP-Complete.

Let us consider the following system of equations

$$\begin{cases} X\Lambda Y = B; \\ X\Sigma Y \equiv C \pmod{2p}. \end{cases} \tag{21}$$

where p is an odd prime, matrices X, Y, Σ and C are defined over the semiring of positive integers \mathcal{N}^0 , and matrices Λ and B over the ring \mathbb{Z} . Furthermore, the parity of matrices Λ and Σ is the same, i.e., $\Lambda - \Sigma = 2T$, where $T \in \mathcal{M}_{\mathbb{Z}}$.

Theorem 4. The decision CSMMQ problem, defined by System (21), is NP-Complete.

Proof. It is easy to assume also with overwhelming probability, that matrices X and Y defined over the \mathcal{N}^0 are not invertible. We define the following sub-problem of Problem (21) by reducing its first equation modulo $2p$:

$$\begin{cases} X\Lambda Y \equiv B \pmod{2p}; \\ X\Sigma Y \equiv C \pmod{2p}. \end{cases} \tag{22}$$

Clearly, if the answer to the initial Problem (21) is YES, then the same answer applies also to Problem (22), since to obtain the solution of the Problem (21) extra matrices T and S in the relations

$$X = (2p)T + \tilde{X}_{2p};$$

$$Y = (2p)S + \tilde{Y}_{2p}$$

have to be found. Here matrices \tilde{X}_{2p} and \tilde{Y}_{2p} satisfy the Problem (22).

We can rewrite the System (22) in the following way by using Chinese Remainder Theorem:

$$\begin{cases} X\Lambda Y \equiv B \pmod{p}; \\ X\Sigma Y \equiv C \pmod{p}. \end{cases} \quad (23)$$

$$\begin{cases} X\Lambda Y \equiv B \pmod{2}; \\ X\Sigma Y \equiv C \pmod{2}; \end{cases} \quad (24)$$

It is important to note, that, due to Chinese Remainder Theorem, Systems (23) and (24) must be considered separately. These systems of equations provide two different and mutually independent components of solution of Problem (22). Matrices \tilde{X}_{2p} and \tilde{Y}_{2p} satisfying System (22) are calculated as follows:

$$\tilde{X}_{2p} = p\tilde{X}_2 + (p+1)\tilde{X}_p;$$

$$\tilde{Y}_{2p} = p\tilde{Y}_2 + (p+1)\tilde{Y}_p,$$

where matrices \tilde{X}_p and \tilde{Y}_p satisfy System (23) and \tilde{X}_2 and \tilde{Y}_2 satisfy System (24).

We can assume, that solution of (23) can be found in polynomial time if at least one of matrices X or Y are invertible modulo p . However, nevertheless we cannot recover the solution of (22) from the one component $(\tilde{X}_p, \tilde{Y}_p)$, i.e., the component $(\tilde{X}_2, \tilde{Y}_2)$ is required. It is directly implied by the Chinese Remainder Theorem isomorphism.

Furthermore, since matrices Λ and Σ have the same parity the following congruence is valid:

$$\Lambda \equiv \Sigma \pmod{2}.$$

Hence we have $B \equiv C \pmod{2}$, since otherwise the answer to Problem (22) is NO. However in this case we can remove either one of equations of System (24) and hence we obtain a CSBMMQ problem. This problem was proven to be NP-Complete in Theorem 2.

We have shown, that the proof of complexity of Problem (21) relies on the complexity of CSBMMQ problem. Since CSBMMQ is NP-Complete and is a sub-problem of CSMMQ Problem (21), then the latter is also NP-Complete. \square

Remark 7. Theorem 3 is the key factor, which allows us to claim the correctness of Theorem 4. However, based on our logic presented here, we cannot claim, that the singular MMQ problem is NP-Complete over \mathcal{Z}_p , where p is prime, due to the fact that CSBMMQ problem is not a sub-problem of the latter problem.

To demonstrate the relation of CSMMQ Problem (21) to modified medial semigroup \mathcal{S} let us define the following mappings:

$$\lambda(b^\beta a^i b^j a^\alpha) = (i + \alpha) - (j + \beta); \quad (25)$$

$$\sigma(b^\beta a^i b^j a^\alpha) = (i + \alpha) + (j + \beta). \quad (26)$$

Remark 8. Obviously Mappings (25) and (26) define functions of powers i and j if we preset the values of α and β .

Remark 9. In general we have $\lambda(w) \in \mathcal{Z}$ and $\sigma(w) \in \mathcal{N}^0$. Furthermore, if $\sigma(w) = 0$, then w is an empty word, i.e., $w = 1$.

