

Article

Enhanced Matrix Power Function for Cryptographic Primitive Construction

Eligijus Sakalauskas

Department of Applied Mathematics, Faculty of Mathematics and Natural Sciences, Kaunas University of Technology, Studentu Str. 50-324, LT-51368 Kaunas, Lithuania; eligijus.sakalauskas@ktu.lt; Tel.: +370-698-78477

Received: 29 December 2017; Accepted: 7 February 2018; Published: 10 February 2018

Abstract: A new enhanced matrix power function (MPF) is presented for the construction of cryptographic primitives. According to the definition in previously published papers, an MPF is an action of two matrices powering some base matrix on the left and right. The MPF inversion equations, corresponding to the MPF problem, are derived and have some structural similarity with classical multivariate quadratic (MQ) problem equations. Unlike the MQ problem, the MPF problem seems to be more complicated, since its equations are not defined over the field, but are represented as left–right action of two matrices defined over the infinite near-semiring on the matrix defined over the certain infinite, additive, noncommuting semigroup. The main results are the following: (1) the proposition of infinite, nonsymmetric, and noncommuting algebraic structures for the construction of the enhanced MPF, satisfying associativity conditions, which are necessary for cryptographic applications; (2) the proof that MPF inversion is polynomially equivalent to the solution of a certain kind of generalized multivariate quadratic (MQ) problem which can be reckoned as hard; (3) the estimation of the effectiveness of direct MPF value computation; and (4) the presentation of preliminary security analysis, the determination of the security parameter, and specification of its secure value. These results allow us to make a conjecture that enhanced MPF can be a *candidate* one-way function (OWF), since the effective (polynomial-time) inversion algorithm for it is not yet known. An example of the application of the proposed MPF for the Key Agreement Protocol (KAP) is presented. Since the direct MPF value is computed effectively, the proposed MPF is suitable for the realization of cryptographic protocols in devices with restricted computation resources.

Keywords: matrix power function (MPF); cryptography; key agreement protocol (KAP); conjectured one-way function (OWF)

1. Introduction

Quantum computers and Internets of Things (IoTs) are the recent technologies influencing the development of cryptographic protocols. The resistance to quantum cryptanalysis became important after Peter W. Shor proposed polynomial-time quantum cryptanalysis [1] for the traditional cryptographic primitives such as Diffie–Hellman key exchange protocol, RSA and ElGamal cryptosystems, Digital signature algorithm (DSA), and Elliptic Curve cryptosystem (ECC). These primitives were based on so-called classical candidate one-way functions (OWFs), such as discrete exponent and the multiplication of large prime numbers.

The demand for the effective realization of cryptographic protocols is influenced by the Internet of Things (IoT) technology.

One of the perspective trends is the creation of OWFs, the security of which relies on the NP-hard problems [2]. So far, there are no known effective quantum cryptanalytic algorithms solving NP-hard problems; therefore, this cryptographic trend is a significant part of so-called post-quantum cryptography. Several trends to create cryptographic primitives that can resist quantum cryptanalysis

attacks, e.g., lattice-based cryptography, have been proposed, but we briefly outline those related to our work. Such a primitive is the OWF based on the multivariate quadratic (MQ) problem, the decision version of which has been proven to be NP-complete and the computational version to be NP-hard [2,3]. This OWF has some connection with the OWF presented here based on the enhanced matrix power function (MPF) problem. Despite some unsuccessful attempts [4,5], this direction is viewed as promising [6].

Another trend for building primitives in post-quantum cryptography is to use noncommuting algebraic structures. This idea was proposed by Neil R. Wagner and Marianne R. Magyarik in their paper [7], providing the origin of the trend of noncommuting cryptography [8].

So far, the main focus of this trend was directed to using noncommuting groups such as braid groups, Thompson groups, polycyclic groups, Grigorchuk groups, matrix groups, etc. A very interesting approach using an abstract noncommuting group was proposed by Anshel–Anshel–Goldfeld, outlined in the survey by Myasnikov et al. [8]. Using commutator equality and introducing the algebraic eraser notion, the authors created a key agreement protocol.

Nevertheless, almost all of these approaches were cryptanalyzed and the weaknesses of these protocols were revealed.

Several related papers can be found from up to the year 2017, but those also employ noncommuting groups in their design, e.g., [9]. As an example of application of nonsymmetric structures, the noncommutative rings have been used for noise-free symmetric fully homomorphic encryption [10]. Another example is a Learning-With-Errors (LWE) problem based on group rings [11]. It seems that there is some interest in using not only noncommuting but also nonsymmetric algebraic structures in cryptography, as we present in this paper.

Previously, we have made some attempts to use noncommuting cryptography based on the complexity of simultaneous matrix conjugacy and discrete logarithm problems to construct cryptographic primitives [12]. Some response to this publication, which was named STR protocol in short, was noticed, investigating security aspects against quantum cryptanalysis and effectivity of realization [13–16]. Nevertheless, some weaknesses of the STR protocol were found [17].

In this paper, a new enhanced matrix power function (MPF) is proposed, as a continuation of previous publications in this field. The MPF itself was first introduced in [18] for the construction of a symmetric cipher. Further results in this direction can be found in [19]. The application of MPF for the construction of asymmetric cryptographic primitives can be found in [20–24]. An analysis of the effective realization in electronic devices with restricted computation resources was presented in [24–26].

However, recently, a successful attempt to attack protocols based on MPF was presented in [27]. In their paper, the authors have shown that a discrete logarithm attack (DLA) remains a serious issue for these types of protocols. Based on their results, the authors of [27] suggested some improvements. Furthermore, in the conclusion of their paper, the authors presented a question to scientific society as to whether it is possible to construct a protocol based on MPF using noncommuting algebraic structures resistant to known attacks. One of the objectives of this manuscript is to show that this construction is possible.

The main objective of this research is to construct an MPF based on infinite, noncommuting and nonsymmetric algebraic structures. It is reasonable to expect that such a construction can be more resistant to quantum cryptanalysis, since it is effective in the case when algebraic structures have some periodicity and symmetry. This approach differs from other noncommuting cryptography approaches, outlined above, that employ symmetric algebraic structures, e.g., groups.

The following supporting tasks are formulated:

- (1) Find infinite, noncommuting, and nonsymmetric algebraic structures for the construction of the enhanced MPF, satisfying associativity conditions, which are necessary for cryptographic applications;

- (2) Prove that MPF inversion is polynomially equivalent to the solution of a certain kind of generalized multivariate quadratic (MQ) problem which can be reckoned as hard;
- (3) Estimate the effectiveness of direct MPF value computation;
- (4) Perform preliminary security analysis and determine security parameters and their secure values.

By completing these tasks, we show that proposed the MPF can be a candidate OWF for cryptographic applications, namely for the realization of a key agreement protocol (KAP) presented in Construction 1.

The rest of this paper is organized as follows:

In Section 2, we present an abstract MPF construction without the specification of concrete algebraic structures. We also present the main notations and definitions as well as a KAP in its symbolic form.

Algebraic structures for the introduction of the platform semigroup are proposed in Section 3, namely a medial semigroup S_M and a modified medial semigroup S . The normal forms of these semigroups are constructed. On the base of the exponent semiring $R = N^0$ of natural numbers with zero, the near-semiring NSR is introduced to define exponent functions on S_M and S .

In Section 4, the enhanced MPF, based on platform semigroup S and with power matrices defined over NSR , is constructed. It is proved that this MPF is associative and that the MPF problem is polynomially equivalent to a certain kind of generalized MQ problem, which is reckoned as hard. The conjecture is made that the MPF problem is hard as well. The asymptotic estimates of the effective computation of the direct MPF value are given.

In Section 5, some comments and conclusions are presented.

In Section 6 provides an illustration of a Key Agreement Protocol (KAP) with artificially small matrix orders.

2. The Construction of the Abstract MPF

An MPF is the function that computes the matrix obtained by powering some given matrix by two numerical matrices—one on the left and the other on the right. It is somewhat similar to matrix multiplication by two matrices on 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, we define the base matrix over the multiplicative (semi)group S and power matrices over some numerical (semi)ring R . We call semigroup S a *platform (semi)group*—which, according to the MPF definition, is multiplicative—and R an *exponent (semi)ring*. The appropriate matrix semigroups M_S and M_R contain base matrices and power matrices, respectively.

There is some analogy of MPF with the well-known Diffie-Hellman function in terms of the action of one algebraic structure on the other. Let us assume that we have the commutative multiplicative group of integers modulo p , $Z_p^* = \{1, 2, \dots, p-1\}$, and commutative additive group of integers modulo $p-1$, $Z_{p-1} = \{0, 1, \dots, p-2\}$. Then for any $\omega \in Z_p^*$, and any $x \in Z_{p-1}$, the following discrete exponent (power) function can be defined:

$$\omega^x = z \bmod p, z \in Z_p^*. \quad (1)$$

In this case we can say that group Z_{p-1} is acting on the group. Since this action is defined in commutative numerical algebraic structures, the notation of left and right action ${}^y\omega^x$ has no real meaning and is equivalent to $\omega^{xy} = \omega^{yx}$.

Let for example, X, Y , and W be matrices where X, Y are defined over the set of integers $Z = \{0, \pm 1, \pm 2, \dots\}$ in matrix set M_Z , and matrix W is defined over the set of complex integers $C = Z + iZ$, where $i^2 = -1$ in matrix set M_C . Then, since matrices are non-commuting, the notion of left and right action of M_Z in M_C can be introduced in the following way:

$$XWY = Z, Z \in M_C \quad (2)$$

where matrices X , W , and Y are multiplied using the convenient matrix multiplication rule.

In a similar way, we can define the two-sided MPF (or simply MPF), using matrices defined over certain algebraic structures. This symbolic form of MPF is as follows:

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

We first define one-sided MPFs in the following way:

Definition 1. The left-sided MPF corresponding to matrix W powered by matrix X on the left with MPF value equal to matrix $C = \{c_{ij}\}$ has the following form:

$${}^X W = C, \quad c_{ij} = \prod_{k=1}^m w_{jk}^{x_{ik}} \quad (4)$$

Definition 2. The right-sided MPF corresponding to matrix W powered by matrix Y on the right with MPF value equal to matrix $D = \{d_{ij}\}$ has the following form:

$$W^Y = D, \quad d_{ij} = \prod_{k=1}^m w_{ik}^{y_{kj}} \quad (5)$$

Using Definitions 1 and 2, we can now define the two-sided MPF.

