mathematics

MDPI

Article

Sigma Identification Protocol Construction Based on MPF Defined over Non-Commuting Platform Group

Aleksejus Mihalkovich *,†, Kestutis Luksys † and Eligijus Sakalauskas †

Department of Applied Mathematics, Faculty of Mathematics and Natural Sciences, Kaunas University of Technology, 44249 Kaunas, Lithuania; kestutis.luksys@ktu.lt (K.L.); eligijus.sakalauskas@ktu.lt (E.S.)

* Correspondence: aleksejus.michalkovic@ktu.lt

† These authors contributed equally to this work.

Abstract: In this paper, we present the construction of a sigma identification protocol based on matrix power function (MPF) defined over a certain non-commuting platform group. We use the previously defined templates for generating public parameters of our protocol to overcome the problem that a two-sided MPF in general is not associative. We prove that the proposed sigma identification protocol is resistant to eavesdropping adversary attacks. Furthermore, relying on the asymptotic knowledge soundness property proven in this paper, we show that our protocol is also resistant against active adversary attacks with an overwhelming probability.

Keywords: sigma identification protocol; matrix power function; non-commuting cryptography

MSC: 94A60

Citation: Mihalkovich, A.; Luksys, K.; Sakalauskas, E. Sigma Identification Protocol Construction Based on MPF Defined over Non-Commuting Platform Group. *Mathematics* **2022**, *10*, 2649. https://doi.org/10.3390/math10152649

Academic Editor: Angel Martín-del-Rey

Received: 28 June 2022
Accepted: 25 July 2022
Published: 28 July 2022

1. Introduction

In the virtual world, protection of user identities is extremely important. However, to gain access to some restricted information, the user has to identify himself first. Naive approaches to this procedure such as a password system have proven ineffective and insufficient since many people use rather simple and easy-to-remember passwords, and many ways are known to recover them, e.g., dictionary attacks, total scan, or even personal experience. Hence, it may be easy to forge an identity by impersonating someone close, such as a friend or a work colleague. Though there exist a number of techniques to aggravate password recovery, it is clear that the lifespan of such systems is short. The sooner these disappear, the safer it will be for us all.

A modern solution to user identification problems is to use protocols designed specifically for such needs. Identification (ID) protocols are executed between two parties: the Prover and the Verifier. The Prover possesses a pair of keys **PrK** and **PuK** that are related to his/her identity. In ID protocols, **PrK** is usually called a witness for the statement **PuK**. Secure ID protocols are executed by the conversation between Prover and Verifier and must satisfy the zero-knowledge proof (ZKP) paradigm, i.e., the Prover proves his identity without revealing **PrK**, in which case conversation is accepted. The information available to the Verifier is the Prover's public key **PuK** (the statement) and additional data computed during protocol execution [1].

In this paper, we consider an approach to creating an identification protocol proposed by Schnorr in [2]. His scheme was later named the sigma protocol since its three-step structure resembles the Greek letter Σ. This general structure is shown below in Figure 1. Similarly, Okamoto protocol [3] or Chaum–Pedersen protocol [4] can be adapted to obtain working SIPs on their bases.

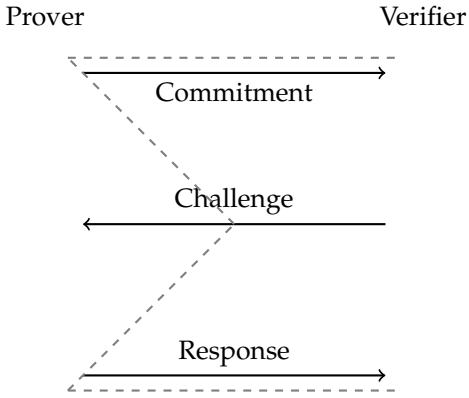

Figure 1. The structure of a sigma protocol.

Evidently, the Verifier has to check if the received response truly identifies the Prover and, if so, grants him access to the restricted content. Therefore the sigma identification protocol (SIP) has to withstand any impersonation attacks.

Direct attacks are fairly easy to handle. These are aimed at the recovery of the private key of the user given his public key. In this way, an attacker can impersonate a legal user by acquiring full access to his personal data. Direct attacks can be avoided by using one-way functions—a concept well-known in modern cryptography.

Eavesdropping impersonation attacks are dealt with by ensuring that an unauthorized user cannot acquire any useful information based on the conversation between the two parties of SIP. In this scenario, the attacker is passive, i.e., he just listens to the conversations without making any efforts to modify them in some way. SIP can withstand this type of attack if it can be viewed as a zero-knowledge proof, i.e., any Prover who can identify himself knows some private information (namely the secret key k) that is linked to his physical identity.

