symmetry

MDPI

Article

Sigma Identification Protocol Construction Based on MPF

Eligijus Sakalauskas [1,*], Inga Timofejeva [2] and Ausrys Kilciauskas [3]

[1] Department of Applied Mathematics, Kaunas University of Technology, K. Donelaicio Str. 73, 44249 Kaunas, Lithuania
[2] Center for Nonlinear Systems, Kaunas University of Technology, Studentu 50-147, 51368 Kaunas, Lithuania; inga.timofejeva@ktu.lt
[3] Department of Applied Informatics, Vytautas Magnus University, K. Donelaičio Str. 58, 44248 Kaunas, Lithuania; ausrys.kilciauskas@vdu.lt
* Correspondence: eligijus.sakalauskas@ktu.lt

Abstract: A new sigma identification protocol (SIP) based on matrix power function (MPF) defined over the modified medial platform semigroup and power near-semiring is proposed. It is proved that MPF SIP is resistant against direct and eavesdropping attacks. Our security proof relies on the assumption that MPF defined in the paper is a candidate for one-way function (OWF). Therefore, the corresponding MPF problem is reckoned to be a difficult one. This conjecture is based on the results demonstrated in our previous studies, where a certain kind of MPF problem was proven to be NP-complete.

Keywords: matrix power function; sigma identification protocol; security against eavesdropping attack; candidate for one-way function

Citation: Sakalauskas, E.; Timofejeva, I.; Kilciauskas, A. Sigma Identification Protocol Construction Based on MPF. *Symmetry* **2021**, *13*, 1683. https://doi.org/10.3390/sym13091683

Academic Editors: Ming-Chin Chuang and Jeng-Shyang Pan

Received: 21 July 2021
Accepted: 9 September 2021
Published: 13 September 2021

1. Introduction

In this paper a new paradigm for the so-called Sigma Identification Protocol (SIP) based on the authors' earlier proposed new candidate for one-way function (OWF) is presented. In general, Sigma protocols are three-round protocols similar to the well-known Schnorr identification protocol. They are typically used as sub-protocols in more complicated settings and for more advanced use. For example, Sigma protocols can easily be transformed into corresponding identification and signature schemes. Another application is to design protocols that allow one party to prove to another that certain facts are true (without revealing private information). For example, to prove that encrypted value V lies in a certain range without revealing any other information about V. Sigma protocols can be combined to make new Sigma protocols. For example, in the AND-proof construction, a Prover can convince a Verifier that he knows witnesses for a pair of statements. In the OR-proof construction, a Prover can convince a Verifier that he knows witnesses for one of two statements. These examples convince us that the development of Sigma protocols based on new paradigms is promising.

The construction of cryptographic primitives based on matrix power function (MPF) belongs to the field of so called non-commuting cryptography [1], [2]. The development of non-commuting cryptography is important due to the need to replace traditional cryptographic methods vulnerable to quantum cryptanalysis. Peter W. Shor has proposed the polynomial-time quantum cryptanalysis [3] for the traditional cryptographic primitives such as Diffie—Hellman key exchange protocol, RSA and ElGamal cryptosystems, Digital signature algorithm (DSA) and Elliptic Curve DSA (ECDSA).

One of the promising trends is the creation of OWFs, the security of which relies on the NP-hard problems [4]. Thus far, there are no known effective quantum cryptanalytic algorithms solving NP-hard problems; therefore, this cryptographic trend is a significant part of the so-called post-quantum cryptography [5]. One of the trends to create cryptographic primitives that can resist quantum cryptanalysis attacks is lattice-based cryptography [6]

and hidden field equations (HFE) based cryptosystems [7–10]. Despite some cryptanalytic attacks on the HFE cryptosystem [8,9], this trend is viewed as promising [10].

MPF is somewhat related to the multivariate polynomials used in HFE cryptosystems since the complexity of so called MPF problem and the NP-completeness of this problem is proved using polynomial-time reduction of multivariate quadratic (MQ) problem [7]. Referencing [11] it is proved that certain kinds of MPF problems are NP-complete as well [12,13].

In this paper the novel MPF based sigma identification protocol (SIP) is presented using several specifically selected algebraic structures introduced in [14]. The concept of abstract MPF as well as main definitions for the construction of SIP are given in Section 2. The algebraic structures for the construction of MPF are defined in Section 3. MPF SIP is presented in Section 4. The security of MPF SIP against eavesdropping attacks is proven in Section 5. In Section 6, the selection of security parameters as well as the efficiency analysis are presented. The discussions and conclusions are presented in Section 7. The table of notations used in this paper as well as the numerical example are displayed in the Abbreviations and Appendix A, respectively.

2. The Construction of the Abstract Matrix Power Function

In this section, the matrix power function (MPF) is constructed in an abstract form without specifying exact algebraic structures that will be introduced in subsequent sections. Let $X = \{x_{il}\}$, $W = \{w_{lj}\}$ and $Y = \{y_{jk}\}$ be $m \times m$ matrices over some semiring, and indices $i, j, k, l \in I_m = \{1, 2, \ldots, m\}$. Multiplying matrix W by matrix X from the left and by matrix Y from the right yields a new matrix $Q = \{q_{ik}\}$.

$$XWY = Q; \sum_{j=1}^{m} \sum_{l=1}^{m} x_{il} w_{lj} y_{jk} = q_{ik}; i, j, k, l \in I_m. \tag{1}$$

Let $\boldsymbol{S}$ be some multiplicative semigroup and $\boldsymbol{R}$ some numerical semiring. In the case that MPF $\boldsymbol{S}$ is named a platform semigroup and $\boldsymbol{R}$ an exponent semiring. The exponent semiring of natural numbers with zero is denoted by $\boldsymbol{N}_0 = \{0, 1, 2, \ldots\}$. The corresponding semigroup of matrices defined over $\boldsymbol{S}$ is denoted by $\boldsymbol{M_S}$ and the semiring of power matrices defined over $\boldsymbol{R}$ is denoted by $\boldsymbol{M_R}$. Then, using an analogy with the matrix multiplication defined in (1), the left MPF, the right MPF and the left-right or simply MPF are introduced for $X, Y \in \boldsymbol{M_R}$, $x_{il}, y_{jk} \in \boldsymbol{R}$ and for $W \in \boldsymbol{M_S}$, $w_{lj} \in \boldsymbol{S}$ as follows.

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

$$^{X}W = C \quad c_{ij} = \prod_{l=1}^{m} w_{lj}^{x_{il}}. \tag{2}$$

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

$$W^{Y} = D \quad d_{lk} = \prod_{j=1}^{m} w_{lj}^{y_{jk}}. \tag{3}$$

Definition 3. *The left-right, or simply MPF corresponds to the matrix W powered by matrix X from the left and by matrix Y from the right with the MPF value equal to the matrix $Q = \{q_{ik}\}$ and is expressed in the following way:*

$$^{X}W^{Y} = A, \quad a_{ik} = \prod_{j=1}^{m} \prod_{l=1}^{m} w_{lj}^{x_{il} \cdot y_{jk}}; i, j, k, l \in I^{(m)}. \tag{4}$$

The MPF definition is related to the following associativity identities.

Definition 4. *MPF is one-side, (left-side or right-side) associative and two-side associative if the following respective identities hold:*

$$^{Y}(^{X}W) = {}^{(YX)}W = {}^{YX}W;\ (W^{X})^{Y} = W^{(XY)} = W^{XY}. \tag{5}$$

$$(^{X}W)^{Y} = {}^{X}(W^{Y}) = {}^{X}W^{Y}. \tag{6}$$

In general, MPF is a function F: $\boldsymbol{M_R} \times \boldsymbol{M_S} \times \boldsymbol{M_R} \to \boldsymbol{M_S}$. To be concise, we will use the notation MPF_S^R for the definition of MPF with base matrix defined over the platform semigroup $\boldsymbol{S}$ in $\boldsymbol{M_S}$ and with power matrices defined over the exponent semiring $\boldsymbol{R}$ in $\boldsymbol{M_R}$. The categorical interpretation of MPF is presented in [15], in the context of the construction of several key agreement protocols. We slightly reformulate the notions used in the authors' interpretation by the following proposition, which is more appropriate for our study.