Definition 3. The two-sided MPF corresponds to matrix W powered by matrix X on the left and by matrix Y on the right with MPF value equal to matrix $Q = \{q_{ij}\}$, and is expressed in the following way:

$${}^X W^Y = Q, \quad q_{ij} = \prod_{k=1}^m \prod_{l=1}^m w_{kl}^{x_{ik} \cdot y_{lj}} \quad (6)$$

The MPF definition is related to the following associativity identities.

Identity 1. MPF is one-side associative, (left-side and right-side associative, respectively) if the following identities hold:

$$\begin{aligned} Y({}^X W) &= (YX)W = YXW \\ (W^X)^Y &= W^{(XY)} = W^{XY} \end{aligned} \quad (7)$$

Identity 2. MPF is two-side associative if the following identities hold:

$$({}^X W)^Y = X(W^Y) = XW^Y \quad (8)$$

Definition 4. MPF is associative if it is one-side and two-side associative.

It follows from Definition 3 that, in general, an MPF is a function $F : M_R \times M_S \times M_R \mapsto M_S$. Further, to be short, we will use the notation MPF_S^R for the definition of an MPF with a base matrix defined over platform semigroup S and with power matrices defined over exponent semiring R . Furthermore, we present the following definitions:

Definition 5. The direct MPF value computation is to find matrix Q in Equation (3), when matrices X , Y , and W are given.

Definition 6. The inverse MPF value computation is to find matrices X and Y in Equation (3), when matrices W and Q are given.

So far, all matrices in the construction of the MPF were defined over certain commutative algebraic structures, namely, the base matrix was defined over the commutative numerical (semi)group S and power matrices over the commutative numerical ring R .

Lemma 1. *If R is a commutative numerical semiring and S is a commutative semigroup, then the MPF is associative.*

The proof can be found in [19].

In [28], the categorical interpretation of MPF, taken from [22], is presented in the context of the construction of several key agreement protocols. We slightly reformulate the notions used in this interpretation by the following statement, which is more appropriate for our study.

Statement 1. *If MPF is associative, then M_S is a multiplicative M_R -semibimodule.*

This means that there exist bilinear, right, and left actions of matrix semiring M_R on matrix semigroup M_S . According to the definition of action, it must satisfy the associative law corresponding to Definition 4. Since matrix semigroup M_S is multiplicative, then the M_R -semibimodule M_S is multiplicative in our case.

Previously, we used the MPF in our research to construct cryptographic primitives, namely, KAP, symmetric, and asymmetric encryption protocols. The suggested protocols are based on the problem, defined as follows:

Definition 7. *The MPF problem is the computation of the MPF inverse value.*

Having in mind that the existence of one-way functions (OWFs) is not proven yet, we will follow the common practice for the proposition of new candidate OWFs for cryptographic application. Consequently, the two necessary (but not sufficient) conditions for MPF to be a *candidate* (OWF) are the following.

Definition 8.

- (1) *The computation of the MPF direct value is computationally easy;*
- (2) *The MPF problem is polynomially equivalent to a certain hard problem without a known polynomial time algorithm.*

By MPF-based OWF security, we mean the complexity of computation of the inverse MPF value, which corresponds to the solution of the MPF problem. In some cases, e.g., when a discrete logarithm function can be applied to the MPF, the MPF problem can be transformed to the special system of MQ equations defined over the field or ring. In our earlier publications, we referred to this problem as the matrix MQ (MMQ) problem [20]. However, MQ and MMQ problems have significant differences. The classical MQ problem corresponds to the system of random generated MQ equations consisting of unknown quadratic and linear monomials, while the MMQ problem corresponds to the system of equations generated by random matrices and has only quadratic monomials with unknown variables.

The computation of the direct MPF value is effective and its asymptotic polynomial time estimation is presented below in Section 4.

On the other hand, referencing the complexity of certain generalized MQ problems related to the MPF_S^R problem, it is shown that there is no known polynomial-time algorithm for its solution. Thus, we make the following conjecture.

Conjecture 1. *The necessary conditions for the construction of cryptographic protocols based on MPF_S^R are the following:*

- (1) *It is associative;*

- (2) Matrices X and Y are members of some subsets M_{R_1} and M_{R_2} of commuting matrices in M_R respectively, i.e., for any $U \in M_{R_1}$ and $V \in M_{R_2}$

$$UX = XU, YV = VY \quad (9)$$

- (3) MPF_S^R satisfies the clauses of Definition 8.

The intriguing idea was to extend the MPF construction to noncommutative algebraic structures, namely, S and R , thereby giving higher expected complexity of the MPF problem and higher potential security for the construction of cryptographic primitives. The main problem with this approach was the loss of associativity of MPF, which made its application in cryptography impossible.

A breakthrough in the construction of an associative MPF based on noncommuting algebraic structures occurred when we found out that the infinite, noncommutative medial semigroup [29] (denoted by S_M) can be used. This paper presents the development of this idea by introducing modified medial semigroup S as a *platform semigroup* and a new kind of exponent functions on S with exponents defined in the specially constructed *exponent near-semiring (NSR)*. The notion of the near-semiring can be found in [30]. The generic properties of semigroup S directly induce the properties of the *NSR*. The semigroup S is constructed from the medial semigroup S_M by introducing two extra relations. Semigroups S_M and S are infinite, multiplicative, and noncommutative. The *NSR* is infinite and noncommutative with respect to the addition operation.

If matrix W is defined over the noncommuting platform semigroup S , then for the construction of cryptographic protocols it is required to introduce (use) the normal form in S . This normal form is introduced in the next section. If MPF_S^R satisfies Conjecture 1, then the construction of a key agreement protocol (KAP) in symbolic form can be realized in the following way.

Construction 1. Let $X, U \in M_{R_1}$ and $Y, V \in M_{R_2}$ (i.e., $UX = XU, YV = VY$), and let the public parameters be matrix $W \in M_S$ and subsets M_{R_1} and M_{R_2} . Then the KAP consists of the following steps.

- (1) Alice chooses two secret matrices, $X \in M_{R_1}$ and $Y \in M_{R_2}$, at random, then computes the MPF value $A = {}^X W^Y$ and sends it to Bob;
- (2) Bob chooses two secret matrices, $U \in M_{R_1}$ and $V \in M_{R_2}$, at random, then computes the MPF value $B = {}^U W^V$ and sends it to Alice;
- (3) Alice and Bob compute the same secret key $K_A = K_B = K$ in the following way:

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

The security analysis of KAP, constructed on the base of algebraic structures introduced in Section 3, is presented in Section 4.

3. The Definition of Algebraic Structures

To construct a platform semigroup for MPF, the class of multiplicative medial semigroups [25] is used. We consider medial semigroup S_M when its presentation consists of two generators a, b and relations R_M written in the following way:

$$S_M = \langle a, b | R_M \rangle \quad (10)$$

$$R_M : \omega_1 a b \omega_2 = \omega_1 b a \omega_2 \quad (11)$$

where ω_1 and ω_2 are arbitrary *nonempty* words in S_M , written in terms of generators a and b .

The reason for the introduction of the medial semigroup is the existence of the following identity, based on the relation R_M , valid for all words $\omega_1, \omega_2 \in S_M$ and any exponent $e \in \mathbb{N}^0$, where \mathbb{N}^0 is the semiring of natural numbers with zero:

$$(\omega_1 \omega_2)^e = \omega_1^e \omega_2^e \quad (12)$$

To construct platform semigroup S for the MPF in Equation (3), two extra relations R_1 and R_2 are added to S_M :

$$\begin{aligned} R_1 : ba^5b^4 &= ba^2b; \\ R_2 : ab^5b^4 &= ab^2a. \end{aligned} \quad (13)$$

These relations can be generalized in other forms. In our manuscript we will deal only with these ones.

Thus, modified medial semigroup S has the following presentation:

$$S = \langle a, b | R_M, R_1, R_2 \rangle \quad (14)$$

Notice that we define S as a multiplicative, noncommuting, noncancellative, and infinite semigroup which is a nonsymmetric algebraic structure.

Remark 1. The sum of exponents of generators a and b equals 5 on the left side of R_1 and R_2 in Equation (13) and equals 2 on the right side.

Semigroups S_M and 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 $\omega \in S_M$:

$$\omega 1 = 1\omega = \omega, \quad \omega^0 = 1, \quad 0 \in \mathbb{N}^0 \quad (15)$$

Definition 9. In any semigroup S , two words ω and ω' are equivalent, i.e., $\omega \equiv \omega'$, if ω' is obtained from ω by applying any sequence of relations defined in S to ω and vice versa. Two words ω and ω' are equal, i.e., $\omega = \omega'$ if they are written in the same form, e.g., $\omega = ab^2a^3bb^4$ and $\omega' = aa^2b^3ab^4$.

Definition 10. Equivalence class E_{q_ω} of any $\omega \in S$ consists of all words equivalent to ω .

For the introduction of the normal form in any semigroup S , we will follow the convenient normal form definition for groups.

Definition 11. The normal form in any semigroup S is defined if there exists a surjective function $\eta : S \rightarrow S_\eta$ (when $S_\eta \subset S$) based on the set of relations defined in S and satisfying the following condition: $\omega_1 \equiv \omega_2$ if, and only if, images of any ω_1 and ω_2 in S have equal images in S_η , i.e.,

$$\eta(\omega_1) = \eta(\omega_2) = \omega_{nf} \in S_\eta \quad (16)$$

Returning to the semigroup S in Equation (14), there are infinitely many equivalent words to a certain word $\omega \in S$ —e.g., let $\omega = bb^4a^5a$; then $\omega_1 = ba^5b^4a$, $\omega_2 = ba^2ba$, $\omega_3 = ba^8b^7a$, etc., are equivalent words being in the equivalence class

$$E_{q_\omega} = \left\{ \omega_1 = ba^5b^4a, \omega_2 = ba^2ba, \omega_3 = ba^8b^7a, \dots \right\}.$$

On the contrary, there are elements with equivalence classes consisting of the single element, e.g., elements a^i and b^j .