It is clear that if we preset two exponents $\alpha, \beta \in \{0, 1\}$, then the pair $(\lambda(w), \sigma(w))$ defines a unique element w if these elements have the same parity and satisfy inequality $|\lambda(w)| < \sigma(w)$. Clearly, this reduction is polynomial since for a fixed pair $\varphi_{(\alpha_0, \beta_0)}(\lambda, \sigma)$ we have:

$$\begin{cases} i = \frac{\lambda + \sigma}{2} - \alpha_0; \\ j = \frac{\sigma - \lambda}{2} - \beta_0. \end{cases} \tag{27}$$

Then the following theorem can be formulated:

Theorem 5. The mapping $\lambda(w)$ is an invariant of the reduction, i.e., $\lambda(w) = \lambda(w_{nf})$, and the mapping $\sigma(w)$ is an invariant modulo $2p$ of the reduction, i.e., $\sigma(w) \equiv \sigma(w_{nf}) \pmod{2p}$, where w_{nf} is the any word in \mathcal{S} reduced to its normal form.

The proof of this theorem follows from the definition of the reduction and thus we omit it. The defined mappings have the following important property:

$$\lambda(w^k) = k\lambda(w); \tag{28}$$

$$\sigma(w^k) = k\sigma(w). \tag{29}$$

Let us assume that the entries of matrices Λ and Σ satisfy the conditions presented in Problem (21). Then the following one-to-one-mapping mapping can be defined:

$$\varphi_{(\alpha_0, \beta_0)}(\lambda, \sigma) = b^{\beta_0} a^i b^j a^{\alpha_0}, \tag{30}$$

where the values of α_0 and β_0 are fixed.

Example 1. Assume, that $\lambda = 3$ and $\sigma = 7$. Then we have:

$$\begin{aligned} \varphi_{(0,0)}(3, 7) &= a^5 b^2; \\ \varphi_{(0,1)}(3, 7) &= a^4 b^2 a; \\ \varphi_{(1,0)}(3, 7) &= b a^5 b; \\ \varphi_{(1,1)}(3, 7) &= b a^4 b a. \end{aligned}$$

Furthermore, if $\lambda = -3$ and $\sigma = 7$, then:

$$\begin{aligned} \varphi_{(0,0)}(-3, 7) &= a^2 b^5; \\ \varphi_{(0,1)}(-3, 7) &= a b^5 a; \\ \varphi_{(1,0)}(-3, 7) &= b a^2 b^4; \\ \varphi_{(1,1)}(-3, 7) &= b a b^4 a. \end{aligned}$$

However, $\varphi_{(\alpha_0, \beta_0)}(3, 6)$ and $\varphi_{(\alpha_0, \beta_0)}(7, 3)$ are undefined for any values of α_0 and β_0 .

If we apply mapping $\varphi_{(\alpha_0, \beta_0)}$ to the pair of matrices (Λ, Σ) elementwise then we obtain a matrix $W = \{w_{ij}\}$, where the entries w_{ij} are defined as follows:

$$w_{ij} = \varphi_{(\alpha_0, \beta_0)}(\lambda_{ij}, \sigma_{ij}). \tag{31}$$

Now we introduce the following expression:

$$X(\Lambda, \Sigma)Y = (X\Lambda Y, X\Sigma Y),$$

and apply the mapping $\varphi_{(\alpha_0, \beta_0)}$ to it. Due to Properties (28) and (29) we have:

$$\varphi_{(\alpha_0, \beta_0)}(X\Lambda Y, X\Sigma Y) = {}^X W^Y. \quad (32)$$

where the entries of matrix W are defined by Expression (31). Furthermore, we apply the mapping $\varphi_{(\alpha_0, \beta_0)}$ to the pair of matrices (B, C) in Problem (21) to obtain the following matrix:

$$\varphi_{(\alpha_0, \beta_0)}(B, C) = D,$$

where the entries of matrix D are defined by Expression (31). The two latter equations can be combined to yield $\text{MPF}_S^{\mathcal{N}^0, \mathcal{C}}$ problem, symbolically presented in Definition 1.

Theorem 6. $\text{MPF}_S^{\mathcal{N}^0, \mathcal{C}}$ is NP-Complete.

Proof. Due to the properties of mappings $\lambda(w)$ and $\sigma(w)$ in Expressions (25)–(27), the property of bijective mapping $\varphi_{(\alpha_0, \beta_0)}$ and Theorem 4, we find that CSBMMQ is a sub-problem of $\text{MPF}_S^{\mathcal{N}^0, \mathcal{C}}$. Since, according to Theorem 2, CSBMMQ is NP-Complete, then the $\text{MPF}_S^{\mathcal{N}^0, \mathcal{C}}$ problem is NP-Complete as well. \square

Remark 10. In fact, circulant MPF problem is NP-Complete in more general case, since for matrices X and Y with no zero entries only the upper left corner and bottom right corner entries of the base matrix W play an important role. More precisely the first and the last literal of the specified entries produce fixed values α_0 and β_0 . Normal forms of other entries of the base matrix W are irrelevant.