Proposition 1. *If MPF is associative, then $\boldsymbol{M_S}$ is a multiplicative $\boldsymbol{M_R}$-semibimodule.*

This means that there exist bilinear (left and right) actions of the matrix semiring $\boldsymbol{M_R}$ on the matrix semigroup $\boldsymbol{M_S}$. According to the definition of action, it must satisfy the associative law corresponding to Definition 4. Since matrix semigroup $\boldsymbol{M_S}$ is multiplicative, then $\boldsymbol{M_R}$-semibimodule $\boldsymbol{M_S}$ is multiplicative in our case. The following lemma is presented without proof. The proof can be found in [14].

Lemma 1. *If $\boldsymbol{R}$ is a commutative numerical semiring (e.g., $\mathbf{N}_0 = \{0, 1, 2, \ldots\}$) and $\boldsymbol{S}$ is a commutative semigroup, then MPF is two-side associative.*

The direct MPF value computation requires finding matrix A in (4), when matrices X, Y and W are given. The inverse MPF value computation requires finding matrices X and Y in (4), when matrices W and A are given. The MPF problem is the computation of the inverse MPF value.

Definition 5. *A function F: $\boldsymbol{Dom} \to \boldsymbol{Ran}$ with finite sets of domain ($\boldsymbol{Dom}$) and range ($\boldsymbol{Ran}$) is a candidate for **one-way function** (OWF) if for all $d \in \boldsymbol{Dom}$ the $F(d)$ can be computed by a polynomial time algorithm, but any polynomial time randomized algorithm that attempts to compute an inverse value $F^{-1}(r) = d$ for F, where $r \in \boldsymbol{Ran}$ is given, succeeds with negligible probability. That is, for all randomized algorithms, all positive integers c and all sufficiently large $n = length(d)$, the probability to compute an inverse value r for F is at most n^{-c}. The probability is taken over the choice of r from the discrete uniform distribution in $\boldsymbol{Ran}$.*

Paraphrasing this definition in a non-formal way, MPF is candidate for OWF if: (1) the MPF direct value computation is easy, and (2) the MPF problem is hard.

The computation of the direct MPF value is effective and can be done by powering elements of the platform semigroup $\boldsymbol{S}$ by elements of the exponent semiring $\boldsymbol{R}$ with relatively small values (e.g., up to 5 used in this study). It is related to the matrix multiplication by the two matrices from the left and right. In this paper we present some evidence that the solution of the MPF problem is hard.

Proposition 2. *The necessary requirements for MPF for the proposed SIP are the following: (1) it is a candidate for OWF, (2) it is associative, and (3) the following distributive identity holds:*

$$^{(U+X)}W^{(+Y)} = {}^{U}W^{V} * {}^{U}W^{Y} * {}^{X}W^{V} * {}^{X}W^{Y}, \tag{7}$$

*where * is a Hadamard product of matrices [16].*

3. The Definition of Algebraic Structures

In order to construct a platform semigroup for MPF, the class of modified multiplicative medial semigroups [17] is used. A medial semigroup S_M has the presentation consisting of two generators a, b and relation R_M is defined in the following way:

$$\boldsymbol{S_M} = <a, b \mid R_M>, \tag{8}$$

$$R_M: w_1abw_2 = w_1baw_2, \tag{9}$$

where w_1 and w_2 are arbitrary non-empty words in $\boldsymbol{S_M}$, 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 $w_1, w_2 \in \boldsymbol{S_M}$ and any exponent $e \in \boldsymbol{N_0}$, where $\boldsymbol{N_0} = \{0, 1, 2, \dots\}$ is the semiring of natural numbers with zero:

$$(w_1w_2)^e = {w_1}^e{w_2}^e. \tag{10}$$

In order to construct a platform semigroup $\boldsymbol{S}$ for MPF in (4), two extra relations R_1 and R_2 are added to $\boldsymbol{S_M}$:

$$R_1: a^5 = a; R_2: b^5 = b. \tag{11}$$

These relations can be generalized for arbitrary finite exponents instead of 5, however, only relations (11) are considered in this paper for simplicity. Thus, modified medial semigroup $\boldsymbol{S}$ has the following presentation:

$$\boldsymbol{S_M} = <a, b \mid R_M, R_1, R_2>. \tag{12}$$

Note that we define S as a multiplicative, non-commuting and cancellative semigroup.

Proposition 3. *Semigroups $\boldsymbol{S_M}$ and $\boldsymbol{S}$ are transformed into monoids by introducing an empty word as a multiplicatively neutral element, denoted by 1. Then, conveniently, the following identities hold for all w in $\boldsymbol{S_M}$ and $\boldsymbol{S}$:*

$$w1 = 1w = w, w^0 = 1; 0 \in \boldsymbol{N_0}. \tag{13}$$

Using relation R_M in (9) any word in $\boldsymbol{S_M}$ can be transformed to the form $w = b^s a^t b^u a^v$ moving generators a, b left and right, where $s, t, u, v \in \boldsymbol{N_0}$. Let $w = b^s a^t b^u a^v$ be such word in $\boldsymbol{S_M}$. Reformulating the Theorem 12 in [14], the normal form w_{nf} of word w in the semigroup $\boldsymbol{S_M}$ is defined by the following function nf: $\boldsymbol{S_M} \rightarrow \boldsymbol{S_{M,nf}}$ and is expressed by the relation:

$$w_{nf} = \max_{t,u}(b^s a^t b^u a^v) = b^\beta a^{i_a} b^{i_b} a^\alpha = nf(w); \alpha, \beta \in \{0, 1\}; i_a, i_b \in N_0. \tag{14}$$

The normal form in the modified medial semigroup $\boldsymbol{S}$ is defined by the following theorem.

Theorem 1. *The normal form w_η of the word w_{nf} in the normal form of $\boldsymbol{S_M}$, is represented by the function η: $\boldsymbol{S_M} \rightarrow \boldsymbol{S}$ and obtained by applying the minimization procedure of exponents i_a, i_b in (14) using the relations R_1, R_2:*

$$w_\eta = \min_{i_a, j_b} w_{nf}(\beta, i_a, j_b, \alpha) = \min_{i_a, j_b}(b^\beta a^{i_a} b^{j_b} a^\alpha) = b^\beta a^i b^j a^\alpha = \eta(w_{nf}); \alpha, \beta \in \{0, 1\}; i_a, i_b \in N_0. \tag{15}$$

Since $\boldsymbol{S}$ is a multiplicative semiring, the following exponent identities hold for any generator $g \in \{a, b\}$:

$$g^i g^j = g^{i+j}; (g^i)^j = g^{ij}. \tag{16}$$

Addition and multiplication tables for exponents i, j are presented in Tables 1 and 2 below.

Table 1. Addition (+) table for exponents *i*, *j*.

+	**0**	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	1	2	3	4	1
2	2	3	4	1	2
3	3	4	1	2	3
4	4	1	2	3	4

Table 2. Multiplication (•) table for exponents *i*, *j*.

•	**0**	**1**	**2**	**3**	**4**
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	2	4
3	0	3	2	1	4
4	0	4	4	4	4

Referencing relations R_1, R_2 the semiring $\boldsymbol{N}_0$ can be replaced by the finite semiring $\boldsymbol{N}_4 = \{0, 1, 2, 3, 4\}$. This semiring has an additive semigroup with index 1 and period 4. The exponent functions defined on $\boldsymbol{S}$ are determined by non-negative exponents in semiring $\boldsymbol{N}_4$.

We generalize these functions by introducing the "imaginary" unit ι which has some weak analogy with complex numbers in classical numerical algebra based on the imaginary unit i ($i^2 = -1$). According to this "analogy" the set of complex exponents can be introduced and denoted by $\iota{\cdot}\boldsymbol{N}_4$, where "·" denotes a formal multiplication of ι by any number in $\boldsymbol{N}_4$. According to our assumption and using the relation R_M in (9), the following properties of exponent ι are defined:

$$\iota^2 = 1, 1 \in \boldsymbol{N_4}; a^{\iota} = b; b^{\iota} = a; t + \iota{\cdot}u \neq \iota{\cdot}u + t, \tag{17}$$

where $t, u \in \boldsymbol{N}_4$. This means that elements $t + \iota{\cdot}u$ and $\iota{\cdot}u + t$ do not commute.