Relations in S can be used in the direction to reduce the value of exponents of generators a and b . There are also words in S for which the exponent of generators a and b cannot be reduced. We call these elements *elementary* and they are included in the set ε , where $i, j \in \mathbb{N}^0$:

$$\varepsilon = \{1, a^i, a^i b, a^i b^2, a^i b^3, a^i b^4, b^j, b^j a, b^j a^2, b^j a^3, b^j a^4, \dots\} \tag{17}$$

According to the convenient practice in noncommuting cryptography, the construction of cryptographic protocols requires the introduction of the normal form. The purpose of a normal form is the unique interpretation of operations performed in noncommuting structures. In our case, the unique interpretation of entries of matrix Q in Equation (3) is required.

It is easy to see that any $\omega \in S_M$ can be uniquely transformed to the following equivalent form using relation R_M :

$$\omega_0 = g_1 a^{i_0} b^{j_0} g_2; g_1, g_2 \in \{a, b\}; i_0, j_0 \in \mathbb{N}^0 \tag{18}$$

where g_1 is the left boundary generator and g_2 is the right boundary generator, i.e., $g_1, g_2 \in \{a, b\}$. This representation is obtained by grouping together generators a with their exponents and moving them to the left (and, analogously, generators b to the right), using relation R_M , while g_1, g_2 remain unchanged. Then, the exponents of the same grouped generators are summed up. Since relation R_M preserves the sum of exponents of generators a and b , such a representation of ω is unique.

Theorem 1. *The normal form ω_{nf} of any word ω_0 in semigroup S_M is expressed by the following function $nf : S_M \mapsto S_{M,nf}$ expressed by the relation:*

$$\omega_{nf} = \max_{\alpha, \beta} b^{\beta b} a^{r_a} b^{s_b} a^{\alpha a} = b^{\beta} a^{i_a} b^{j_b} a^{\alpha} = nf(\omega); \alpha, \beta \in \{0, 1\}; r_a, s_b \in \mathbb{N}^0 \tag{19}$$

Proof. We must prove that any word $\omega \in S_M$ can be uniquely expressed in the form of Equation (19) and that the normal forms of two words ω_1 and ω_2 are equal if, and only if, $\omega_1 \equiv \omega_2$.

According to Equation (18), let ω be expressed uniquely in the form $\omega_0 = g_1 a^{i_0} b^{j_0} g_2$. Then ω_0 can be rewritten to ω_{nf} by assigning to the exponents β and α maximal values, either 0 or 1, defined by boundary generators g_1 and g_2 . If $g_1 = b$, then $\beta = 1$; else, $\beta = 0$. If $g_2 = a$, then $\alpha = 1$; else, $\alpha = 0$. Since this representation is in one-to-one correspondence with g_1 and g_2 , it is unique.

To prove the second statement, the set of words in their normal forms $b^{\beta} a^{i_a} b^{j_b} a^{\alpha}$ is considered. In this set, the multiplication operation can be introduced by the transformation of the resulting word $\omega = \omega_1 \omega_2$ to the form ω_{nf} . We denote the set of words written in the form ω_{nf} by $S_{M,nf}$.

Lemma 2. *Let T be an additive noncommuting semigroup consisting of the tuples (β, i, j, α) , where $\alpha, \beta \in \{0, 1\} \subset \mathbb{N}^0$ and $i, j \in \mathbb{N}^0$, 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 $\varphi : S_{M,nf} \mapsto T$, which can be expressed by the following relation for any word ω_{nf} :

$$\varphi(\omega_{nf}) = \varphi(b^{\beta} a^{i_a} b^{j_b} a^{\alpha}) = (\beta, i, j, \alpha)$$

To be concise, we omit the proof.

Now we prove that if $\omega_1 \equiv \omega_2$, then Equation (16) holds, and vice versa.

Let $nf(\omega) = \omega_{nf}$ as defined by Equation (19). Normal forms of ω_1 and ω_2 are expressed in the following way: $nf(\omega_1) = \omega_{1,nf} = b^{\beta_1} a^{i_1} b^{j_1} a^{\alpha_1}$ and $nf(\omega_2) = \omega_{2,nf} = b^{\beta_2} a^{i_2} b^{j_2} a^{\alpha_2}$. Referencing Lemma 2, $\varphi(\omega_{1,nf}) = (\beta_1, i_1, j_1, \alpha_1)$ and $\varphi(\omega_{2,nf}) = (\beta_2, i_2, j_2, \alpha_2)$. Since the sum of exponents is preserved under transformations using relation R_M and according to the rule of assignment of values

0 and 1 to the exponents α_1, β_1 and α_2, β_2 , we have $\beta_1 = \beta_2, i_1 = i_2, j_1 = j_2, \alpha_1 = \alpha_2$. Since φ is an isomorphism, $\omega_{1,nf} = \omega_{2,nf}$.

The proof in the opposite direction is the following: let $\omega_{1,nf} = \omega_{2,nf} = \omega_{nf}$; then ω_{nf} represents its equivalency class with respect to relation R_M . The members of this equivalency class will be words ω_1 and ω_2 obtained by applying R_M ; hence, $\omega_1 \equiv \omega_2$.

Example 1. Let $\omega_1 = a^i, \omega_2 = b^j$, and $\omega_3 = aba^kba$, then

$$\begin{aligned} nf(\omega_1) &= b^0 a^{i-1} b^0 a = \omega_{1,nf}; \varphi(\omega_{1,nf}) = (0, i - 1, 0, 1); \\ nf(\omega_2) &= b a^0 b^{j-1} a^0 = \omega_{2,nf}; \varphi(\omega_{2,nf}) = (1, 0, j - 1, 0); \\ nf(\omega_3) &= b^0 a^{k+1} b^2 a = \omega_{3,nf}; \varphi(\omega_{3,nf}) = (0, k + 1, 2, 1). \end{aligned}$$

The normal form in S is constructed on the base of the normal form in S_M by using relations R_M, R_1 , and R_2 for the subsequent minimization of exponents i_a and j_b in Equation (19). The following functions are required to be introduced: the floor function $\lfloor i/j \rfloor$ for the ratio of natural numbers i, j and the minimum function $\min(i, j)$ for $i, j \in \mathbb{N}^0$. Taking into account Remark 1, we introduce the following variable based on these functions:

$$\mu = \lfloor \min(i, j) / 5 \rfloor. \tag{20}$$

Let us consider the word ω_{nf} written in equivalent form ω_0 in Equation (18). If $i_0 = j_0 = 5$, then when using R_M and any of relations R_1 or R_2 the following identity holds:

$$g_1 a^5 b^5 g_2 = g_1 a^2 b^2 g_2. \tag{21}$$

This relation can be applied for the one-step minimization of exponents $i_0, j_0 \geq 5$. Taking in mind Remark 1, the exponents i_0 and j_0 can be expressed in the following unique way:

$$i_0 = n_i 5 + r_i, j_0 = n_j 5 + r_j; n_i = \lfloor i_0 / 5 \rfloor, n_j = \lfloor j_0 / 5 \rfloor; r_i, r_j < 5. \tag{22}$$

Then, using variable μ defined in Equation (20), the word ω_0 can be rewritten in the following equivalent form:

$$\omega' = g_1 (a^5 b^5)^\mu a^{i-5\mu} b^{j-5\mu} g_2. \tag{23}$$

Taking into account relations R_M, R_1 , and R_2 and Equation (21), we obtain the following word ω_1 equivalent to ω_0 and $\omega' \in S$:

These considerations allow us to create the normal form in semigroup S .

$$\omega_1 = g_1 a^{i_0-3\mu} b^{j_0-3\mu} g_2 = g_1 a^{i_1} b^{j_1} g_2 \tag{24}$$

Theorem 2. For the given word ω_{nf} in normal form of S_M , its normal form ω_η in S is represented by the function $\eta : S_M \mapsto S$ and expressed by a finite n -step recurrent minimization procedure of exponents i_a and j_b in Equation (19) using relations R_M, R_1 , and R_2 :

$$\omega_\eta = \min_{i_a, j_b} \omega_{nf}(i_a, j_b) = \min_{i_a, j_b} \max_{\beta, \alpha} b^\beta a^{i_a} b^{j_b} a^\alpha = b^\beta a^{i_a} b^{j_b} a^\alpha = \eta(\omega_{nf}). \tag{25}$$

Proof. We rewrite word ω_{nf} to ω_0 according to Equation (18) and perform the minimization procedure for this word, obtaining word ω_1 :

$$\omega_1 = \min_{i_0, j_0} \omega_0(i_0, j_0) = \min_{i_0, j_0} g_1 a^{i_0} b^{j_0} g_2. \tag{26}$$

Let both $i_0, j_0 \geq 5$. Then, the first step to minimize exponents i_0 and j_0 is performed using Equation (18)–(21). As a result, the new equivalent word $\omega_1 = g_1 a^{i_1} b^{j_1} g_2$ is obtained, where $i_1 = i_0 - 3\mu_0, j_1 = j_0 - 3\mu_0$, and $\mu_0 = \lfloor \min(i_0, j_0)/5 \rfloor$.

The unique word ω_0 representation by ω_1 follows from the unique representation of i_0 and j_0 by Equation (22). If both $i_1, j_1 \geq 5$ in ω_1 , then the second step of minimization is performed analogously, and the unique word ω_2 is obtained with exponents $i_2 = i_1 - 3\mu_1, j_2 = j_1 - 3\mu_1$ and $\mu_1 = \lfloor \min(i_1, j_1)/5 \rfloor$.

This recurrence is continued up to the $(n - 1)$ th step while relation $i_{n-1}, j_{n-1} \geq 5$ does not hold. The unique word ω_{n-1} is obtained in the form:

$$\omega_{n-1} = g_1 a^{i_{n-1}} b^{j_{n-1}} g_2; \tag{27}$$

$$i_{n-1} = i_{n-2} - 3\mu_{n-2}, j_{n-1} = j_{n-2} - 3\mu_{n-2}; \tag{28}$$

$$\mu_{n-2} = \lfloor \min(i_{n-2}, j_{n-2})/5 \rfloor. \tag{29}$$

If ω_{n-1} is in the set of elementary words ϵ defined above in Equation (17), then the minimization procedure stops. The word ω_{n-1} is uniquely transformed to the normal form in S by the function $nf(\omega_{n-1}) = \omega_\eta$ in Equation (19). Otherwise, the word ω_{n-1} is subsequently minimized using the last n th step minimization procedure according to the following two alternative conditions. If $\beta_{n-1} = 1, i_{n-1} \geq 5$, and $j_{n-1} = 4$, then the final n th step of minimization is applied by using relation R_1 in Equation (11). If $\alpha_{n-1} = 1, i_{n-1} = 4$, and $j_{n-1} \geq 5$, then R_2 is applied to end the minimization process. Finally, the unique normal form $\omega_n \in S$ in S is obtained, represented by Equation (25).