An active impersonation attacker tries to gain valuable information from conversations by carefully selecting challenges and responses in such a way that he could produce an acceptable conversation without having to acquire the user's private key. In this case, both parties of the SIP are protected by the knowledge soundness property, i.e., a malicious user can be identified using two acceptable conversations with identical commitments.

Sigma protocol is a concept well-known to cryptographic society. Though Schnorr sigma protocol is the most classic example, other similar protocols have been proposed. Several examples can be found in [5], where Beullens considered sigma protocols with a helper and used the Fiat–Shamir transform to obtain signature schemes. Furthermore, in his paper, Beullens analyses zero-knowledge-based post-quantum signatures and mentions the permuted kernel problem (PKP), which requires finding an unknown permutation such that the permuted vector $\vec{\mathbf{v}}$ is in the null space of the linear operator $\mathbf{A}$ given that $\mathbf{A}$ and $\vec{\mathbf{v}}$ are known. This problem together with the considered signature scheme was proposed by Shamir in [6] and is known to be HP-hard. To our knowledge, it is the closest scheme to our proposition (at least in the sense that it relies on the problem being defined for linear operators).

The drawback of the Shamir approach is its knowledge soundness property, which necessitates a large number of parallel rounds to obtain a secure signature [5]. Our approach to constructing a working SIP involves matrix operations as well. However, as opposed to schemes considered in [5], we expect a significantly better result regarding the soundness property of our SIP.

The traditional approach for SIP construction makes use of a discrete exponent function over a large finite ring of integers. Examples of such protocols were proposed by Schnorr in [2], Okamoto in [3], and Chaum and Pedersen in [4]. The security of such protocols relies on the discrete logarithm problem (DLP). However, our research is based on an assumption that the DLP can be solved effectively since we use matrix operations. Since these operations can be executed by using reasonably small multiplication and expo-

nentiation tables, we gain a significant boost in performance as compared to the traditional approach. Furthermore, the security of the SIP proposed in this paper relies on different phenomena, namely the complexity of inverting the so-called matrix power function (MPF). It was previously proven in [7] that this problem is NP-complete. We think that at the very least it can be considered evidence that our proposal is resistant to quantum cryptanalysis. This comes from an assumption that NP-complete problems are hard to crack even for quantum computers. Important to note is the fact that we used the same templates defined in [8]. Notably, DLP does not provide sufficient security against quantum cryptanalysis.

In this paper, we continue our research in the non-commuting asymmetric cryptography field. Recently we demonstrated how two users can agree on a shared key by executing a key exchange protocol based on the MPF defined over a non-commuting platform group [8]. There we used highly non-linear matrix mapping, where the entries of the base matrix were chosen from a non-commuting modular group of size 16. We revise the definitions of this mapping and the so-called group $\mathtt{M}_{16}$ as well as their basic properties in greater detail in the upcoming Section 2. Notably, there we define templates for the base matrix and the power matrices in such a way that key exchange would be successful despite the lack of some important properties of MPF.

Our previous attempt to construct a SIP using MPF defined over a non-commuting semigroup was presented in [9]. There, MPF was defined over the non-commuting medial semigroup, which by nature, is almost commuting. This property implies that the main MPF identity necessary to construct a SIP is valid together with the two-sided associativity of MPF [9]. In that paper, we have shown that the proposed SIP is resistant to passive impersonation attacks by demonstrating that our protocol is a special honest Verifier zero knowledge.

Things go differently and are more complicated if we consider inherently non-commuting platform groups or semigroups. In this case, we lose two-sided associativity, but in doing so, we increase expected security. The problem was solved by defining the sets of commuting matrices for the private key (**PrK**) and commitment matrices generation. This is precisely the idea we used previously to construct a working key exchange between Alice and Bob. Further examination of the properties of MPF defined over $\mathtt{M}_{16}$ has shown that the templates presented in [8] are suitable for our current goals. Hence, in this paper, we present SIP based on the MPF defined over the non-commuting group $\mathtt{M}_{16}$. Due to the result proven in [7], we expect that our proposal belongs to the field of post-quantum cryptography.

As we have mentioned, in Section 2, we revise the mathematical background used in this paper. After that, we present the main object of this paper—a working SIP based on MPF—in Section 3. In Section 4, we consider the resistance of our SIP to impersonation attacks as described above. Lastly, we present our conclusions at the end of the paper.