The algebraic structure termed a near-semiring [18] was introduced for the construction of MPF in [14]. In general, it can be defined in the following way.

Definition 6. *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, and <**NSR**; ·; 1> is a multiplicative monoid with neutral element 1, satisfying the following (two-sided) axioms for all x, y, z in **NSR**:*

$$x{\cdot}(y + z) = x{\cdot}y + x{\cdot}z, \text{ and } \quad (x + y){\cdot}z = x{\cdot}z + y{\cdot}z, \tag{18}$$

$$0 + x = x + 0 = x; 0{\cdot}x = x{\cdot}0 = 0; 1{\cdot}x = x{\cdot}1 = x. \tag{19}$$

Referencing to this definition the special type ***NSR*** required for MPF SIP construction is defined in the following way.

Definition 7. *The exponent near-semiring **NSR** consist of non-commuting additive monoid <**NSR**; +; 0> and commuting multiplicative monoid <**NSR**; ·; 1> satisfying Definition 6 and is a union of the following sets*

$$\boldsymbol{NSR} = \boldsymbol{N_4} + \iota{\cdot}\boldsymbol{N_4} + \boldsymbol{N_4} \cup \iota{\cdot}\boldsymbol{N_4} + \boldsymbol{N_4} + \iota{\cdot}\boldsymbol{N_4}, \tag{20}$$

where the set $\boldsymbol{N_4} + \iota{\cdot}\boldsymbol{N_4} + \boldsymbol{N_4}$ defines the class of elements $\{t + \iota{\cdot}u + v\}$ and the set $\iota{\cdot}\boldsymbol{N_4} + \boldsymbol{N_4} + \iota{\cdot}\boldsymbol{N_4}$—the class $\{t{\cdot}\iota + u + v{\cdot}\iota\}$, where $t, u, v \in \boldsymbol{N_4}$.

The presentation of the semigroup $\boldsymbol{S}$ by relations R_M, R_1, R_2 in (9) and (11) induces certain properties and relations in ***NSR*** that can be directly verified and are presented below without the proof.

Proposition 4. *For any $x, y \in \boldsymbol{NSR}$, where $x = t + \iota \cdot u + v$ and $y = \iota \cdot t + u + \iota \cdot v$ and $t, u, v \in \boldsymbol{N_4}$, the following identities hold for the exponents of generators a and b in* $\boldsymbol{S}$*:*

$$a^x = a^{t+\iota \cdot u+v} = a^t a^{\iota \cdot u} a^v = a^t b^u a^v; a^y = a^{\iota \cdot t+u+\iota \cdot v} = a^{\iota \cdot t} a^u \; a^{\iota \cdot v} = b^t a^u b^v. \tag{21}$$

Identity to (21) can be extended for any word $w \in \boldsymbol{S}$:

$$w^x = w^{t+\iota \cdot u+v} = w^t \overline{w}^u w^v; w^y = w^{\iota \cdot t+u+\iota \cdot v} = \overline{w}^t w^u \overline{w}^v, \tag{22}$$

where the word $\overline{w}$ is obtained from w by renaming the generator a to b and b to a respectively. It is easily verified that the exponent function in $\boldsymbol{S}$ satisfies the following more general identities for any $w, w_1, w_2 \in \boldsymbol{S}$ and any $x, y \in \boldsymbol{NSR}$:

$$w^x w^y = w^{(x+y)} = w^{x+y}; \qquad (w^x)^y = w^{(x \cdot y)} = w^{x \cdot y}, (w_1 w_2)^x = (w_1)^x (w_2)^x. \tag{23}$$

The partial case of (23) are the following identities: $a^x \; a^y = a^{x+y}$, $(a^x)^y = a^{(x \cdot y)} = a^{x \cdot y}$ and $(a_1 a_2)^x = (a_1)^x (a_2)^x$ for any $a, a_1, a_2 \in \boldsymbol{S}$ and $x, y \in \boldsymbol{NSR}$. The same is valid for the generator b. The illustration of the computation of exponents in $\boldsymbol{S}$ is presented in Example 1 below.

The set of matrices defined over the $\boldsymbol{NSR}$ is denoted by $\boldsymbol{M_{NSR}}$.

Referencing to the Proposition 1, we present the following easily verifiable theorem without a proof.

Theorem 2. $\boldsymbol{M_S}$ *is a multiplicative* $\boldsymbol{M_{NSR}}$*-semibimodule.*

Since $\boldsymbol{NSR}$ is acting on the semigroup $\boldsymbol{S}$ as an exponent function, then $\boldsymbol{M_{NSR}}$ is acting on $\boldsymbol{M_S}$ as MPF. According to Definition 7 and semigroup $\boldsymbol{S}$ presentation in (12) the following proposition can be formulated.

Proposition 5. $\boldsymbol{NSR}$ *introduced in the Definitions 6 and 7 has non-commuting additive monoid <***NSR***; +; 0> and commuting multiplicative monoid <***NSR***; ·; 1>, i.e., for all* $x, y, z_1, z_2 \in \boldsymbol{NSR}$ *the following identities hold:*

$$z_1 + x + y + z_2 = z_1 + y + x + z_2. \tag{24}$$

$$x \cdot y = y \cdot x. \tag{25}$$

Relation (25) implies the following identity:

$$\iota \cdot x = x \cdot \iota. \tag{26}$$

Example 1. *The computation of w^x. Let $w = b^3aba^2$ and $x = 2 + \iota \cdot 3 + 4$, then the 1-st step of the computation is performed in the following way.*

$$w^x = w^{2+\iota \cdot 3 \cdot + 4} = (b^3aba^2)^{2+\iota \cdot 3+4} = (b^3aba^2)^2 \; (b^3aba^2)^{\iota \cdot 3} \; (b^3aba^2)^4 = (b^6a^2b^2a^4) \; (a^9b^3a^3b^6) \; (b^{12}a^4b^4a^{48})$$

At the second step transformation to the normal form (15), every word in parentheses is performed.

$$(b^6a^2b^2a^4) \; (a^9b^3a^3b^6) \; (b^{12}a^4b^4a^{48}) = (b^7aba^5) \; (a^{12}b^9) \; (b^{15}aba^{11}) = (b^3aba) \; (a^4b) \; (b^3aba^3) = = ba^9b^8a = bab^4a.$$

The final word is found using R_1 and R_2 as well, where $b^8 = b^4$, $a^9 = a$.

The gray part of Table 1 represents the additive subgroup $\boldsymbol{N_4}^+ = \{1, 2, 3, 4\}$ with neutral element equal to 4. Subgroup $\boldsymbol{N_4}^+$ has the subset of two generators $\boldsymbol{\Gamma} = \{1, 3\}$. The subgroup $\boldsymbol{N_4}^+$ and generators $\boldsymbol{\Gamma}$ will play an important role in proving the uniform distribution of conversations and the security against eavesdropping attack of MPF SIP in Section 5. Moreover, relations R_1, R_2 in (11) define the smallest exponent $e = 5$ where subgroup $\boldsymbol{N_4}^+$ has at least two generators. It is important to have a random choice in the set having at

least two generators and will be used in our construction as well. The gray part of Table 2 represents the multiplicative semigroup $\boldsymbol{N_4}^+$ in $\boldsymbol{N_4}$. It is easily verified that $\boldsymbol{N_4}^+$ is a sub-semiring of $\boldsymbol{N_4}$. Replacing $\boldsymbol{N_4}$ by $\boldsymbol{N_4}^+$ in Definition 7, we obtain a new near-semiring as a sub-semiring of ***NSR*** which is denoted by ***sNSR***. The matrix set over the ***sNSR*** is denoted by $\boldsymbol{M_{aNSR}}$ and matrix set with entries in $\boldsymbol{\Gamma} = \{1, 3\}$ is denoted by $\boldsymbol{M_\Gamma}$. MPFs defined by the multiplicative $\boldsymbol{M_{sNSR}}$-semibimodule $\boldsymbol{M_S}$ and by the multiplicative $\boldsymbol{M_{sNSR}}$-semibimodule $\boldsymbol{M_S}$ are denoted by MPF_S^{NSR} and MPF_S^{sNSR} respectively.