So far, we have considered exponent functions defined on S , determined by non-negative exponents in semiring $R = N^0$. We generalize these functions by introducing certain “imaginary” exponents, yielding “complex” exponents and having some weak analogy with complex numbers in classical numerical algebra based on the imaginary unit $i (i^2 = -1)$.

According to [26] and other related sources, the set of all mappings on an additive semigroup with identity zero is the standard example of a so-called near-semiring. It is a closed algebraic structure with two operations, namely, addition and multiplication (composition) of mappings.

A near-semiring is a nonempty set A with two binary operations “+” and “·”, and a constant 0 such that $(A; +; 0)$ is a monoid (not necessarily commutative) and $(A; \cdot)$ is a semigroup. These structures are related by one (right or left) distributive law, and, accordingly, the 0 is the one-side (right or left, respectively) absorbing element.

Following this general construction, we introduce a special kind of near-semiring (NSR), defining exponent functions on the modified medial semigroup S . In order to preserve the main properties of exponent functions (they are specified in Equation (39) below), we must replace the one-side distributive law and absorbing (zero) element law by two-sided ones, respectively.

Despite the difference between the convenient definition and ours, we will assume that NSR introduced below stands for the *special-type* near-semiring. The notion *special-type* is implied by the fact that medial semigroups are special-type semigroups and that exponent functions are special-type functions on these semigroups.

Definition 12 A near-semiring NSR is a nonempty set with two binary operations “+” and “·”, such that $(NSR; +; 0)$ is an additive monoid with neutral element $0 \in N^0$, and $(NSR; \cdot; 1)$ is a multiplicative monoid with neutral element $1 \in N^0$, satisfying the following (two-sided) axioms for all x, y, z in NSR:

$$\begin{aligned} x \cdot (y + z) &= x \cdot y + x \cdot z; \\ (y + z) \cdot x &= y \cdot x + z \cdot x; \end{aligned} \tag{30}$$

$$0 \cdot x = x \cdot 0 = 0. \tag{31}$$

Since exponent functions are mappings on the modified medial semigroup S , defined by exponent values in the NSR , we supply the monoid $(NSR; +; 0)$ with the following extra relation R^+ of the medial semigroup type introduced in Equation (11). For all nonzero x, y, z_1, z_2 in NSR , the following relation R^+ holds:

$$R^+ : z_1 + x + y + z_2 = z_1 + y + x + z_2 \tag{32}$$

In addition, we assume that multiplicative monoid $(NSR; \cdot, 1)$ is commutative, i.e., for all $x, y \in NSR$,

$$x \cdot y = y \cdot x. \tag{33}$$

In analogy with complex numbers over the integers or reals, we introduce the “imaginary” unit denoted by ι and satisfying the following relations for all $u \in N^0$:

$$\iota \cdot u = u \cdot \iota; \iota^2 = 1; 1 \in N^0 \tag{34}$$

where the first relation is implied by Equation (33).

The exponent ι of generators a and b in S is defined in the following way:

$$a^\iota = b; b^\iota = a. \tag{35}$$

We claim, that NSR consists of the union of the following sets:

$$NSR = (N^0 + \iota N^0 + N^0) \cup (\iota N^0 + N^0 + \iota N^0) \tag{36}$$

where the set $N^0 + \iota N^0 + N^0$ defines the class of elements $\{t + \iota \cdot u + v\}$ and the set $\iota N^0 + N^0 + \iota N^0$ defines the class $\{\iota \cdot t + u + \iota \cdot v\}$, where $t, u, v \in N^0$.

Theorem 3. *The set NSR is closed with respect to addition and multiplication operations and is a near-semiring according to Definition 12.*

Proof: The closure of NSR follows directly from the relation Equations (11)–(13). Indeed, we can consider only two classes of elements in NSR : $\{t + \iota \cdot u + v\}$ defining the set $N^0 + \iota N^0 + N^0$ and $\{\iota \cdot t + u + \iota \cdot v\}$ defining the set $\iota N^0 + N^0 + \iota N^0$, where $t, u, v \in N^0$. The classes of elements $\{t + \iota \cdot u\} = N^0 + \iota N^0$ and $\{\iota \cdot t + u\} = \iota N^0 + N^0$ are the partial cases of corresponding sets $N^0 + \iota N^0 + N^0$ and $\iota N^0 + N^0 + \iota N^0$, respectively, when $v = 0$. After performing operations between the elements of classes $\{t + \iota \cdot u\}$ and $\{\iota \cdot t + u\}$ and grouping similar terms according to relation R^+ in Equation (32), we obtain an element either in the set $\iota N^0 + N^0 + \iota N^0$ or in $N^0 + \iota N^0 + N^0$. The operations with any other kind of pairs of elements does not yield any other elements except the elements in the sets $N^0 + \iota N^0 + N^0$ and $\iota N^0 + N^0 + \iota N^0$ when similar terms are grouped using relation R^+ .

Theorem 4. *The near-semiring NSR is associative.*

Proof: Since, conveniently, additive and multiplicative monoids $(NSR; +; 0)$ and $(NSR; \cdot, 1)$ are associative, the associativity of mixed operations (multiplication and addition) is implied by distributive law Equation (30) and relation R^+ . Hence, NSR is associative.

Referencing to Equations (30)–(35) and Theorem 3, the only two kinds of “complex” exponents $x = t + \iota \cdot u + v$ and $y = \iota \cdot t + u + \iota \cdot v$, where $t, u, v \in N^0$, can be defined for any generator a or b . For example, for generator a we claim, that

$$\begin{aligned} a^x &= a^{t+\iota \cdot u+v} = a^t a^{\iota \cdot u} a^v = a^t b^u a^v; \\ a^y &= a^{\iota \cdot t+u+\iota \cdot v} = a^{\iota \cdot t} a^u a^{\iota \cdot v} = b^t a^u b^v. \end{aligned} \tag{37}$$

Generalizing the last equations to any word ω in S , we obtain the following relations:

$$\begin{aligned} \omega^x &= \omega^{t+l \cdot u+v} = \omega^t \bar{\omega}^u \omega^v; \\ \omega^y &= \omega^{t+l+u+l \cdot v} = \bar{\omega}^t \omega^u \bar{\omega}^v. \end{aligned} \tag{38}$$

where the word $\bar{\omega}$ is obtained from ω by interchanging generators (a to b and b to a , respectively), according to Equations (37).

It is evident that the exponent function in S_M and S satisfies the following convenient identities for any $\omega, \omega_1, \omega_2 \in S(S_M)$ and any $x, y \in NSR$:

$$\begin{aligned} \omega^x \omega^y &= \omega^{(x+y)} = \omega^{x+y}; \\ (\omega^x)^y &= \omega^{(x \cdot y)} = \omega^{x \cdot y}; \\ (\omega_1 \omega_2)^x &= \omega_1^x \omega_2^x. \end{aligned} \tag{39}$$

Theorem 5. Let ω be either in S_M or in S and $x \in NSR$; then the normal form of ω^x in S is expressed by the word $b^\beta a^i b^j a^\alpha$ defined in Theorem 2.

Proof: Let $\omega \in S_M$ and $x \in NSR$. Then, referencing Theorems 3 and 4 and using Equations (37)–(39), ω^x can be transformed to the word $\omega \in S_M$ with exponents of generators in N^0 . Then, by applying Theorem 1, word ω can be transformed to its normal form ω_{nf} in S_M , and by applying Theorem 2, to its normal form ω_η in S . If $\omega \in S$, the same procedure is applied.

Hence, we constructed near-semiring NSR , defining exponent functions on semigroups S_M and S .

4. Enhanced MPF Construction and Its Security Investigation

According to notation introduced in Section 2, we are dealing with the problems denoted by $MPF_{S_M}^{N^0}, MPF_S^{N^0}, MPF_{S_M}^{NSR}$, and MPF_S^{NSR} .

Theorem 6. $MPF_{S_M}^{NSR}$ and MPF_S^{NSR} are associative, i.e., they satisfy the identities given in Equations (7) and (8).

Proof: The associativity identities are satisfied due to semigroups S_M and S relation Equations (11) and (13), NSR relation Equation (32), and properties of “complex” exponents (37)–(39).

We start from the consideration of $MPF_{S_M}^{N^0}$ and $MPF_S^{N^0}$ problems. We assume that, initially, the base matrix W entries ω_{ij} in Equation (3) are in semigroup S and are expressed in normal forms according to Equation (25) (Theorem 2), i.e.,

$$\omega_{lj} = b^{\beta_{lj}} a^{s_{lj}} b^{t_{lj}} a^{\alpha_{lj}}. \tag{40}$$

Power matrices $X = \{x_{il}\}$ and $Y = \{y_{jk}\}$ are defined over the semiring N^0 , i.e., $x_{il}, y_{jk} \in N^0$, where $i, j, k, l \in I^{(m)} = \{1, 2, \dots, m\}$. Using Equation (40), the entry q_{ik} of matrix Q in Equation (3) can be expressed in the following way:

$$Q = \{q_{ik}\}; q_{ik} = b^{\sum_j \sum_l (\beta_{lj}) \cdot x_{il} \cdot y_{jk}} a^{\sum_j \sum_l (s_{lj}) \cdot x_{il} \cdot y_{jk}} b^{\sum_j \sum_l (t_{lj}) \cdot x_{il} \cdot y_{jk}} a^{\sum_j \sum_l (\alpha_{lj}) \cdot x_{il} \cdot y_{jk}} \tag{41}$$

Referencing Equation (19) (Theorem 1), every q_{ik} can be transformed to its normal form $q_{ik,nf}$ in S_M , thus obtaining matrix Q_{nf} :

$$Q_{nf} = \{q_{ik,nf}\} = \{b^{\beta_{ik}} a^{i_{a,ik}} b^{j_{b,ik}} a^{\alpha_{ik}}\} \tag{42}$$

where exponents $i_{a,ik}$ and $j_{b,ik}$ are exponents in N^0 , $\alpha_{ik}, \beta_{ik} \in \{0, 1\}$, and $i, j, k, l \in I^{(m)}$.