2. Mathematical Background

The main mapping used in our research is the MPF. In some sense, this mapping is a generalization of exponentiation operation defined for matrices. Interestingly enough, it also resembles regular matrix multiplication with slightly changed operations.

Let us revise basic definitions related to MPF. To start with, let us denote by $\mathbb{S}$ a multiplicative semigroup with maximal order of its elements denoted by $\mathrm{ord}(\mathbb{S})$. Hence, we have:

$$s^{\mathrm{ord}(\mathbb{S})} = 1, \quad \forall s \in \mathbb{S},$$

where 1 is the unit of $\mathbb{S}$. We call $\mathbb{S}$ a platform semigroup. Moreover, we refer to the ring of integers $\mathbb{Z}_{\mathrm{ord}(\mathbb{S})}$ as the power ring.

We now define the sets of $m \times m$ square matrices by $Mat_m(\mathbb{S})$ and $Mat_m(\mathbb{Z}_{\mathrm{ord}(\mathbb{S})})$, indicating that the entries of the matrices are in the specified set. Then, we can formally define the left-sided MPF as a mapping $LMPF_{\mathbf{W}}(\mathbf{X}) : Mat_m(\mathbb{Z}_{\mathrm{ord}(\mathbb{S})}) \to Mat_m(\mathbb{S})$ denoted as follows:

$$^{\mathbf{X}}\mathbf{W} = \mathbf{E}_L, \tag{1}$$

where $\mathbf{W} \in Mat_m(\mathbb{S})$ is called the base matrix and is a parameter of the left-sided MPF, $\mathbf{X} \in Mat_m(\mathbb{Z}_{\mathrm{ord}(\mathbb{S})})$ is called the power matrix and is the argument of the left-sided MPF, and $\mathbf{E}_L$ is called the matrix exponent and is the value of the left-sided MPF. Entries of the latter matrix are calculated as follows:

$$(e_L)_{ij} = \prod_{k=1}^{m} w_{kj}^{x_{ik}}.$$

Similarly we can define the right-sided MPF as a mapping $RMPF_{\mathbf{W}}(\mathbf{Y}) : Mat_m(\mathbb{Z}_{\mathrm{ord}(\mathbb{S})}) \rightarrow Mat_m(\mathbb{S})$ denoted as follows:

$$\mathbf{W}^{\mathbf{Y}} = \mathbf{E}_R, \tag{2}$$

where $\mathbf{E}_L$ is the value of the right-sided MPF with entries obtained in the following way:

$$(e_R)_{ij} = \prod_{l=1}^{m} w_{il}^{y_{lj}}.$$

Consequently, the two-sided MPF (or MPF for short) can be defined if the order of matrix exponentiation (in sense of left-sided and right-sided MPFs) does not matter, in which case we have:

$${}^{\mathbf{X}}\mathbf{W}^{\mathbf{Y}} = \mathbf{E}, \tag{3}$$

where the entries of the matrix exponent $\mathbf{E}$ are calculated in the following way:

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

It has been proven previously in [10] that the two-sided MPF can always be defined if the platform semigroup $\mathbb{S}$ is commuting due to the following property:

$$\left({}^{\mathbf{X}}\mathbf{W}\right)^{\mathbf{Y}} = {}^{\mathbf{X}}\left(\mathbf{W}^{\mathbf{Y}}\right). \tag{4}$$

Assuming that MPF is a conjectured one-way function (OWF) [11], matrix $\mathbf{W}$ is associated as a public parameter, matrices $(\mathbf{X}, \mathbf{Y})$ as the private key $(\mathbf{PrK})$, and matrix $\mathbf{E}$ as the public key $(\mathbf{PuK})$.

However, in general, the associativity property (4) does not hold if the platform semigroup is non-commuting, which is exactly the case of our study in this paper. Hence, in general, the order of actions has to be specified by the brackets. Furthermore, since the defined MPFs are quite similar, we refer to all three of them as MPFs, since it is obvious from the presented expressions which one of the three mappings we refer to.

Previously in our research, we mostly used commuting platform semigroups $\mathbb{S}$. However, it was later pointed out by the authors of [12] that cryptographic protocols presented in [13,14] were vulnerable to an attack based on linear algebra. One of the ideas the authors of [12] proposed is that non-commuting algebraic structures could be used as a platform for MPF.