Together with the introduced here near-semirings the introduction of anti-***NSR***, denoted by ***aNSR***, to the original ***NSR*** is necessary. According to (20), ***aNSR*** is defined by:

$$\boldsymbol{aNSR} = -\boldsymbol{N_4} - \iota\cdot\boldsymbol{N_4} - \boldsymbol{N_4} \cup - \iota\cdot\boldsymbol{N_4} - \boldsymbol{N_4} - \iota\cdot\boldsymbol{N_4}, \tag{27}$$

where for any element x in ***NSR*** there exists a unique element x' in ***aNSR*** obtained by switching the sign of x from positive to negative, i.e., $x' = -x$. The matrix set over the ***aNSR*** is denoted by $\boldsymbol{M_{aNSR}}$. For any matrix H in $\boldsymbol{M_{NSR}}$ there exists a unique matrix $-H$ in $\boldsymbol{M_{aNSR}}$ with negative entries. Then, formally, we assume that

$$H - H = O, \tag{28}$$

where O is the zero matrix, i.e., matrix with all entries equal to zero.

This construction will be used in the security proofs for the so-called simulator Sim computations. Several additional properties of MPF_S^{aNSR} are presented below without the proof. Let O be a zero matrix in $\boldsymbol{M_{NSR}}$ and E is a unity matrix in $\boldsymbol{M_S}$ consisting of all entries equal to 1 in $\boldsymbol{S}$. Then according to (7), (27) and (28), for any $W, A \in \boldsymbol{M_S}$ and $U, H \in \boldsymbol{M_{NSR}}$ the following identities hold:

$$A^O = E; {}^OA = E; W * E = E * W = W; \tag{29}$$

$${}^UA^H * {}^UA^{-H} = {}^U(A^{H-H}) = {}^UA^O = {}^UE = E. \tag{30}$$

The last identity remains valid if the presented actions are reversed from the left to the right.

4. MPF Sigma Identification Protocol (SIP)

In general, sigma identification protocols (SIP) are realized using the conversation between the Prover and the Verifier when the Prover proves to the Verifier the knowledge of the secret (e.g., his private key—witness) without revealing knowledge about this secret [19]. In this case it is said that SIP has the Zero Knowledge Proof (ZKP) property [19]. Prover is using his private, public key pair we denote by PrK, PuK named as a witness-statement pair.

We denote any matrix Q that is generated uniformly at random from the matrix set $\boldsymbol{M}$ by $Q \leftarrow \text{rand}(\boldsymbol{M})$.

We use matrix sets $\boldsymbol{M_{sNSR}}$ and $\boldsymbol{M_\Gamma}$ introduced in Section 3 instead of the matrix set $\boldsymbol{M_{NSR}}$ to provide a random uniform distribution of data generated in MPF SIP.

Parties share the same public parameter represented by matrix W in $\boldsymbol{M_S}$ generated at random $W \leftarrow \text{rand}(\boldsymbol{M_S})$. The prover runs the following key pair generation algorithm. For the private key PrK-witness generation two secret matrices X, Y in $\boldsymbol{M_\Gamma} = \{1, 3\}$ are chosen at random:

$$X,Y \leftarrow \text{rand}(\boldsymbol{M_\Gamma}). \tag{31}$$

Then PrK = $(X, Y) \in \boldsymbol{M_\Gamma} \times \boldsymbol{M_\Gamma}$.

The public key PuK-statement is computed using MPF_S^{sNSR} defined above:

$$\text{PuK} = {}^XW^Y = A. \tag{32}$$

Prover distributes his PuK = $A \in \boldsymbol{M_S}$ to all users including Verifier. According to the 3-rd condition in the Proposition 2 represented by the distributive identity (7), we formulate the following easily verified theorem without proof.

Theorem 3. *MPF_S^{sNSR} satisfies the distributive identity (7).*

Definition 8. *Equation (32) defines a set of relations **Rel** between the set of witnesses (PrK) and statements (PuK) which is a subset of the following direct product of sets:* $\mathbf{Rel} \subseteq (\mathbf{M_\Gamma} \times \mathbf{M_\Gamma}) \times \mathbf{M_S}$.

Since relations R_1, R_2 in (11) define a finite semiring $\boldsymbol{S}$, they induce the finiteness of *s**NSR***. Then, sets $\boldsymbol{M_{sNSR}}$ and $\boldsymbol{M_S}$ are finite as well.

Definition 9. *Let matrix $A = \{a_{ij}\}$ be of finite order and assume that all entries q_{ij} can be effectively encoded by the finite string of bits not exceeding polynomial length. Then, matrix A is effectively recognizable in $\boldsymbol{M_S}$ if all its entries can be effectively decoded and effectively transformed to the normal form (15).*

Proposition 6. *Any finite length word w in $\boldsymbol{S}$ can be transformed to the normal form (15) using the linear number of operations with respect to the length of w.*

Definition 10. *Relation **Rel** is efficiently recognizable if every matrix $A' = \{a_{ij}'\}$, where $a_{ij}'$are finite strings of generators a, b in $\boldsymbol{M_S}$, can be effectively transformed into the matrix A in $\boldsymbol{M_S}$ with all entries expressed in the normal form (15).*

Definition 11. *Relation is an effective relation if it is efficiently recognizable.*

Proposition 7. *Relation **Rel** is effective.*

Referencing to the general definition of Sigma protocol in [19], the corresponding definition can be formulated for MPF SIP.

Definition 12. *Let $\boldsymbol{Rel} \subseteq (\boldsymbol{M_\Gamma} \times \boldsymbol{M_\Gamma}) \times \boldsymbol{M_S}$ be an effective relation. An MPF SIP for **Rel** is a pair (P, V) of interactive protocols executed by the Prover and the Verifier. Protocol P is taking a witness-statement pair (PrK, PuK) $\in$ **Rel** as an input. Protocol V is taking as an input statement PuK $\in \boldsymbol{M_S}$. Then after the conversation V outputs **accept** or **reject**.*

MPF SIP is performed during three pass communications named as a conversation between the Prover and the Verifier.

1. Prover generates two matrices $U, V \leftarrow \mathrm{rand}(\boldsymbol{M_\Gamma})$ at random and using his witness-PrK computes the **commitment** $C = (C_0, C_1, C_2)$ consisting of three matrices C_0, C_1, C_2 in $\boldsymbol{M_S}$:
$$C_0 = {}^{U}W^{V}, C_1 = {}^{U}W^{Y}, C_2 = {}^{X}W^{V}. \quad (33)$$
Prover sends C to the Verifier.
2. After receiving C, Verifier generates two matrices $H', H'' \leftarrow \mathrm{rand}(\boldsymbol{M_{sNSR}})$ at random and independently, forms **challenge** $H = (H', H'')$ and sends H to the Prover.
3. Upon receiving H, Prover computes the **response** $R = (S, T)$ consisting of two matrices S, T in $\boldsymbol{M_{sNSR}}$:
$$S = U + H'X, T = V + YH'', \quad (34)$$
and sends $R = (S, T)$ to the Verifier.

At this stage Prover and Verifier complete the conversation. After receiving $R = (S, T)$, Verifier checks if
$$^{S}W^{T} = C_0 * {C_1}^{H''} * {}^{H'}C_2 * {}^{H'}A^{H''}, \quad (35)$$
and if it is the case outputs ***accept***.

The distinct feature of the proposed protocol (against, e.g., Schnorr or Okamoto protocols, [19]) is that the Prover generates a commitment at the first step of the protocol using components X, Y of the witness-PrK = (X, Y).