The latter Equations (41) and (42) represent the system of equations corresponding to $MPF_{S_M}^{N^0}$ in Equation (3). According to [31], it can be called a special type of multivariate quadratic power problem, when unknown monomials are presented in exponents. However, the results of NP-completeness presented in [31] cannot be applied to this problem since it is defined over different algebraic structures with additional commutation constraints (Equation (9)) to random generated matrices X, Y .

The $MPF_{S_M}^{N^0}$ problem can be transformed to an $MPF_S^{N^0}$ problem, transforming entries $q_{ik,nf}$ to their normal forms $q_{ik,\eta} \in S$. Then, according to Equation (25) (Theorem 2), the normal forms of $q_{ik,\eta}$ are found after the n -step recurrent minimization procedure:

$$q_{ik,\eta} = b^{\beta_{ik}} a^{i_{ik}} b^{j_{ik}} a^{\alpha_{ik}} = \min_{i_{a,ik}, j_{b,ik}, \beta_{ik}, \alpha_{ik}} \max b^{\beta_{ik}} a^{i_{a,ik}} b^{j_{b,ik}} a^{\alpha_{ik}} \tag{43}$$

As a result, we obtain matrix $Q_\eta = \{q_{ik,\eta}\}$, which replaces matrix Q in Equation (3).

In the case of an $MPF_{S_M}^{N^0}$ problem, the explicit relations Equations (41) and (42) can be used, relating the exponents of the entries of matrix $Q_{nf} = \{q_{ik,nf}\}$ with the entries of power matrices $X = \{x_{il}\}$ and $Y = \{y_{jk}\}$, and with the exponents of generators a and b in the entries of the base matrix $W = \{\omega_{ij}\}$. Since (in this case) x_{il} and y_{jk} are elements in N^0 , the sum of exponents of generators a and b in the word q_{ik} are preserved and can be expressed by the following formulas:

$$\begin{cases} XE_a Y = H_a; \\ XE_b Y = H_b. \end{cases}$$

These equations can be rewritten in a matrix form by introducing the following matrix notations: $H_a = \{i_{a,ik} + \alpha_{ik}\}$, $H_b = \{j_{b,ik} + \beta_{ik}\}$, $E_a = \{s_{li} + \alpha_{li}\}$, and $E_b = \{t_{li} + \beta_{li}\}$, where, as previously, $i, j, k, l \in I^{(m)} = \{1, 2, \dots, m\}$. Then

$$\begin{aligned} \sum_j \sum_l (s_{lj} + \alpha_{lj}) \cdot x_{il} \cdot y_{jk} &= i_{a,ik} + \alpha_{ik}; \\ \sum_j \sum_l (t_{lj} + \beta_{lj}) \cdot x_{il} \cdot y_{jk} &= j_{b,ik} + \beta_{ik}. \end{aligned} \tag{44}$$

Matrices E_a, E_b and H_a, H_b are obtained from matrices W and $Q = Q_{nf}$ in Equation (3), respectively.

Referencing Definition 9, we can redefine $MPF_{S_M}^{N^0}$ as follows:

Definition 13. The $MPF_{S_M}^{N^0}$ problem is to find matrices X and Y in Equation (44), satisfying commutation conditions Equation (9), when matrices E_a, E_b and H_a, H_b are given.

Equation (44) represents a special type of multivariate quadratic (MQ) problem, since it is generated by randomly generated matrices X and Y and defined over the semiring N^0 . In our previous publication, we called this kind of problem a matrix MQ (MMQ) problem [20]. MMQ equations do not have linear monomials and consist only of quadratic ones. The significant difference between MQ problems and MMQ problems, represented by Equation (44), is that in the latter case matrix equations are defined over the semiring N^0 rather than over the field or ring.

Structurally, the $MPF_{S_M}^{N^0}$ problem is related with the known exact non-negative matrix factorization (Exact NMF) problem [32]. We denote the non-negative matrix H with m rows and n columns by $H_{m \times n}$.

Definition 14. Exact NMF problem: The input is a matrix $H_{m \times n}$ with non-negative entries whose rank is exactly k , for $k \geq 1$. The output is a pair of non-negative matrices $X_{m \times k}, Y_{k \times n}$, satisfying the equation

$$H_{m \times n} = X_{m \times k} Y_{k \times n}. \tag{45}$$

If no such pair of matrices $(X_{m \times k}, Y_{k \times n})$ exists, then the output is a statement of the nonexistence of the solution. The decisional version of the Exact NMF problem takes the same input and gives as output “YES” if such a $(X_{m \times k}, Y_{k \times n})$ pair exists and outputs “NO” otherwise.

In [32] it is proved that the Exact NMF problem is NP-hard.

In [33] the exponential—or even super-exponential—time for a generalization of the Exact NMF problem solution was presented.

In [34], a polynomial-time algorithm for the Exact (and Approximate) NMF problem for every constant k was given. This result holds also for the instances when $m = n = k$, corresponding to instances of matrix Equation (44), assuming that matrices E_a, E_b are identity matrices.

However, this trivial (polynomial-time) reduction from Exact NMF to Equation (44) does not correspond to the $MPF_{S_M}^{N^0}$ problem according to Definition 14, since Exact NMF do not include commutativity conditions on matrices X and Y in Equation (9). The Exact NMF problem complexity with commutativity constraints is not yet known and, therefore, this relation cannot tell anything about the $MPF_{S_M}^{N^0}$ problem complexity.

In the case of the $MPF_S^{N^0}$ problem, the entries of matrix Q in Equation (3) are transformed to the normal forms of semigroup S by the finite minimization procedure of exponents of generators a and b , according to Theorem 2, thus obtaining matrix Q_η . Then, instead of Equation (3), we have the following equation:

$$\tilde{X}W\tilde{Y} = Q_\eta, \quad (46)$$

where \tilde{X} and \tilde{Y} are any matrices satisfying the commutation conditions in Equation (3).

This equation will not have a solution with high probability, since, in general, the resulting exponents of generators in the entries of matrix Q_η will be too small to satisfy Equation (46). For example, let us consider the left side MPF in Equation (2) and, for simplicity, let $m = 2$. Let, for example, $c_{11} = (aba)^2(ba)^3$; then, after powering words a^5b^3a and ba by exponents 2 and 3, respectively, and transforming the resulting word to the normal form of semigroup S_M , we obtain the word $a^{15}b^{12}$. When this word is transformed to the normal form of S , we obtain $c_{11} = a^6b^3$. As we see, there are no two exponents to obtain the word a^6b^3 by exponentiating initial words a^5b^3a and ba without their minimization, i.e., transforming the exponentiation result to the normal form of S . The same is valid when Equation (46) is transformed to the system of matrix equations in the form of Equation (44).

Theorem 7. *If instances of the $MPF_S^{N^0}$ problem are generated in such a way that entries of matrix W are written in the normal form of S and the product of any two entries of matrix W is reducible by relations R_M, R_1, R_2 in Equations (11) and (13), then Equation (46) has solution if, and only if, matrix X has exactly one entry equal to $1 \in N^0$ in each row and matrix Y has exactly one entry equal to $1 \in N^0$ in each column, while all other entries in matrices X and Y are equal to $0 \in N^0$.*

Proof. Sufficiency: Assume that matrix X has exactly one entry equal to $1 \in N^0$ in each row and matrix Y has exactly one entry equal to $1 \in N^0$ in each column, while all other entries in matrices X and Y are equal to $0 \in N^0$. Then matrix Q_η entries in Equation (46) will be equal to certain entries of matrix W depending on the distribution of 1s in matrices X and Y . So, Equation (46) will have a solution.

Necessity: Assume that Equation (46) has a solution, then powers of generators a and b in entries of elements of matrix Q_η are not reduced using R_1, R_2 . Taking in mind that the product of any two entries of matrix W is reducible, we conclude that matrix X has exactly one entry equal to $1 \in N^0$ in each row and matrix Y has exactly one entry equal to $1 \in N^0$ in each column, while all other entries in matrices X and Y are equal to $0 \in N^0$.

The probability is negligible that a random generated matrix X has one entry equal to $1 \in N^0$ in each row, and Y has one entry equal to $1 \in N^0$ in each column, with other entries in X and Y equal to $0 \in N^0$. For example, if entries of $m \times m$ matrices X and Y are randomly generated with uniform

distribution in the set of natural numbers $\{0, 1, \dots, 2^q - 1\}$, then this probability is $p = m^{2m} 2^{-2qm^2}$. For example, for $m = 4$ and $q = 3$, the probability is $p = 2^{-64}$; for $m = 8$ and $q = 3$, it is $p = 2^{-336}$. For brevity, the following proposition is formulated without proof.

Proposition 1. *If instances of matrix W are generated at random and satisfy the conditions of Theorem 7, and matrices X and Y are generated at random with uniform distribution in the set of natural numbers $\{0, 1, \dots, 2^q - 1\}$, then Equation (46) has a solution with asymptotic, negligible, exponentially decreasing probability in parameters m and q .*

The possible way to obtain an equivalent system in order to find any matrices \tilde{X} and \tilde{Y} , when matrices W and $Q_\eta = \{q_{ik,\eta}\}$ are given, is to transform matrix Q_η to equivalent matrix Q_R by using relations R_M, R_1, R_2 in Equations (11) and (13), in the reverse direction than was done when matrix Q in Equation (3) was transformed to the normal form Q_η . We denote the transformation of the word ω in the reverse direction in S by R_ω^{-r} , where r denotes the number of transformation steps. Then we denote the transformation of $q_{ik,\eta}$ in the reverse direction by r_{ik} steps by $R_{ik}^{-r_{ik}}$. To express the reverse transformation of matrix Q_η we construct a transformation matrix $R_\eta = \{R_{ik}^{-r_{ik}}\}$, $i, k \in I^{(m)} = \{1, 2, \dots, m\}$. Then, using the Hadamard matrix product \odot , the matrix $Q_R = R_\eta \odot Q_\eta$ is obtained; this can be expressed in the following way:

$$\tilde{X}W\tilde{Y} = Q_R \quad (47)$$

As a result, the powers of generators a and b in Q_R will be increased, expecting to satisfy Equation (47) with new matrix Q_R instead of Q_η in the right side. However, the transformation of words to their normal forms is a surjective mapping, denoted by η above. In general, a word normal form represents infinitely many equivalent words in S . Therefore, if the words in their normal forms are presented in an $m \times m$ matrix Q_η , then it is not clear which equivalent matrix Q_R to choose to guarantee the solution of Equation (47). If matrices X and Y are generated at random, then definitely, for every entry $q_{ik,\eta}$ of Q_η , the different number of steps r_{ik} will be required to search for matrix Q_R satisfying Equation (47). If we are transforming matrix Q_η in the reverse direction in at most one step, i.e., $r < 2$, then the exhausting set of possible equivalent matrices consists of 2^{m^2} elements. If $r > 1$, then this set consists of $(r - 1)^{m^2}$ elements and is super-exponentially growing in m . For every matrix Q_R in this set, the analogous system of matrix equations like Equation (44) can be retrieved and this system will have a solution if, and only if, Equation (47) has a solution.