Partly due to this reason (although there were other reasons, too), we began a search for suitable non-commuting algebraic groups to be used in our research. One such group was mentioned in [15] and drew our attention due to its simplicity. The modular group $\mathtt{M}_{16}$ is just one of the family of groups of this type. Larger groups with essentially the same structure can be found in [16,17]. In this paper, we consider only the group $\mathtt{M}_{16}$, leaving the other ones for future work.

Notably, the authors of [15] mentioned the group $\mathtt{M}_{16}$ as one of the seven indecomposable groups of size 16, meaning that it is not isomorphic to any products of low-order groups. The general representation of this group is given below:

$$\mathtt{M}_{16} = \langle a, b \mid a^8 = 1, b^2 = 1, ba = a^5 b \rangle,$$

where a and b are two non-commuting generators of the group $\mathtt{M}_{16}$. It can be shown that the cardinality of this group is 16, which is indicated by the index. Basic operations in $\mathtt{M}_{16}$ were explored in [18]. There, we also showed that each element of the considered group can be written in the form $b^{\alpha}a^{x}$, where $\alpha \in \mathbb{Z}_2$ and $x \in \mathbb{Z}_8$. We use this representation throughout the paper. However, to shorten this paper, we omit explicit formulas for basic operations in $\mathtt{M}_{16}$. These can be found in [18].

Since $\mathtt{M}_{16}$ is a non-commuting group, the associativity property (4) fails, along with the following properties of one-sided MPFs, which hold for the commuting semigroup $\mathbb{S}$:

$$\mathbf{X}^{-1}\left({}^{\mathbf{X}}\mathbf{W}\right) = \mathbf{W}; \quad \left(\mathbf{W}^{\mathbf{Y}}\right)^{\mathbf{Y}^{-1}} = \mathbf{W}. \tag{5}$$

To overcome the absence of these properties in [8], we defined templates for the base matrix $\mathbf{W}$ and both power matrices $\mathbf{X}$ and $\mathbf{Y}$. We revise these templates in the next section to keep everything in one place.

3. Sigma Identification Protocol

Our first attempt to present a working SIP based on MPF was made in [9]. Though it was a rather successful idea, our proposal lacked the proof of knowledge soundness property. Essentially, it states that given an input statement and two accepting conversations with distinct commitments, it is always possible to extract a witness for the given statement [1]. Since the multiplicative order of $\mathtt{M}_{16}$ is equal to 8, which is a composite number, we cannot achieve knowledge soundness in the sense of the presented definition. However, in this paper, we prove an important proposition, which demonstrates that it is possible to achieve a slightly weaker asymptotic result concerning this notion.

In this paper, we use the modular group $\mathtt{M}_{16}$ to establish a SIP. Using elements of this group, we define the template for the matrix $\mathbf{W}$ in the following way:

$$\mathbf{W} = \begin{pmatrix} ba^{2\omega_{11}+1} & a^{\omega_{12}} & \dots & b^{\alpha_{1c}}a^{\omega_{1c}} & \dots & ba^{2\omega_{1m}+1} \\ a^{2\omega_{21}} & a^{\omega_{22}} & \dots & b^{\alpha_{2c}}a^{\omega_{2c}} & \dots & a^{2\omega_{2m}} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a^{2\omega_{i1}} & a^{\omega_{i2}} & \dots & b^{\alpha_{ic}}a^{\omega_{ic}} & \dots & a^{2\omega_{im}} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a^{2\omega_{(m-1)1}} & \dots & \dots & \dots & \dots & a^{2\omega_{(m-1)m}} \\ ba^{2\omega_{m1}+1} & a^{\omega_{m2}} & \dots & b^{\alpha_{mc}}a^{\omega_{mc}} & \dots & ba^{2\omega_{mm}+1} \end{pmatrix}, \tag{6}$$

where the values of ω_{ij} can be chosen randomly from the ring $\mathbb{Z}_8$.

Furthermore, let us define two additional matrices, $\mathbf{L}$ and $\mathbf{R}$, satisfying the following templates:

$$l_{i1} + l_{im} \equiv 0 \bmod 2 \quad \forall i = 1, 2, \dots, m. \tag{7}$$

$$r_{cj} \equiv \begin{cases} 2 \bmod 4, & \text{if } j = c \\ 0 \bmod 4, & \text{otherwise} \end{cases} \quad \forall j = 1, 2, \dots, m. \tag{8}$$

Due to the lack of the associativity property (4) in the general case, the purpose of the presented templates is to ensure that the SIP is valid. In other words, if these templates are neglected, then the correctness of the protocol fails, i.e., the Prover and the Verifier are not capable of producing an accepting conversation. The reason behind this is the non-commutative nature of the platform group $\mathtt{M}_{16}$. This nature is represented by the extra summands appearing when performing operations with the elements of $\mathtt{M}_{16}$ due to the identity $ba = a^5b$. The purpose of the templates is to control these extra summands.