Completeness. On the common statement input PuK = A, the honest Prover knows witness-PrK = (X, Y) for PuK and succeeds in convincing the Verifier of his knowledge with probability 1. It follows from the validity of associativity identity (6) and distribution identity (7):

$$^{S}W^{T} = {}^{(U+H'X)}W^{(V+YH'')} = {}^{U}W^{V} * {}^{U}W^{YH''} * {}^{H'X}W^{V} * {}^{HX'}W^{YH'} = {}^{U}W^{V} * ({}^{U}W^{Y})^{H''} * {}^{H'}({}^{X}W^{V}) * {}^{H'}({}^{X}W^{Y})^{H'} = C_0 * {C_1}^{H''} * {}^{H'}C_2 * {}^{H'}A^{H''}.$$

Verifier uses the conversation (C, H, R) together with the Prover's statement PuK = A for the verification and yields accept if (35) holds.

The test example of this protocol is presented in Appendix A.

5. Security Analysis

We consider the main three main kind of attacks for SIP presented in [19] ordered by their power, i.e., direct attack, eavesdropping attack and active attack. The weakest attack of the three is a direct attack and it is applied mainly for password protected systems which can also be realized using symmetric cryptography. The outcome of these attacks is either adversary impersonation of legal Prover or even compromisation of legal prover's secret, namely his password or private key PrK-witnwss. The detailed description of the attack game and the theorem formulating security against this attack is presented in ([19], Section 18.3). Since this attack is not of direct interest for our research, we only use the security formulation for this attack in our construction in Theorem 4 below as an intermediate result to consider the more powerful eavesdropping attack. In this section we prove the conditions under which the proposed MPF SIP is resistant against eavesdropping attack finalizing it in Theorems 5 and 6. Unfortunately, we were not able to prove the resistance against most powerful active attack for the reasons presented below.

Assumption 1. *MPF_S^{NSR} is a candidate for one-way function (OWF).*

This assumption can be supported by our previous results presented in [11–14]. The MPF is constructed using similar algebraic structures as in [14]. In [12,13] the NP-completeness of the similar MPF problem is proven. MPF function introduced there is defined in finite modified medial platform semigroup and finite power near-semiring. Despite the lack of proof of the NP-completeness of the MPF problem defined here, we can present some links of this MPF with the well-known multivariate quadratic (MQ) problem which is proved to be NP-complete over any field [7]. Let φ: $\boldsymbol{S} \to \boldsymbol{S_a}$ is the homomorphism of the semigroup $\boldsymbol{S}$ to the semigroup $\boldsymbol{S_a}$ defined by the introduced new relation $b = 1$. Then $\boldsymbol{S_a} = \{1, a, a^2, a^2, a^4\}$ is a cyclic monoid with index 1 and period 4 [20]. The corresponding public matrix denoted by W'. Then the entries of this public matrix W' consist of elements a^i, where $I \in \{0, 1, 2, 3, 4\}$ due to relation R_1. Analogously, the ***NSR*** can be homomorphically transformed to the set of integers $\boldsymbol{Z}_5 = \{0, 1, 2, 3, 4\}$ by introducing the relation $\iota = 0$. Then the matrices X', $Y' \leftarrow \text{rand}(\boldsymbol{Z_5})$ are generated.

Since $\boldsymbol{S_a}$ is a cyclic semigroup then the discrete logarithm operation dlog_a with the base a can be applied elementwise to the MPF relation ${}^{X'}(W')^{Y'} = A'$. In this case we obtain MQ problem but defined not over the field $\boldsymbol{F}_5 = \{0, 1, 2, 3, 4\}$ (where operations are defined mod 5) since according to relation R_1 in (11) the exponents of generator a cannot be reduced mod 5. It seems that the obtained MQ problem represented by matrix equation

$$\text{dlog}_a({}^{X'}(W')^{Y'}) = \text{dlog}_a(A'),$$

is at least no less complex than the "standard" MQ problem. Then, we can make an assumption that MPF introduced in (4), (32), where unknown monomials are in exponents is a candidate for one-way function (OWF).

This assumption is required to prove that the proposed MPF SIP is secure against the eavesdropping attack and to select the values of the security parameters.

Referencing to Assumption 1 and [19], we can formulate the following theorem.

Theorem 4. *If MPF_S^{NSR} is a candidate for OWF and the challenge space is super-poly, then MPF SIP identification protocol is secure against the direct attack.*

Proof. According to the Assumption 1, MPF_S^{NSR} is a candidate for OWF.

Referencing to the relations R_1, R_2 in (11), the challenge space is exponential with respect to the order m of matrices in $\boldsymbol{M_{NSR}}$. The cardinality of $\boldsymbol{M_{NSR}}$ is no less than 5^{2mm}, thus, it is super poly as well. □

It is easily verified that Assumption 1 and Theorem 4 can be applied to MPF_S^{sNSR}.

In order to formulate the security against the eavesdropping attack, we need the definition and the proof of the Honest Verifier Zero Knowledge (HVZK) property [19] for MPF SIP. We realized that instead of HVZK of MPF SIP we can prove a rather stronger result denoted as a special HVZK.

Definition 13. *Identification protocol is a special HVZK if there exists an efficient probabilistic algorithm called a simulator Sim such that for all possible witness-statement pairs or private and public key pairs (PrK, PuK) the following two conditions hold: 1) the output distribution of Sim on input (PuK, H) is identical to the distribution of transcript of a conversation (C, H, R) between Prover on input (PrK, PuK) and Verifier on input Puk, and 2) for all inputs PuK and H, algorithm Sim always outputs a pair (C, R) such that (C, H, R) is an accepting conversation for PuK.*

Following the methodology presented in [19], the following theorem can be formulated.

Theorem 5. *MPF SIP protocol is a special HVZK.*

Proof. On Sim input R', H' and PuK, the valid commitment $C' = (C_{0'}, C_{1'}, C_{2'})$ and corresponding transcript of a conversation (C', H', R') must be generated with identical distribution as (C, H, R) between the Prover and the Verifier. □

Lemma 2. *Let W be a public parameter and two pairs of matrices $X,Y \leftarrow rand(\boldsymbol{M_\Gamma})$, $X',Y' \leftarrow rand(\boldsymbol{M_\Gamma})$ are generated uniformly at random, then the entries of matrices $A = {}^{X}W^{Y}$ and $A' = {}^{X'}W^{Y'}$ computed according to (32) are uniformly distributed.*

Proof of Lemma. Define two subsemigroups in $\boldsymbol{S}$, namely $\boldsymbol{S_a} = \{a, a^2, a^3, a^4\}$, $\boldsymbol{S_b} = \{b, b^2, b^3, b^4\}$ and a set of exponents of generators in $\boldsymbol{S}$ denoted earlier by $\boldsymbol{N_4}^+ = \{1, 2, 3, 4\}$. Then exponent function of generator a in $\boldsymbol{S_a}$ provides the following 1-to-1 mapping $\exp_a$: $\boldsymbol{N_4}^+ \rightarrow \boldsymbol{S_a}$. Since $\exp_a$ is 1-to-1, then for any $I \leftarrow \text{rand}(\boldsymbol{N_4}^+)$ the value $\exp_a(i) = a^i$ will have a uniform random distribution. The same is valid for the function $\exp_b$: $\boldsymbol{N_4}^+ \rightarrow \boldsymbol{S_b}$. Let $\exp_{a,a}$: $\boldsymbol{N_4}^+ \times \boldsymbol{N_4}^+ \rightarrow \boldsymbol{S_a}$ is a function defining multiplication of generator a^i by generator a^j, where $i, j \leftarrow \text{rand}(\boldsymbol{N_4}^+)$, i.e., $\exp_{a,a}(i, j) = a^i a^j = a^{i+j}$. According to R_1 in (11), function $\exp_{a,a}(i, j)$ provides a 4-to-1 mapping and hence the value a^e obtained after the reduction of exponent a^{i+j} using R_1 will have a uniform random distribution.

Let us consider the double exponent function expexp_a: $\boldsymbol{N_4}^+ \times \Gamma \rightarrow \boldsymbol{S_a}$, where $\text{expexp}_a(i, k) = (a^i)^k$ with $I \in \boldsymbol{N_4}^+$, $k \in \Gamma$. This function provides a 2-to-1 mapping. Let i, k values are random and uniformly distributed, then the value $(a^i)^k$ is also random and uniformly distributed. The same is valid for the generator b and for complex exponents $\iota \cdot i$ and $\iota \cdot k$. In the latter case complex unit ι simply changes a to b and vice versa.