Definition 15 *The $MPF_S^{N^0}$ problem is to find any \tilde{X} and \tilde{Y} satisfying Equation (47) and commutation conditions Equation (9), when matrices W and Q_η are given, where $Q_R = R_\eta \odot Q_\eta$ and R_η is any reverse transformation matrix found by a random search procedure in an exponentially large set, providing solution existence of Equation (47).*

Dichotomy 1. *If the search of matrix Q_R , providing the solution of Equation (47), can be performed in polynomial time, then the decisional $MPF_S^{N^0}$ problem is in NP; otherwise, it is not in NP and not in Co-NP.*

The MPF_S^{NSR} problem can be derived from Equation (3) if matrices X and Y are defined over the NSR and are in M_{NSR} , and matrix W is defined over the S and is in M_S . We will show that this problem is much more complicated than the $MPF_S^{N^0}$ problem. It inherits the $MPF_S^{N^0}$ problem's difficulties, since the statements of Theorem 6 and Proposition 1 can be reformulated for the MPF_S^{NSR} problem as well. Therefore, the analogue of Equation (46) will not have a solution with an overwhelming probability and a search procedure for the suitable matrix Q_R in the right side of Equation (46) must be performed in the same way as in the case of the $MPF_S^{N^0}$ problem. An Equation of (47) type can be found with the difference that matrices \tilde{X} and \tilde{Y} are defined over the NSR . That is what the MPF_S^{NSR} problem inherits from the $MPF_S^{N^0}$ problem together with the same formal Definition 15. Therefore, for

further consideration, the references to Equations (46) and (47) will be used to represent the MPF_S^{NSR} problem, as well.

Recall that, according to Lemma 2 in Theorem 1, T is an additive noncommuting semigroup consisting of the tuples (β, i, j, α) and there exists an isomorphism $\varphi : S_{M,nf} \mapsto T$, where $S_{M,nf}$ is a semigroup of words in normal forms of S_M . Recall that $\varphi(b^\beta a^i b^j a^\alpha) = (\beta, i, j, \alpha)$. Since NSR possesses an imaginary variable, which we denoted by ι , the transformation of Equation (47) to a system of the same type as Equation (44) is not possible, since exponents of generators a and b are confused and cannot be equated. We denote the set of matrices over non-commuting additive semigroup T by M_T , which is a semigroup with respect to the matrix sum, when matrix elements are summed according to Lemma 2 in Theorem 1.

Theorem 8. *The solution of the $MPF_{S_M}^{NSR}$ problem is polynomially equivalent to the solution of matrix MQ (MMQ) problem defined by left–right bilinear action of matrices in M_{NSR} on matrix semigroup M_T .*

Proof. Referencing isomorphism φ in Theorem 1 and Equations (14) and (35), the action \bullet of the “imaginary” unit ι in NSR to the tuple (β, i, j, α) in T for distinct $\alpha, \beta \in \{0, 1\}$ and $i, j \in N^0$ is expressed in the following way:

$$\begin{aligned} \iota \bullet (0, i, j, 0) &= (0, i, j, 0) \bullet \iota = (0, i - 1, j - 1, 0); \\ \iota \bullet (0, i, j, 1) &= (0, i, j, 1) \bullet \iota = (1, j, i, 0); \\ \iota \bullet (1, i, j, 0) &= (1, i, j, 0) \bullet \iota = (0, j, i, 1); \\ \iota \bullet (1, i, j, 1) &= (1, i, j, 1) \bullet \iota = (0, j + 1, i + 1, 0). \end{aligned}$$

Referencing Equations (37) and (38), the action of “complex” exponents $x = t + \iota \cdot u + v$ and $y = \iota \cdot t + u + \iota \cdot v$ (where $t, u, v \in N^0$) to the elements of T can be found. For example, if $\alpha = \beta = 1$, the following relation takes place for x :

$$x \bullet (1, i, j, 1) = (1, i, j, 1) \bullet x = (1, ti + u(j + 1) + vi + t + v - 1, tj + u(i + 1) + vj + t + v - 1, 1). \tag{48}$$

For distinct $\alpha, \beta \in \{0, 1\}$ and two kinds of “complex” exponents x and y , we obtain eight equations of type Equation (48), which are omitted here for brevity.

Since T is isomorphic to the sub-semigroup of normal forms of the medial semigroup S_M , we can claim that there exists a bilinear (right and left) action of the matrix near-semiring M_{NSR} on matrix semigroup M_T in the same way as bilinear action is defined for MPF in Equation (3). Since the set of words $\{\omega_\eta\}$ in normal forms of S is a subset of $S_{M,nf}$, then by applying isomorphism φ to matrix W and Q_η in Equation (46) we obtain matrices E and P_η in M_T , respectively:

$$\varphi(W) = E, \varphi(Q_\eta) = P_\eta. \tag{49}$$

Then, referencing Equations (30)–(39), the following relations take place:

$$\varphi\left({}^X W^Y\right) = X \bullet \varphi(W) \bullet Y = X \bullet E \bullet Y \tag{50}$$

where \bullet is an MPF-induced action operation of matrices in M_{NSR} to matrices in M_T and corresponds to formal matrix multiplication as in Equation , while multiplication between entries is performed according to Equation (48).

Since φ is an isomorphism and is computed in polynomial time, by combining Equations (49) and (50), Equation (48) can be rewritten in the following form:

$$X \bullet E \bullet Y = P_\eta. \tag{51}$$

Analogously to Equation (48), the obtained system will not have a solution with overwhelming probability and, hence, the same search procedure of matrix $P_R = \varphi(Q_R)$ must be performed to solve the MPF_S^{NSR} problem. Then Equation (51) has to be replaced by the following equation:

$$\tilde{X} \bullet E \bullet \tilde{Y} = P_R. \quad (52)$$

To prove the polynomial equivalence of Equations (47) and (52), we must prove that if \tilde{X} and \tilde{Y} is a solution of Equation (47), then it is a solution of Equation (52), and vice versa. This statement holds, since φ is the polynomial-time computable isomorphism and since identities Equations (30)–(39) hold.

Referencing Theorem 8, the following polynomially equivalent definition to Definition 15 can be formulated.

Definition 16. *The MPF_S^{NSR} problem is to find any \tilde{X} and \tilde{Y} over NSR satisfying Equation (52) and commutation conditions Equation (9), when matrices E and P_η are given, where $P_R = R_\eta \odot P_\eta$, and R_η is any reverse transformation matrix, found by a random search procedure in an exponentially large set, providing the solution existence of Equation (52).*

Since isomorphism φ is computed effectively, an analogous dichotomy can be formulated in this case.

Dichotomy 2. If the procedure of the matrix P_R search can be performed in polynomial time, then the decisional MPF_S^{NSR} problem is in NP; otherwise, it is not in NP and not in Co-NP.

The MPF_S^{NSR} problem according to Definition 16 represents a new kind of MQ problem—namely a matrix MQ (MMQ) problem—which is not defined over the (finite) field or ring. It can be interpreted as the bilinear action of matrices X and Y over the NSR to matrix E over the infinite additive noncommuting semigroup T .

We are making a conjecture that this problem is hard, since it is defined over much more complicated algebraic structures than the classical MQ problem which is used for the creation of cryptographic primitives, e.g., in the HFE cryptosystem. The classical solution methods of the MQ problem, such as Grobner bases or Linearization, are not adequate in this case, since we are dealing with noncommuting and nonsymmetric algebraic systems. So far, there is no understanding on how to deal with system Equation (52). By way of analogy with the classical MQ problem, we can say that matrix Equation (52) corresponds to the system of m^2 equations and $2m^2$ unknown variables in NSR , satisfying Equations (37) and (38). In terms of the MQ problem, this system is neither over-defined, nor under-defined; that increases its complexity.

Conjecture 2. *Since the MPF_S^{NSR} problem is polynomially equivalent to the special kind of generalized MQ problem, which is reckoned to be hard, it can be considered as a candidate one-way function (OWF) for the construction of cryptographic primitives.*

The effectiveness of the computation of the direct MPF_S^{NSR} value is based on the computation of small exponents using multiplication and addition. The size of exponents can be up to 8 bits. After powering matrix W by matrices X and Y in Equation (3), the generators in entries of the obtained matrix are rearranged using Equation (11) and exponents of same generators are summed up, representing the product of the same generators by the one corresponding generator with a certain exponent. After that, the transformation to the normal form of the semigroup S is performed. The asymptotic computation complexity is estimated using the complexity of multiplications of three matrices presented in Equation (2) with asymptotic running time $\mathcal{O}(m^3)$ and using the complexity of the transformation of words to their normal forms in S , using a finite step minimization procedure, with asymptotic running time $\mathcal{O}(\log^2 m)$. Then, the complexity of the direct MPF_S^{NSR} value computation is $\mathcal{O}(m^3 \log^2 m)$.

The security parameter is the order m of matrices used in the MPF. Since there is no theory dealing with Equation (52) due to its definition over noncommuting and nonsymmetric algebraic structures, the secure value of security parameter m is determined by heuristic analogy with the known classical MQ problem. For example, there is no theory on finding a probability of solution existence for an MPF problem for random chosen matrix Q in Equation ((3) as it can be done easily for the system of linear equations. Even for the classical MQ problem and decades of its investigation, based on more or less developed theory, this problem is investigated using a modelling technique on toy examples [35]. Hence, it is impossible so far to obtain a rigorous lower bond for the security parameter m for the MPF_S^{NSR} problem, taking in mind Definition 16.