Publicly fixed parameters are the modular group $\mathtt{M}_{16}$, the ring of integers $\mathbb{Z}_8$, and the order of the square matrices m. Matrix $\mathbf{W} \in Mat_m(\mathtt{M}_{16})$ is chosen randomly according to the presented template (6) and is published online. Moreover, public matrices $\mathbf{L}$ and $\mathbf{R}$, satisfying templates (7) and (8), respectively, are chosen.

The Prover generates his data: a private key $\mathbf{PrK} = (\mathbf{X}, \mathbf{Y})$, where $\mathbf{X}, \mathbf{Y} \in Mat_m(\mathbb{Z}_8)$ can be expressed as polynomials of $\mathbf{L}$ and $\mathbf{R}$, respectively, and a public key $\mathbf{PuK} = \left({}^{\mathbf{X}}\mathbf{W}\right)^{\mathbf{Y}}$. More specifically, we have:

$$\mathbf{X} = x_1\mathbf{L} + x_2\mathbf{L}^2 + \ldots + x_{m-1}\mathbf{L}^{m-1} = \sum_{i=1}^{m-1} x_i\mathbf{L}^i; \tag{9}$$

$$\mathbf{Y} = y_1\mathbf{R} + y_2\mathbf{R}^2 + \ldots + y_{m-1}\mathbf{R}^{m-1} = \sum_{i=1}^{m-1} y_i\mathbf{R}^i; \tag{10}$$

We define the public key $\mathbf{PuK}$ of the Prover using one-sided MPF denoted by $LMPF_{\mathbf{W}}(\mathbf{X})$ and $RMPF_{\mathbf{E}_L}(\mathbf{Y})$. Note that since the order of actions has to be taken into the consideration, the parameter of the left-sided MPF is the publicly known matrix $\mathbf{W}$, whereas the parameter of the right-sided MPF is the matrix $\mathbf{E}_L$ and is not visible online. As mentioned previously, matrices $\mathbf{W}, \mathbf{E}_L \in Mat_m(\mathtt{M}_{16})$, whereas $\mathbf{X}, \mathbf{Y} \in Mat_m(\mathbb{Z}_8)$. Hence, the $\mathbf{PuK} \in Mat_m(\mathtt{M}_{16})$ is calculated in the following way:

$$\mathbf{PuK} = \left({}^{\mathbf{X}}\mathbf{W}\right)^{\mathbf{Y}} = \mathbf{A} \tag{11}$$

In the concept of an ID protocol, the pair $(\mathbf{X}, \mathbf{Y})$ is a witness for the statement $\mathbf{A}$. Further, private matrices $\mathbf{X}$ and $\mathbf{Y}$ commute with $\mathbf{L}$ and $\mathbf{R}$, respectively.

Assume that the Prover desires to prove his identity to the Verifier without revealing it. He initiates the following three-step communication:

1. The Prover picks at random two coefficient vectors $\vec{u}$ and $\vec{v}$ and computes matrices $U, V \in Mat_m(\mathbb{Z}_8)$ as polynomials of $\mathbf{L}$ and $\mathbf{R}$, i.e.,

$$\mathbf{U} = \sum_{i=1}^{m-1} u_i\mathbf{L}^i; \tag{12}$$

$$\mathbf{V} = \sum_{i=1}^{m-1} v_i\mathbf{R}^i; \tag{13}$$

Using these matrices, he calculates a commitment as the following triplet $\vec{\mathbf{C}} = \{\mathbf{C}_0, \mathbf{C}_1, \mathbf{C}_2\}$:

$$\mathbf{C}_0 = \left({}^{\mathbf{U}}\mathbf{W}\right)^{\mathbf{V}}, \quad \mathbf{C}_1 = \left({}^{\mathbf{U}}\mathbf{W}\right)^{\mathbf{Y}}, \quad \mathbf{C}_2 = \left({}^{\mathbf{X}}\mathbf{W}\right)^{\mathbf{V}}. \tag{14}$$