As a consequence, the mentioned above exponents of generators a, b are random and uniformly distributed.

If we have any word $w \in \boldsymbol{S}$ and exponentiate it by i, then after the reduction of exponents corresponding to the generators a and b the uniform distribution of resulting

exponents will be obtained. After that the generators are grouped according to the normal form defined in (15) and this grouping simply corresponds to computing expressions of the type $a^i a^j = a^{i+j}$. Hence the grouping procedure will not change the uniform distribution. As a result, we obtain uniformly distributed normal form w_η in (14).

These results are applied subsequently to the left MPF and right MPF (according to Definitions 1 and 2) to prove the uniform distribution of entries of matrices A and A' being a value of two sided MPF in Definition 3. The proof is performed by induction with respect to the order m of MPF matrices. The first step of induction for $m = 1$ is proved above.

The Lemma is proved. □

Lemma 3. *Suppose the following pairs of matrices $X, Y \leftarrow rand(\boldsymbol{M}_{\boldsymbol{\Gamma}})$, $U, V \leftarrow rand(\boldsymbol{M}_{\boldsymbol{\Gamma}})$, $X', Y' \leftarrow rand(\boldsymbol{M}_{\boldsymbol{\Gamma}})$, $U', V' \leftarrow rand(\boldsymbol{M}_{\boldsymbol{\Gamma}})$ and $H^{\backprime}, H^{\hat{}\prime\prime} \leftarrow rand(\boldsymbol{M}_{\boldsymbol{sNSR}})$ are generated uniformly at random. Then the distribution of entries of matrices S, T in (34) and of matrices S', T' computed by the relations.*

$$S' = U' + H^{\backprime} X', T' = V' + Y' H^{\hat{}\prime\prime}, \tag{36}$$

have the same uniform random distribution.

Proof of Lemma. Firstly, we prove that the product of matrices H′X, YH″ has the same uniform random distribution as the product of matrices H$^{\backprime}$X′, Y′H$^{\hat{}\prime\prime}$. Let us consider a scalar case with $h'x$, yh'' and $h^{\backprime}x'$, $y'h^{\hat{}\prime\prime}$ instead, where h', h'', $h^{\backprime}$, $h^{\hat{}\prime\prime} \in \boldsymbol{N}_4{}^+$ and $x, y, x', y' \in \boldsymbol{\Gamma}$. Then the multiplication function is defined by the mapping $\mathrm{mul}_{h,x}$: $\boldsymbol{N}_4{}^+ \times \boldsymbol{\Gamma} \to \boldsymbol{N}_4{}^+$ which according to Table 2 is 2-to-1. Since multipliers are chosen uniformly at random, then the value $\mathrm{mul}_{h,\,x}(h, x) = hx$ in $\boldsymbol{N}_4{}^+$ is distributed uniformly at random. The same is valid for other terms.

Now consider the addition function $\mathrm{add}_{u,z}$: $\boldsymbol{\Gamma} \times \boldsymbol{N}_4{}^+ \to \boldsymbol{N}_4{}^+$ which according to Table 1 is 2-to-1. Then, since the value $z = hx$ is distributed uniformly at random the value $\mathrm{add}_{u,\,z}(u, z) = s$ is also distributed uniformly at random.

The random and uniform distribution of entries of matrices $H'X$, YH'' and $H^{\backprime}X'$, $Y'H^{\hat{}\prime\prime}$ can be proved by induction using the uniform and random distribution of values of functions $\mathrm{mul}_{h,\,x}$ and $\mathrm{add}_{u,\,z}$. Then, the entries of matrices S, T and S', T' are distributed uniformly at random as well.

The Lemma is proved. □

Proof. Proceeding with the proof of the theorem, the response $R' = (S', T')$ must be computed referencing to (34). Then, the following random matrices in $\boldsymbol{M}_{\boldsymbol{NSR}}$ are generated independently: $U', V' \leftarrow \mathrm{rand}(\boldsymbol{M}_{\boldsymbol{\Gamma}})$, $X', Y' \leftarrow \mathrm{rand}(\boldsymbol{M}_{\boldsymbol{\Gamma}})$. As an additional input the simulator takes two challenge matrices $H^{\backprime}, H^{\hat{}\prime\prime} \leftarrow \mathrm{rand}(\boldsymbol{M}_{\boldsymbol{sNSR}} \times \boldsymbol{M}_{\boldsymbol{sNSR}})$. Then, according to (34):

$$S' = U' + H^{\backprime} X', T' = V' + Y' H^{\hat{}\prime\prime}. \tag{37}$$

Referencing to Lemmas 2 and 3, $R' = (S', T')$ and $R = (S, T)$ have the same uniform distribution and hence the distribution of ${}^{S'}W^{T'}$ is the same as the distribution of ${}^{S}W^{T}$ in (35). According to the Theorem 3 ${}^{S'}W^{T'}$ has the following expression

$${}^{S'}W^{T'} = {}^{(U'+H^{\backprime}X')}W^{(V'+Y'H^{\hat{}\prime\prime})} = {}^{U'}W^{V'} * {}^{U'}W^{Y'H^{\hat{}\prime\prime}} * {}^{H^{\backprime}X'}W^{V'} * {}^{H^{\backprime}X'}W^{Y'H^{\hat{}\prime\prime}} = {}^{U'}W^{V'} * ({}^{U'}W^{Y'})^{H^{\hat{}\prime\prime}} * {}^{H^{\backprime}}({}^{X'}W^{V'}) * {}^{H^{\backprime}}B^{H^{\hat{}\prime\prime}}, \tag{38}$$

where $B = {}^{X'}W^{Y'}$.

For given matrices U', V', X', Y' and $(H^{\backprime}, H^{\hat{}\prime\prime})$ generated uniformly at random and independently, Sim must compute a challenge $C' = (C_{0'}, C_{1'}, C_{2'})$ satisfying the following equation:

$${}^{S'}W^{T'} = C_{0'} * (C_{1'})^{H^{\hat{}\prime\prime}} * {}^{H^{\backprime}}(C_{2'}) * {}^{H^{\backprime}}A^{H^{\hat{}\prime\prime}} \tag{39}$$

Referencing to identity (37), Sim computes

$$C_{0'} = {}^{U'}W^{V'}, C_{1'} = {}^{U'}W^{Y'}, C_{2'} = {}^{X'}W^{V'} * B^{H^{\hat{}\prime\prime}} * A^{-H^{\hat{}\prime\prime}}. \tag{40}$$

According to Theorem 5, the entries of matrices $C_{0'}$, $C_{1'}$, have the same uniform distribution as of matrices C_0, C_1. Since (1) the distribution of ${}^{S'}W^{T'}$ is the same distribution as of ${}^{S}W^{T}$, (2) ${}^{X'}W^{V'}$ is uniformly distributed and (3) the computation of matrix $C_{2'}$ in (39) is based on Hadamar multiplication rule [16] (i.e., elementwise), then the distribution of $C_{2'}$ is the same as the distribution of C_2. Then the commitment $C' = (C_{0'}, C_{1'}, C_{2'})$ has the same distribution as $C = (C_0, C_1, C_2)$. It remains to prove that (C', H', R') is an accepting conversation using the following identities.

$$\begin{aligned} C_{0'} * (C_{1'})^{H^{\wedge''}} * H^{\wedge'}(C_{2'}) * H^{\wedge'}A^{H^{\wedge''}} &= {}^{U'}W^{V'} * ({}^{U'}W^{Y'})^{H^{\wedge'}} * H^{\wedge'}({}^{X'}W^{V'}) * H^{\wedge'}B^{H^{\wedge''}} * H^{\wedge'}A^{-H^{\wedge''}} * H^{\wedge'}A^{H^{\wedge''}} \\ &= {}^{S'}W^{T'} * H^{\wedge'}A^{H^{\wedge''}\text{-}H^{\wedge''}} = {}^{S'}W^{T'} * H^{\wedge'}A^{O} = {}^{S'}W^{T'} * E = {}^{S'}W^{T'}. \end{aligned} \quad (41)$$

The theorem is proved. □

Since special HVZK implies HVZK, then according to the Assumption 1 and Theorems 4 and 5, proposed MPF SIP is secure against the direct attack and is HVZK. The Theorem 19.3 in [19] states that if an identification protocol is secure against direct attacks, and is HVZK, then it is secure against eavesdropping attacks. Referencing to this result we have proven the following theorem.