Many authors have shown that known methods for the solution of a randomly generated MQ problem (e.g., based on Grobner bases and Linearization) rarely give results better than an exhaustive search method. Since, according to Equation (52), the MPF problem is isomorphic to some kind of generalized MQ problem, we accept the assumption that, at this moment, the best attack to the MPF problem could be the exhaustive search attack.

Referencing the analogy of a randomly generated MQ problem over the field $GF(2)$ —when the solution of a system of equations with more than 80 equations and 80 variables, using known methods of solution (say, Grobner bases or Linearization), is intractable—the security parameter value for the MPF problem is determined. In this case, the exhaustive search of 80 variables in $GF(2)$ runs in time 2^{80} . For example, considering the hidden field equation (HFE) algorithm described in the extended version of [35], the attack presented in [36] is expected to run in time 2^{152} , when the extended linearization (XL) method is used. According to [37], a possible improvement of this attack runs in time 2^{82} , which is still worse than the 2^{80} complexity of exhaustive search.

Taking an analogy of these considerations, we propose to choose $m \geq 10$, hence determining the lower bound of the m value heuristically, which may seem to have extra in reserve. If $m = 10$, then the matrix Equation (52) corresponds to $m^2 = 100$ equations with $2m^2 = 200$ unknown variables in NSR . We are making a conjecture that it will be currently enough to prevent any cryptanalysis attack (though unknown yet) on the key agreement protocol presented in Construction 1, including by an exhaustive search attack. In this consideration, the additional complexity to find matrix P_R in Equation (52) was not taken into account, which contributes to a significant part of the MPF_S^{NSR} problem's complexity.

According to Construction 1, the public key (PuK) for the KAP construction is matrix W and the private key (PrK) is matrices X, Y (and U, V , respectively) of dimension $m \times m$. Let entries $w_{lj} = b^{\beta_{lj}} a^{r_{lj}} b^{s_{lj}} a^{\alpha_{lj}}$; $a, b \in S$; $\alpha_{lj}, \beta_{lj} \in \{0, 1\}$; $r_{lj}, s_{lj} \in N$ of matrix W be expressed in the normal form of S according to the Theorem 2. Assume, that w_{lj} is expressed by 8 bits by assigning two bits to α_{lj}, β_{lj} and six bits to r_{lj}, s_{lj} . If the value of security parameter $m = 10$, then $8 \times 100 = 800$ bits will be required for the storage of matrix W .

Let entries x_{il}, y_{jk} of matrices X, Y be expressed in NSR in the form (36). Then, assigning the same 8 bit length for these entries, the storage of these requires $2 \times 8 \times 100 = 1600$ bits.

With this connection, we think we can currently formulate the following conjecture.

Conjecture 3. MPF_S^{NSR} can be considered as a candidate one-way function (OWF) for the construction of the key agreement protocol (KAP), since

- (1) the direct MPF_S^{NSR} value computation is effective;
- (2) the MPF_S^{NSR} is associative;
- (3) the MPF_S^{NSR} problem is hard (according to Conjecture 2).

5. Discussion and Conclusions

Despite the fact that the existence of one-way functions (OWFs) is not yet proved, many authors are trying to propose new so-called conjectured or candidate OWFs for cryptographic applications and showing the complexity of their inversion by associating them with other polynomially equivalent

hard problems. This paper is just one more attempt to do so by introducing a new enhanced matrix power function (MPF) based on infinite, nonsymmetric, and noncommutative algebraic systems. It can be expected that the use of such algebraic systems can increase the complexity of the inversion of the corresponding candidate OWF and, as a consequence, the security of the constructed cryptographic primitives.

The main problem in making useful MPFs based on noncommuting algebraic systems for cryptography is the loss of associativity. This paper presents a solution to this problem.

The complexity of the MPF_S^{NSR} problem implies the complexity of the inversion of the corresponding candidate OWF and the security of the cryptographic primitives. It is shown that the MPF_S^{NSR} problem is polynomially equivalent to some generalized MQ problem, which is reckoned to be hard. It is the so-called matrix MQ (MMQ) problem, which is not defined over the (finite) field, but can be interpreted as bilinear left–right action of matrices X and Y over the NSR to matrix E over a certain (introduced here) infinite, nonsymmetric, additive, and noncommuting semigroup T .

It is not yet proven that the computational MPF_S^{NSR} problem is NP-hard, since the polynomial-time reduction from any NP-hard to MPF_S^{NSR} problem is not yet found, despite significant attempts. As is known, quantum cryptanalytic algorithms can easily cope with problems which have some periodicities or symmetries. Since MPF_S^{NSR} is defined over infinite, nonsymmetric, and noncommuting algebraic structures (having no periodicities or symmetries), it seems that current quantum cryptanalytic algorithms could face a problem dealing with this kind of problem. The actual complexity class of the MPF_S^{NSR} problem is not yet known. If the proof that the MPF_S^{NSR} problem is NP-hard is found, and if a certain quantum cryptanalysis algorithm solves any problem in the NP-hard complexity class in polynomial time, then it will solve the MPF_S^{NSR} problem in polynomial time as well.

The security parameter m is defined as corresponding to the order of matrices used in the MPF definition. Since there is no theory dealing with the system of MPF equations (due to its definition over the noncommuting and nonsymmetric infinite algebraic structures), the security parameter's value is determined by heuristic analogy with the known classical MQ problem.

In this connection, the secure value for m is proposed to be $m \geq 10$. Then, in order to solve the MPF_S^{NSR} problem and to break the key agreement protocol (KAP) in Construction 1, the adversary must solve matrix Equation (52) corresponding to the system of $m^2 = 100$ equations with $2m^2 = 200$ unknown variables in NSR .

The asymptotic time for the computation of the direct MPF_S^{NSR} value is effective and is performed in $\mathcal{O}(m^3 \log^2 m)$. The computation of the direct value of many traditional candidate OWFs is based on the modular exponent function in large groups. These operations are time-consuming and usually require the use of special co-processors to speed up computations. Instead of exponentiation of large integers (512–2048 bits long) in the case of traditional candidate OWFs, we can deal with $m \times m$ matrices and perform operations with their entries of a few bits in length.

The main practical result of this paper is the construction of a KAP, definition of security parameters, and calculation of secure parameter values. The public key (PuK) for KAP construction is matrix W and the private key (PrK) is matrices X, Y (and U, V , respectively) of dimension $m \times m$. The security parameter is m and its secure value is proposed to be $m \geq 10$. Then the storage requirement for the public and private keys are 800 and 1600 bits, respectively. The latter is based on heuristic analogy with the well-known MQ problem since there is no theory yet dealing with the problems involved (i.e., noncommuting and nonsymmetric algebraic systems). Deeper consideration of the MPF complexity presented here can be performed in subsequent studies, thereby influencing the key lengths and security parameter values.

Referencing the heuristic analogy with the MQ problem, when existing methods for the MQ problem solution rarely give results better than total scan (except for in some special cases), the proposed PrK length prevents total scan attack. Since the methods of solution of MPF_S^{NSR} are unknown yet and there is not even any theory on how to handle such a kind of system of equations,

we hypothesize that the proposed key length in practice will provide sufficient security against a total attack and the attack presented in [27].

Taking in mind that the computation of the direct MPF_S^{NSR} value is effective and its inversion is polynomially equivalent to a certain type of generalized MQ problem, we are making a conjecture that MPF_S^{NSR} can be a candidate OWF.

Overall, the novelty of results presented in the paper can be summarized as follows: a new type of candidate OWF based on infinite, noncommuting, and nonsymmetric algebraic structures is presented in the class of OWFs of noncommuting cryptography. According to our knowledge so far, only a few nonsymmetric OWFs have been proposed in this class. Hence, we can expect to achieve greater security even against quantum cryptanalysis since it is more effective in cryptosystems using symmetric structures with periodicities.

6. Example of KAP Realization with Artificially Small Matrix Orders

We consider matrices of order 3×3 . The public matrix W with entries written in normal and in shortened form when $a^0 = 1, b^0 = 1$ is chosen as follows:

$$W = \begin{pmatrix} b^0 a^4 b^3 a & b^0 a b^0 a^0 & b a b^0 a^0 \\ b^0 a b a^0 & b a^3 b a & b^0 a^5 b^4 a^0 \\ b a^4 b^0 a^0 & b a b^3 a^0 & b^0 a^2 b^4 a \end{pmatrix} = \begin{pmatrix} a^4 b^3 a & a & b a \\ a b & b a^3 b a & a^5 b^4 \\ b a^4 & b a b^3 & a^2 b^4 a \end{pmatrix}.$$

According to Construction 1, we have matrices $X, U \in M_{R_1}, Y, V \in M_{R_2}$, where M_{R_1} and M_{R_2} are subsets of M_S of commuting matrices. For effective protocol realization we propose to use M_{R_1} and M_{R_2} as subsets of circulant matrices [38]. According to Equation (36), we define subsets M_{R_1} and M_{R_2} as sets of circulant matrices defined either over the set $N^0 + \iota N^0$ or the set $\iota N^0 + N^0$.

The following theorem is presented without proof.

Theorem 9. For any circulant matrix $X \in M_{R_1}$, and any circulant matrix $U \in M_{R_2}$ (or vice versa), X and U are commuting.