2. The Verifier generates a challenge in the form of $\vec{\mathbf{H}} = \{\mathbf{H}_1, \mathbf{H}_2\}$, where $\mathbf{H}_1 \in Sp(\mathbf{L}), \mathbf{H}_2 \in Sp(\mathbf{R})$. Here, we used a convenient notations $Sp(\mathbf{L})$ and $Sp(\mathbf{R})$ to denote linear spans of the first $m-1$ powers of $\mathbf{L}$ and $\mathbf{R}$, respectively. He sends the challenge $\vec{\mathbf{H}}$ to the Prover.
3. The Prover responds by computing a vector $\vec{\mathbf{S}} = \{\mathbf{S}_1, \mathbf{S}_2\}$, where:

$$\mathbf{S}_1 = \mathbf{U} + \mathbf{H}_1\mathbf{X};$$
$$\mathbf{S}_2 = \mathbf{V} + \mathbf{Y}\mathbf{H}_2.$$

The response $\vec{\mathbf{S}}$ is sent to the Verifier.

The Verifier accepts if the following identity is valid:

$$\left({}^{\mathbf{S}_1}\mathbf{W}\right)^{\mathbf{S}_2} = \mathbf{C}_0 \odot \mathbf{C}_1^{\mathbf{H}_2} \odot {}^{\mathbf{H}_1}\mathbf{C}_2 \odot {}^{\mathbf{H}_1}\mathbf{A}^{\mathbf{H}_2}. \tag{15}$$

Interestingly enough, the order of actions on the right-hand side of identity (15) does not matter since all the base matrices (i.e., $\mathbf{C}_i$s and $\mathbf{A}$) consist of commuting entries.

Note also that the Prover uses parts of his private key to compute the commitment $\vec{\mathbf{C}}$. This fact distinguishes our scheme from others, e.g., Schnorr or Okamoto sigma protocols.

The validity of the presented protocol relies on the following facts:

Fact 1. The defined templates (7) and (8) are preserved for polynomial structure (9)–(13) of power matrices X, Y, U, V.

Fact 2. Due to the template (7), the intermediate result of raising $\mathbf{W}$ to the matrix power on the left has identical distribution of generator b. In other words, the locations of this generator in the intermediate result are constant for all matrices in the set $Sp(\mathbf{L})$.

Fact 3. Due to the template (8), the matrix exponent has commuting entries contained in the set $\langle a \rangle = \{e, a, a^2, \ldots, a^7\}$.

Fact 4. All the left power matrices commute. The same is true for right power matrices.

Due to the presented facts, the following identity holds:

$$^{\mathbf{U}}\left(\left(^{\mathbf{X}}\mathbf{W}\right)^{\mathbf{Y}}\right)^{\mathbf{V}} = {}^{\mathbf{X}}\left(\left(^{\mathbf{U}}\mathbf{W}\right)^{\mathbf{V}}\right)^{\mathbf{Y}}.$$

Notably, the latter identity resembles a similar property of MPF if the platform group is commuting. However, in our case, the order of actions has to be taken into consideration. Nevertheless, due to Facts 2 and 3, we can perform actions with power matrices on both sides, such as collecting or distributing through terms as if the platform group was commuting, as long as we stick to the defined templates. For these reasons we have:

$$\mathbf{C}_0 \odot \mathbf{C}_1^{\mathbf{H}_2} \odot {}^{\mathbf{H}_1}\mathbf{C}_2 \odot {}^{\mathbf{H}_1}\mathbf{A}^{\mathbf{H}_2} = \left(^{\mathbf{U}}\mathbf{W}\right)^{\mathbf{V}} \odot \left(\left(^{\mathbf{U}}\mathbf{W}\right)^{\mathbf{Y}}\right)^{\mathbf{H}_2} \odot {}^{\mathbf{H}_1}\left(\left(^{\mathbf{X}}\mathbf{W}\right)^{\mathbf{V}}\right) \odot {}^{\mathbf{H}_1}\left(\left(^{\mathbf{X}}\mathbf{W}\right)^{\mathbf{Y}}\right)^{\mathbf{H}_2} =$$
$$= \left(^{\mathbf{U}+\mathbf{H}_1\mathbf{X}}\mathbf{W}\right)^{\mathbf{V}+\mathbf{Y}\mathbf{H}_2} = \left(^{\mathbf{S}_1}\mathbf{W}\right)^{\mathbf{S}_2}.$$

It is also important to note that public key generation is one-way under the assumption that MPF is a candidate OWF. The two major facts supporting our assumption are:

- All the matrices defined over the ring $\mathbb{Z}_8$ satisfying templates (7) and (8) are not invertible modulo 2, and hence, the same is true for modulo 8;
- Since `text` is indecomposable, the discrete logarithm mapping or any kind of its analog cannot be defined for the elements of this group.