Theorem 6. *MPF SIP is secure against the eavesdropping attack.*

Unfortunately, we are not able to prove the security of MPF SIP against an active attack since we have not proved the soundness of MPF SIP. Our construction is based on far more complicated algebraic structures than many traditional identification protocols including Schnorr protocol.

6. Selection of the Security Parameters and Efficiency Analysis

Since relations R_1, R_2 are fixed, the security parameter is the order m of matrices defining MPF. Then, according to (32) PrK and PuK matrix relation in the Definition 8 consists of m^2 exponent equations of the type (4). According to the Assumption 1 and the belief that the solution of randomly generated MQ system is hopeless when system consists of $n \geq 80$ equations with $v \geq 80$ variables [9], it is sensible to choose the number of exponent equations of the type (4) corresponding to the matrix equation (32) to be no less than 80. Then, m can be chosen to be equal to 10, 11, 12. In this case the number of exponent equations is equal to 100, 121, 144 correspondingly. To represent ***NSR*** elements of the types $t + \iota \cdot u + v$ and $t \cdot \iota + u + v \cdot \iota$, where $t, u, v \in \{1, 2, 3, 4\}$ 9 bits are required. Thus, memory requirement for PrK = (X, Y) is $2 \times 9\ m^2$ bits. To represent the word w in $\boldsymbol{S}$ in normal form (15) 6 bits are required. So, PuK = A representation requires $6\ m^2$ bits.

Effectivity of SIP is related to the left and right MPF value computations in (2) and (3) and can be performed using exponentiation tables of the size 4x4 in our case. Transformation of matrix entries to the normal form requires asymptotically O (m^2) operations. The computational resources for the one-sided MPF value computation are equivalent to the matrix multiplication and are asymptotically at most O (m^3). SIP realization for Prover requires 6 one-sided MPF values computation, 2 multiplication of matrices in ***NSR*** requiring O (m^3) operations and two additions of matrices in ***NSR*** requiring O (m^2) operations. Both matrix multiplication and addition can be performed using the table of operations of the size 4×4 as shown in Tables 1 and 2.

For the Verifier's side one must compute MPF values presented in (35). It takes two one-sided MPF computations for the left side of (35) and six one-sided MPF computations. Hence asymptotically it takes O (m^3) operations.

7. Discussion and Conclusions

It was an intriguing idea for the authors to create and analyze Sigma identification protocol (SIP) based on the matrix power function (MPF) defined over the specially selected algebraic structures, namely modified platform medial semigroup $\boldsymbol{S}$ and power near-

semiring (***NSR***). The initial medial semigroup is infinite, cancellative, multiplicative and non-commuting and is chosen to have two generators a and b. The modification of this medial semigroup is performed by introducing two extra relations R_1 and R_2 for the generators. It induces certain homomorphism yielding finite semigroup and preserving other properties of medial semigroup. In order to construct MPF, the certain power ***NSR*** is constructed. The properties of ***NSR*** are induced by the generic relation R_M of medial semigroup which makes addition operation non-commuting. Therefore, the notion of ***NSR*** is applied. The reason is that constructed ***NSR*** is simply not a semiring.

These algebraic structures are far more complicated than the structures used currently in well-known identification and sigma identification protocols, e.g., Schnorr or Okamoto protocols. They are based on relatively simple algebraic structures, namely cyclic groups $\boldsymbol{Z_p}^*$ or $\boldsymbol{G_q}$. MPF SIP construction based on more complicated algebraic structures was successful since a very important property of MPF presented in Proposition 2 was satisfied. In this connection we are expecting that proposed MPF SIP should provide greater security than existing Sigma protocols based on numerical cyclic groups. The investigation of the resistance against quantum cryptanalysis attack is very attractive and could be dedicated for the future research.

MPF, presented here, has some similarity to the certain MPF problem which was proven to be NP-complete in our previous publications [12,13]. It is believed so far that NP-complete problems cannot be effectively solved by quantum computers. The security of MPF SIP presented here relies on the assumption that this MPF problem is a candidate for one-way function (OWF).

Following the methodology, notions and security analysis of Sigma protocols presented in D. Boneh, and V. Shoup tutorial we proved that the proposed SIP is secure against the eavesdropping attack. Unfortunately, the proof that this protocol is secure against active attack was not presented since we have not proved the soundness of this protocol yet. The soundness of identification protocols is easily proven for simple algebraic structures, namely $\boldsymbol{Z_p}^*$ or $\boldsymbol{G_q}$. In our case, however, the algebraic structures are far more complicated and existing proof methodology used in cyclic groups cannot be applied.

Author Contributions: Conceptualization, methodology and investigation E.S.; Software, validation, writing—review and editing I.T.; Software, writing—original draft preparation A.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Acknowledgments: Many thanks to the Reviewers and their remarks, allowing us to substantially improve the security proof as well as the overall quality of the paper.

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

Abbreviations

Symbol	Explanation
ι	Imaginary unit in ***NSR***, wiyh the property $\iota^2 = 1$.
A	Public key (PuK) matrix and statement in MPF SIP.
a, b	Generators in modified medial semigroup $\boldsymbol{S}$.
aNSR	Anti Near-semiring to the ***NSR***.
$C = (C_0, C_1, C_2)$	Commitment consisting of three matrices C_0, C_1, C_2 and computed by the Prover.
DSA	Digital signature algorithm
ECDSA	Elliptic curve digital signature algorithm
H', H''	Challenge matrices generated by Verifier.
HFE	Hidden field equations cryptosystem

Symbol	Explanation
$\boldsymbol{M_{NSR}}$	Set of matrices over ***NSR***.
MPF	Matrix Power Function.
$MPF_S{}^{NSR}$	Matrix Power Function defined by the matrices over base semiring ***S*** and exponent matrices over ***NSR***.
$\boldsymbol{M_S}$	Set of matrices defined over semiring ***S***.
$\boldsymbol{N_0}$	Semiring of natural numbers with zero.
NSR	Near-semiring.
OWF	One-way function
PrK = (X, Y)	Private key or witness in MPF SIP consisting of two generated at random matrices X, Y over the ***NSR***.
PuK = A	Public key and statement for PrK consisting of matrix A over the semiring ***S***.
Rel	Effective relation for MPF SIP relating a witness-PrK with statement PuK.
RSA	Rivest, Shamir, Adleman cryptosystem
S	Modified medial semigroup.
s, t, u, v	Positive integers.
SIP	Sigma Identification Protocol.
$\boldsymbol{S_M}$	Medial semigroup.
sNSR	Sub-near-semiring in ***NSR***.
V, U	Random matrices generated in ***NSR*** for commitment C computation.
w	Word in medial semigroup $\boldsymbol{S_M}$ or modified medial semigroup ***S***.
X, Y	Component matrices of PrK and witness over the ***NSR***.
x, y, z	Exponents of generators in ***NSR***.