Referencing this theorem, Alice chooses the following matrices X and Y :

$$X = \begin{pmatrix} 2\iota + 1 & \iota + 2 & 3\iota + 3 \\ 3\iota + 3 & 2\iota + 1 & \iota + 2 \\ \iota + 2 & 3\iota + 3 & 2\iota + 1 \end{pmatrix}, Y = \begin{pmatrix} 3\iota & 2\iota & 4\iota \\ 4\iota & 3\iota & 2\iota \\ 2\iota & 4\iota & 3\iota \end{pmatrix}.$$

Bob chooses the following matrices U and V :

$$U = \begin{pmatrix} 2 + 3\iota & 1 + \iota & 2 + \iota \\ 2 + \iota & 2 + 3\iota & 1 + \iota \\ 1 + \iota & 2 + \iota & 2 + 3\iota \end{pmatrix}, V = \begin{pmatrix} 2 + 2\iota & 4 + \iota & 1 + 3\iota \\ 1 + 3\iota & 2 + 2\iota & 4 + \iota \\ 4 + \iota & 1 + 3\iota & 2 + 2\iota \end{pmatrix}.$$

Alice computes matrix A and sends it to Bob.

$$A = {}^X W^Y = \begin{pmatrix} a^3 b^3 & a^3 b^6 & a^6 b^3 \\ a^{18} b^3 & a^{19} b^2 & a^8 b^4 \\ a^3 b^{18} & a^2 b^{16} & a^4 b^{11} \end{pmatrix}$$

Bob computes matrix B and sends it to Alice.

$$B = {}^U W^V = \begin{pmatrix} a^6 b^2 a & a^8 b^4 a & a^3 b^{18} a \\ a^2 b^{34} a & a^{11} b^4 a & a^3 b^{11} a \\ a b^6 a & a^2 b^{16} a & a^2 b^4 a \end{pmatrix}$$

Alice computes the secret common key.

$$K_A = {}^X B^Y = \begin{pmatrix} a^2 b^{10} & a^4 b^{29} & a^3 b^6 \\ a^{41} b^4 & a^4 b^{47} & a^3 b^{33} \\ a^2 b^{31} & a^{70} b^2 & a^{36} b^3 \end{pmatrix}$$

Bob computes the secret common key.

$$K_B = {}^U A^V = \begin{pmatrix} a^2 b^{10} & a^4 b^{29} & a^3 b^6 \\ a^{41} b^4 & a^4 b^{47} & a^3 b^{33} \\ a^2 b^{31} & a^{70} b^2 & a^{36} b^3 \end{pmatrix}$$

Parties agree on the common secret key, since $K_A = K_B = K$.

7. Further Research

The main challenge to investigating the security of the proposed MPF is to continue attempts to prove the NP-completeness of the MPF problem. On the other side, a more consistent investigation of MPF security against possible attack scenarios is required. These objectives can be achieved by deeper theoretical investigation of MPF cryptanalytic equations, since there is no theory yet dealing with the problems involved.

Acknowledgments: The author highly appreciates Prof. Simon R. Blackburn in Department of Pure Mathematics in Mathematics Royal Holloway University of London for his attention to this work and valuable advice. The author also gives thanks to his colleagues Aleksejus Mihalkovich and Inga Timofejeva for their contribution in the professional editing of this manuscript, testing example preparation, and other aid.

Conflicts of Interest: The author declares no conflict of interest.

References

- Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **1997**, *26*, 1484–1509. [CrossRef]
- Garey, M.; Johnson, D. *Computers and Intractability: A Guide to Theory of NP-Completeness*; H. Freeman: New York, NY, USA, 1979.
- Patarin, J.; Goubin, L. Trapdoor One-Way Permutations and Multivariate Polynomials. In Proceedings of the First International Conference on Information and Communication Security, LNCS, Beijing, China, 11–14 November 1997; Volume 1334, pp. 356–368.
- Wolf, C. Hidden Field Equations. (HFE)-Variations and Attacks. Ph.D. Thesis, Ruhr-University, Bochum, Germany, 2002.
- Faugere, J.; Antoine, J. Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Grobner bases. In *Advances in Cryptology-CRYPTO*; Springer: Berlin/Heidelberg, Germany, 2003; pp. 44–60.
- Yasuda, T.; Dahan, X.; Huang, Y.-J.; Takagi, T.; Sakurai, K. MQ Challenge: Hardness Evaluation of Solving Multivariate Quadratic Problems. Available online: <http://eprint.iacr.org/2015/275.pdf> (accessed on 28 January 2018).
- Wagner, N.R.; Magyarik, M.R. A public-key cryptosystem based on the word problem. In *Advances in Cryptology*; Springer: Berlin/Heidelberg, Germany, 1985; pp. 19–36.
- Myasnikov, A.G.; Shpilrain, V.; Ushakov, A. *Non-Commutative Cryptography and Complexity of Group-Theoretic Problems*; American Mathematical Society: Providence, RI, USA, 2011.
- Kumar, G.; Hemraj, S. Novel Noncommutative Cryptography Scheme Using Extra Special Group. *Secur. Commun. Netw.* **2017**, *2017*. [CrossRef]
- Li, J.; Wang, L. Noise-Free Symmetric Fully Homomorphic Encryption Based on Noncommutative Rings. Available online: <http://eprint.iacr.org/2015/641.pdf> (accessed on 28 January 2018).
- Cheng, Q.; Zhuang, L. LWE from Non-commutative Group Rings. *arXiv*, 2016.

12. Sakalauskas, E.; Tvarijonas, P.; Raulynaitis, A. Key Agreement Protocol (KAP) Using Conjugacy and Discrete Logarithm Problems in Group Representation Level. *Informatika* **2007**, *18*, 115–124.
13. Jacobs, K. A Survey of Modern Mathematical Cryptology. Available online: http://trace.tennessee.edu/utk_chanhonoproj/1406 (accessed on 24 March 2013).
14. Sracic, M. Quantum Circuits for Matrix Multiplication. Available online: <https://www.math.ksu.edu/reu/sumar/QuantumAlgorithms.pdf> (accessed on 4 August 2014).
15. Jacobs, K.; Prenner, M. *Cryptanalysis of the Sakalauskas, Tvarijonas, and Raulynaitis Key Agreement Protocol (STR-KAP)*; Technical Report; Kansas State University: Manhattan, KS, USA, 2011; Available online: <https://www.math.ksu.edu/reu/sumar/georgespaper.pdf> (accessed on 14 January 2012).
16. Ottaviani, V.; Zaroni, A.; Regoli, M. Conjugation as public key agreement protocol on mobile cryptography. In Proceedings of the 2010 International Conference Security and Cryptography (SECRYPT), Athens, Greece, 26–28 July 2010; IEEE: Piscataway, NJ, USA, 2010; pp. 1–6.
17. Myasnikov, A.D.; Ushakov, A. Quantum algorithm for the discrete logarithm problem for matrices over finite group rings. *Groups Complex. Cryptol.* **2012**, *6*, 31–36. [[CrossRef](#)]
18. Sakalauskas, E.; Lukšys, K. Matrix Power S-Box Construction. Available online: <http://eprint.iacr.org/2007/214> (accessed on 3 November 2007).
19. Sakalauskas, E.; Luksys, K. The Matrix Power Function and its Application to Block Cipher Sbox Construction. *Int. J. Innov. Comput. Inf. Control* **2007**, *4*, 2655–2664.
20. Sakalauskas, E.; Mihalkovich, A. New Asymmetric Cipher of Non-Commuting Cryptography Class Based on Matrix Power Function. *Informatika* **2014**, *25*, 283–298. [[CrossRef](#)]
21. Sakalauskas, E.; Mihalkovich, A. Candidate One-Way Function Based on Matrix Power Function with Conjugation Constraints. In Proceedings of the Bulgarian Cryptography Days 2012, Sofia, Bulgaria, 20–21 September 2012; pp. 29–33.
22. Sakalauskas, E.; Listopadskis, N.; Tvarijonas, P. Key Agreement Protocol (KAP) Based on Matrix Power Function. In *Information Science and Computing, Book 4 Advanced Studies in Software and Knowledge Engineering*; FOI ITHEA: Sofia, Bulgaria, 2008; pp. 92–96.
23. Sakalauskas, E.; Mihalkovich, A.; Venčkauskas, A. Improved Asymmetric Cipher Based on Matrix Power Function with Provable Security. *Symmetry* **2017**, *9*, 9. [[CrossRef](#)]
24. Mihalkovich, A.; Sakalauskas, E.; Venčkauskas, A. New Asymmetric Cipher Based On Matrix Power Function and Its Implementation in Microprocessors Efficiency Investigation. *Electron. Electr. Eng.* **2013**, *19*, 119–122.
25. Luksys, K.; Sakalauskas, E.; Venčkauskas, A. Implementation analysis of matrix power cipher in embedded systems. *Electron. Electr. Eng.* **2012**, *118*, 95–98. [[CrossRef](#)]
26. Vitkus, P.; Sakalauskas, E.; Listopadskis, N.; Vitkiene, R. Microprocessor realization of key agreement protocol (KAP) based on Matrix power function. *Electron. Electr. Eng.* **2012**, *117*. [[CrossRef](#)]
27. 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: Cham, Switzerland, 2016; pp. 343–354.
28. Inassaridze, N.; Kandelaki, T.; Ladra, M. Categorical interpretations of some key agreement protocols. *arXiv*, 2011.
29. Chrislock, J.L. On medial semigroups. *J. Algebra* **1969**, *12*, 1–9. [[CrossRef](#)]
30. Krishna, K.V. Near-Semirings: Theory and Application. Ph.D. Thesis, IIT Delhi, New Delhi, India, 2005.
31. Sakalauskas, E. The Multivariate Quadratic Power Problem over Zn is NP-Complete. *Inf. Technol. Control* **2012**, *41*, 33–39. [[CrossRef](#)]
32. Vavasis, A.S. On the complexity of nonnegative matrix factorization. *SIAM J. Optim.* **2009**, *3*, 1364–1377. [[CrossRef](#)]
33. Cohen, J.E.; Rothblum, U.G. Nonnegative Ranks, Decompositions, and Factorizations of Nonnegative Matrices. *Linear Algebra Appl.* **1993**, *190*, 149–168. [[CrossRef](#)]
34. Arora, S.; Ge, R.; Kannan, R.; Moitra, A. Computing a nonnegative matrix factorization—Provably. In Proceedings of the Forty-Fourth Annual ACM Symposium on Theory of Computing, STOC '12, New York, NY, USA, 19–22 May 2012; ACM: New York, NY, USA, 2012; pp. 145–162.

35. Patarin, J. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Saragossa, Spain, 31 May–4 June 1996; Springer: Berlin/Heidelberg, Germany, 1996.
36. Shamir, A.; Kipnis, A. *Cryptanalysis of the HFE Public Key Cryptosystem*; Springer: Berlin/Heidelberg, Germany, 1999; pp. 19–30.
37. Courtois, N.; Klimov, A.; Patarin, J.; Shamir, A. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Bruges, Belgium, 14–18 May 2000; Springer: Berlin/Heidelberg, Germany, 2000.
38. Davis, P.J. *Circulant Matrices*; Wiley: New York, NY, USA, 1970.



© 2018 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).