It is important to note that these two facts are also the key factors that protect our protocol from the attack presented in [12]. In other words, the presented facts prevent the transformation of Equation (11) to a linear form, thus protecting both the Prover and the Verifier.

Notably, it is possible to define the discrete logarithm function for $\mathbf{C}_i$s and $\mathbf{A}$. However, by that point, the non-commutative nature of $\mathtt{M}$ has been lost, and hence, this fact cannot be used for cryptanalysis of our protocol. Moreover, since during the verification process the value of $\left(^{\mathbf{S}_1}\mathbf{W}\right)^{\mathbf{S}_2}$ is unknown, there are too many variables to deal with despite the fact that a discrete logarithm can be applied to the expression $\mathbf{C}_0 \odot \mathbf{C}_1^{\mathbf{H}_2} \odot {}^{\mathbf{H}_1}\mathbf{C}_2 \odot {}^{\mathbf{H}_1}\mathbf{A}^{\mathbf{H}_2}$.

Combined, these facts protect both protocol parties from the approach presented in [12]. Moreover, in [7], we proved NP-completeness of an MPF problem defined over $\mathtt{M}_{16}$ with precisely the setup for power matrices described in this paper. Interestingly enough, the lack of invertible matrices was greatly beneficial in that proof.

4. Security against Eavesdropping and Active Adversaries

One-wayness of the MPF ensures that our proposal can withstand direct attacks, i.e., the secret key $(\mathbf{X}, \mathbf{Y})$ cannot be extracted from the public key $\mathbf{A}$.

However, to resist other possible attacks on our sigma protocol, we have to establish other important properties. First, we consider the special honest Verifier zero knowledge (HVZK) property described explicitly in [1].

Theorem 1. *The MPF-based Sigma protocol presented above is a special HVZK.*

Proof. The simulator takes as an input the public key $\mathbf{A}$ and the challenge $\vec{\mathbf{H}}$, where $\mathbf{H}_1 \in Sp(\mathbf{L})$ and $\mathbf{H}_2 \in Sp(\mathbf{R})$. Furthermore, it generates the response vector $\vec{\mathbf{S}}$ by uniformly selecting matrices $\mathbf{S}_1 \in Sp(\mathbf{L})$ and $\mathbf{S}_2 \in Sp(\mathbf{R})$. Using this information, the simulator computes the commitment vector as follows:

$$\vec{\mathbf{C}} = \{ {}^{\mathbf{S}_1-\mathbf{H}_1}\mathbf{W}^{\mathbf{S}_2-\mathbf{H}_2}; {}^{\mathbf{S}_1-\mathbf{H}_1}W; \mathbf{W}^{\mathbf{S}_2-H_2} \odot \mathbf{W}^{\mathbf{H}_2} \odot \mathbf{A}^{-\mathbf{H}_2} \}. \tag{16}$$

The output is an accepting conversation $(\vec{\mathbf{C}}, \vec{\mathbf{H}}, \vec{\mathbf{S}})$ for the public key $\mathbf{A}$, since

$$\left({}^{\mathbf{S}_1-\mathbf{H}_1}\mathbf{W}^{\mathbf{S}_2-\mathbf{H}_2}\right) \odot \left({}^{\mathbf{S}_1-\mathbf{H}_1}\mathbf{W}\right)^{\mathbf{H}_2} \odot {}^{\mathbf{H}_1}\left(\mathbf{W}^{\mathbf{S}_2-\mathbf{H}_2} \odot \mathbf{W}^{\mathbf{H}_2} \odot \mathbf{A}^{-\mathbf{H}_2}\right) \odot {}^{\mathbf{H}_1}\mathbf{A}^{\mathbf{H}_2} = {}^{\mathbf{S}_1}\mathbf{W}^{\mathbf{S}_2}$$

as desired.