Appendix A. Numerical Example of the MPF SIP

A numerical illustration of the MPF SIP is presented below for the matrices with dimensions 3×3. Firstly, PrK = (X, Y) components are generated, where X,$Y \leftarrow$ rand($\boldsymbol{M_{NSR}}$). The entries of X, Y are chosen in the form $\{t + \iota \cdot u + v\}$ as elements in ***NSR*** (see Proposition 4), where t, u, v are in $\boldsymbol{N_4}^+ = \{1, 2, 3, 4\}$ according to Corollary 5.6. For convenience the imaginary unit ι in (17) is replaced by latin notation i.

$$X = \begin{bmatrix} 1+i+1 & 3+3i+3 & 1+3i+1 \\ 1+3i+1 & 1+i+1 & 3+3i+3 \\ 3+3i+3 & 1+3i+1 & 1+i+1 \end{bmatrix}$$

$$Y = \begin{bmatrix} 3+i+3 & 3+3i+1 & 1+i+3 \\ 1+i+3 & 3+i+3 & 3+3i+1 \\ 3+3i+1 & 1+i+3 & 3+i+3 \end{bmatrix}$$

Next, Public matrix W is generated at random ($W \leftarrow$ rand($\boldsymbol{M_S}$)) and PuK = $A = {}^X W^Y$ is computed referencing to (4), (21)–(23), (32).

$$W = \begin{bmatrix} ba^3b^3a & ba^2ba & bab^3a \\ bab^3a & ba^2b^3a & bab^2a \\ bab^3a & bab^3a & ba^3b^3a \end{bmatrix}$$

$$A = \begin{bmatrix} ba^4 & ba^3b^2a & bab^2a \\ ba^3b^2a & ba^4 & ba^2 \\ ba^2 & bab^2a & ba^3b^2a \end{bmatrix}$$

Two matrices U, V are generated U,$V \leftarrow$ rand($\boldsymbol{M_{sNSR}}$) for the computation of **commitment**.

$$U = \begin{bmatrix} 1+3i+3 & 3+i+3 & 3+3i+1 \\ 3+3i+1 & 1+3i+3 & 3+i+3 \\ 3+i+3 & 3+3i+1 & 1+3i+3 \end{bmatrix}$$

$$V = \begin{bmatrix} 3+i+1 & 3+3i+3 & 1+1i+3 \\ 1+1i+3 & 3+i+1 & 3+3i+3 \\ 3+3i+3 & 1+1i+3 & 3+i+1 \end{bmatrix}$$

Then, according to (33), Prover computes the **commitment** $C = (C_0, C_1, C_2)$ consisting of three matrices C_0, C_1, C_2 in $\boldsymbol{M_S}$ and sends it to the Verifier.

$$C_0 = \begin{bmatrix} ba^2 & ba^3b^2a & ba^3b^2a \\ ba^2 & ba^3b^2a & ba^3b^2a \\ ba^3b^2a & ba^2 & ba^2 \end{bmatrix}$$

$$C_1 = \begin{bmatrix} ba^4 & ba^3b^2a & bab^2a \\ ba^4 & ba^3b^2a & bab^2a \\ bab^2a & ba^2 & ba^4 \end{bmatrix}$$

$$C_2 = \begin{bmatrix} ba^2 & ba^3b^2a & ba^3b^2a \\ bab^2a & ba^4 & ba^4 \\ ba^4 & bab^2a & bab^2a \end{bmatrix}$$

Verifier generates the **challenge** consisting of two matrices H',H'' $\leftarrow$ rand($\boldsymbol{M_{sNSR}}$):

$$H' = \begin{bmatrix} 1+i+1 & 2+2i+2 & 3+3i+3 \\ 3+3i+3 & 1+i+1 & 2+2i+2 \\ 2+2i+2 & 3+3i+3 & 1+i+1 \end{bmatrix}$$

$$H'' = \begin{bmatrix} 4+4i+4 & 2+3i+4 & 1+2i+4 \\ 1+2i+4 & 4+4i+4 & 2+3i+4 \\ 2+3i+4 & 1+2i+4 & 4+4i+4 \end{bmatrix}$$

Upon receiving H',H'' the Prover computes the response matrices S, T according to (34) where $S = U + H'X$, $T = V + YH''$. The entries of these matrices are the exponents of generators a, b in semigroup $\boldsymbol{S}$ and are presented in non-reduced form.

$$S = U + H'X = \begin{bmatrix} 1+59i+67 & 1+45i+51 & 1+47i+55 \\ 1+47i+55 & 1+59i+67 & 1+45i+51 \\ 1+45i+51 & 1+47i+55 & 1+59i+67 \end{bmatrix}$$

$$T = V + YH'' = \begin{bmatrix} 1+74i+108 & 1+80i+110 & 1+72i+104 \\ 1+72i+104 & 1+74i+108 & 1+80i+110 \\ 1+80i+110 & 1+72i+104 & 1+74i+108 \end{bmatrix}$$

After reduction using relations R_1, R_2 in (11) the Prover computes the **response** $R = (S, T)$ and sends it to the Verifier, where matrices S, T are expressed in the following way:

$$S = U + H'X = \begin{bmatrix} 1+3i+3 & 1+i+3 & 1+3i+3 \\ 1+3i+3 & 1+3i+3 & 1+i+3 \\ 1+i+3 & 1+3i+3 & 1+3i+3 \end{bmatrix}$$

$$T = V + YH'' = \begin{bmatrix} 1+2i+4 & 1+4i+2 & 1+4i+4 \\ 1+4i+4 & 1+2i+4 & 1+4i+2 \\ 1+4i+2 & 1+4i+4 & 1+2i+4 \end{bmatrix}$$

Upon receiving $R = (S, T)$, Verifier checks if the identity (35) holds:

$${}^{S}W^{T} = C_0\, C_1^{H''\ H'} C_2\, {}^{H'} A^{H''} = \begin{bmatrix} ba^2ba & b^2a & b^4a \\ b^4a & ba^2b^3a & ba^2ba \\ b^2a & ba^2ba & ba^2b^3a \end{bmatrix}$$

Since in this case the identity (35) is satisfied, the Verifier outputs **accept**.

References

1. Myasnikov, A.; Shpilrain, V.; Ushakov, A. *Group-Based Cryptography*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2008.
2. Myasnikov, A.G.; Shpilrain, V.; Ushakov, A. *Non-Commutative Cryptography and Complexity of Group-Theoretic Problems*; American Mathematical Society: Providence, RI, USA, 2011.
3. Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **1997**, *26*, 1484–1509. [CrossRef]
4. Garey, M.; Johnson, D. *Computers and Intractability: A Guide to Theory of NP-Completeness*; H. Freeman: New York, NY, USA, 1979.
5. Chen, L.; Jordan, S.; Liu, Y.; Moody, D.; Peralta, R.; Perlner, R.; Smith-Tone, D. *Report on Post-Quantum Cryptography*; US Department of Commerce, National Institute of Standards and Technology: Gaithersburg, MD, USA, 2016; Volume 12.
6. Micciancio, D.; Regev, O. Lattice-based cryptography. In *Post-Quantum Cryptography*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 147–191.
7. 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.
8. Wolf, C. Hidden Field Equations. (HFE)-Variations and Attacks. Ph.D. Thesis, Ruhr-University, Bochum, Germany, 2002.
9. 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.
10. 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 1 July 2021).
11. Sakalauskas, E. The Multivariate Quadratic Power Problem over Zn is NP-complete. *Inf. Technol. Control* **2012**, *41*, 33–39. [CrossRef]
12. Sakalauskas, E.; Mihalkovich, A. MPF Problem over Modified Medial Semigroup Is NP-complete. *Symmetry* **2018**, *10*, 571. [CrossRef]
13. Mihalkovich, A.; Sakalauskas, E.; Luksys, K. Key Exchange Protocol Defined over a Non-Commuting Group Based on an NP-complete Decisional Problem. *Symmetry* **2020**, *12*, 1389. [CrossRef]
14. Sakalauskas, E. Enhanced matrix power function for cryptographic primitive construction. *Symmetry* **2018**, *10*, 43. [CrossRef]
15. Inassaridze, N.; Kandelaki, T.; Ladra, M. Categorical interpretations of some key agreement protocols. *J. Math. Sci.* **2013**, *195*, 439–444. [CrossRef]
16. Horn, R.A.; Johnson, C.R. *Matrix Analysis*; Cambridge University Press: Cambridge, UK, 2012.
17. Chrislock, J.L. On medial semigroups. *J. Algebra* **1969**, *12*, 1–9. [CrossRef]
18. Krishna, K.V. Near-Semirings: Theory and Application. Ph.D. Thesis, IIT Delhi, New Delhi, India, 2005.
19. Boneh, D.; Shoup, V. A Graduate Course in Applied Cryptography. Available online: https://toc.cryptobook.us/book.pdf (accessed on 1 July 2021).
20. Pierre, A.G. *Semigroups: An Introduction to the Structure Theory*; Routledge: Oxfordshire, UK, 2017.