5. Conclusions

1. The proof of NP-Completeness of author's constructed MPF in previous Symmetry journal publication is presented. It is a new evidence, that this type of MPF can be considered for construction of a non-commuting cryptography primitive as a conjectured OWF.
2. The proof is based on two main approaches: we prove that certain GSAT is NP-Complete using modified Schaefer criteria, and, using this result, we prove that this GSAT is a sub-problem of the considered MPF problem. Hence this type of MPF problem is NP-Complete.
3. It is a new step to prove that KAP presented in our previous publication mentioned above has a provable security property.

Author Contributions: This article was supervised by E.S. who proposed the methodology later improved by both authors. A.M. performed the investigation and analyzed the obtained results together with his supervisor. Both authors collected resources for the paper. A.M. wrote the paper.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

MPF	Matrix power function
OWF	one-way function
MQ problem	Multivariate quadratic problem
MMQ problem	Matrix MQ problem

BMMQ problem	Binary matrix MQ problem
SBMMQ problem	Singular binary matrix MQ problem
CSBMMQ problem	Constrained singular binary matrix MQ problem
GSAT problem	General satisfiability problem
NP-Complete problem	Non-deterministic polynomial complete problem
CNF	Conjunctive normal form

References

- Mihalkovich, A.; Sakalauskas, E. Asymmetric cipher based on MPF and its security parameters evaluation. In Proceedings of the Lithuanian Mathematical Society, Klaipeda, Lithuania, 11–12 June 2012; VU Matematikos ir Informatikos Institutas: Vilnius, Lithuania, 2012; Ser. A, Volume 53, pp. 72–77.
- Mihalkovich, A.; Sakalauskas, E.; Venckauskas, A. New asymmetric cipher based on matrix power function and its implementation in microprocessors efficiency investigation. *Elektron. Elektrotech.* **2013**, *19*, 119–122. [[CrossRef](#)]
- Sakalauskas, E.; Listopadskis, N.; Tvarijonas, P. Key Agreement Protocol (KAP) Based on Matrix Power Function. In *Advanced Studies in Software and Knowledge Engineering*; International Book Series “Information Science and Computing”; World Scientific: Singapore, 2008; pp. 92–96.
- Sakalauskas, E.; Luksys, K. Matrix Power S-Box Construction. IACR Cryptology ePrint Archive 2007. Available online: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.78.2327&rep=rep1&type=pdf> (accessed on 26 October 2018).
- Sakalauskas, E.; Mihalkovich, A. New asymmetric cipher of non-commuting cryptography class based on matrix power function. *Informatika* **2014**, *25*, 283–298. [[CrossRef](#)]
- Sakalauskas, E. The multivariate quadratic power problem over Z_n is NP-Complete. *Inf. Technol. Control* **2012**, *41*, 33–39. [[CrossRef](#)]
- Sakalauskas, E.; Mihalkovich, A. Improved Asymmetric Cipher Based on Matrix Power Function Resistant to Linear Algebra Attack. *Informatika* **2017**, *28*, 517–524. [[CrossRef](#)]
- Sakalauskas, E.; Mihalkovich, A.; Venckauskas, A. Improved asymmetric cipher based on matrix power function with provable security. *Symmetry* **2017**, *9*, 9. [[CrossRef](#)]
- Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.* **1999**, *41*, 303–332. [[CrossRef](#)]
- Sakalauskas, E. Enhanced Matrix Power Function for Cryptographic Primitive Construction. *Symmetry* **2018**, *10*, 43. [[CrossRef](#)]
- Garey, M.R.; Johnson, D.S. *Computers and Intractability*; WH Freeman: New York, NY, USA, 2002.
- Patarin, J.; Goubin, L. Trapdoor one-way permutations and multivariate polynomials. In Proceedings of the International Conference on Information and Communications Security, Beijing, China, 11–14 November 1997; Springer: Berlin, Germany, 1997; pp. 356–368.
- Schaefer, T.J. The complexity of satisfiability problems. In Proceedings of the Tenth Annual ACM Symposium on Theory of Computing, San Diego, CA, USA, 1–3 May 1978; ACM: New York, NY, USA, 1978; pp. 216–226.
- Davis, P.J. *Circulant Matrices*; Wiley: New York, NY, USA, 1970.
- Sakalauskas, E.; Mihalkovich, A. Candidate One-Way Function Based on Matrix Power Function with Conjugation Constraints. In Proceedings of the Conference proceedings Bulgarian Cryptography Days 2012, Sofia, Bulgaria, 20–21 September 2012; pp. 29–37.
- Liu, J.; Zhang, H.; Jia, J. A linear algebra attack on the non-commuting cryptography class based on matrix power function. In Proceedings of the International Conference on Information Security and Cryptology, Beijing, China, 4–6 November 2016; Springer: Berlin, Germany, 2016; pp. 343–354.
- Chrislock, J.L. On medial semigroups. *J. Algebra* **1969**, *12*, 1–9. [[CrossRef](#)]
- Dechter, R.; Pearl, J. Structure identification in relational data. *Artif. Intell.* **1992**, *58*, 237–270. [[CrossRef](#)]