Notably, in our previous paper [8], we considered the distribution of the entries of the matrix exponent $\mathbf{A}$. There we showed that for power matrices $\mathbf{X}$ and $\mathbf{Y}$ uniformly chosen from $Sp(\mathbf{L})$ and $Sp(\mathbf{R})$, this distribution is asymptotically uniform. Correcting a small issue in that proof, we claim that the obtained distribution is, in fact, uniform, since in the last step there is no longer the need to apply limits. Hence, we have identical results for the simulator and the parties of the protocol. □

Secondly, we consider the knowledge soundness property of our scheme. We begin by establishing a one-to-one link between the pairs $(\mathbf{X}, \mathbf{Y})$ and $(\mathbf{U}, \mathbf{V})$. We base our proof on the following property of the MPF:

$$\left({}^{\alpha\mathbf{X}}\mathbf{W}\right)^{\alpha^{-1}\mathbf{Y}} = \left({}^{\mathbf{X}}\mathbf{W}\right)^{\mathbf{Y}}. \tag{17}$$

The proof of this property in the case of a commuting platform semigroup follows immediately from the definition of the MPF. Hence, the solutions of Equation (11) come from the set of proportional matrices $(\alpha\mathbf{X}', \alpha^{-1}\mathbf{Y}')$, where $\mathbf{W}$ and $\mathbf{A}$ are publicly known and $\mathbf{X}', \mathbf{Y}'$ is some solution of (11). An essential fact is that these are the only solutions given that the platform group is $\mathbb{Z}_p$ and the power ring is $\mathbb{Z}_{p-1}$, where p is a prime.

Notably, since multiplying by a coefficient preserves the defined templates of the matrices, the property (17) holds for the non-commuting platform group $\mathtt{M}_{16}$ as well. In fact, since in our case $\alpha^{-1} \equiv \alpha \bmod 8$ for all odd values of α, the presented family of solutions consists of 4 distinct pairs. Evidently, all $\mathbf{X}'$s in these pairs also commute with matrix $\mathbf{L}$, whereas all $\mathbf{Y}'$s commute with matrix $\mathbf{R}$. Due to the fact that as of now we cannot prove the absence of other solutions of (11) in the case of non-commuting platform group $\mathtt{M}_{16}$, we introduce the following heuristic:

Heuristic 1. *All the solutions* $(\mathbf{X}', \mathbf{Y}')$ *of Equation* (11) *with respect to* $(\mathbf{X}, \mathbf{Y})$ *satisfying the commutativity constraints can be written as follows:*

$$\mathbf{X}' = \alpha\mathbf{X}, \quad \mathbf{Y} = \alpha^{-1}\mathbf{Y},$$

where α *is an odd element of* $\mathbb{Z}_8$.

Relying on the presented heuristic, we prove the following lemma:

Lemma 1 (Private key alternative)**.** *Assume that the private key* $\mathbf{PrK} = (\mathbf{X}, \mathbf{Y})$ *is fixed and the Heuristic 1 holds. Then, there is a unique pair* $(\mathbf{U}, \mathbf{V})$ *such that* $\mathbf{U} \in Sp(\mathbf{L})$ *and* $\mathbf{V} \in Sp(\mathbf{R})$*, which corresponds to the fixed commitment vector* $\vec{\mathbf{C}}$*.*

Proof. Let us consider the system of Equation (14). Then due to the presented heuristic, we have the following families of solutions for each of the presented equations (if we consider them individually): $((\beta\mathbf{U}, \beta\mathbf{V}))$, $((\gamma\mathbf{U}, \gamma\mathbf{Y}))$ and $((\delta\mathbf{X}, \delta\mathbf{V}))$. However, since the private key can be expressed as $\mathbf{X}' = \alpha\mathbf{X}$ and $\mathbf{Y}' = \alpha\mathbf{Y}$, all three presented families of solutions intersect at $\beta = \alpha$, $\gamma = \alpha$, and $\delta = \alpha$. Hence, the pair of matrices $(\alpha\mathbf{U}, \alpha\mathbf{V})$ corresponds to a secret pair $(\alpha\mathbf{X}, \alpha\mathbf{Y})$. Evidently, this pair is unique, which completes the proof. □

Consider the following system of matrix relations:

$$\begin{aligned} \mathbf{A}(\mathbf{X}, \mathbf{Y}, \mathbf{U}, \mathbf{V}) &= \left({}^{\mathbf{X}}\mathbf{W}\right)^{\mathbf{Y}}, \\ \mathbf{C}_0(\mathbf{X}, \mathbf{Y}, \mathbf{U}, \mathbf{V}) &= \left({}^{\mathbf{U}}\mathbf{W}\right)^{\mathbf{V}}, \\ \mathbf{C}_1(\mathbf{X}, \mathbf{Y}, \mathbf{U}, \mathbf{V}) &= \left({}^{\mathbf{U}}\mathbf{W}\right)^{\mathbf{Y}}, \\ \mathbf{C}_2(\mathbf{X}, \mathbf{Y}, \mathbf{U}, \mathbf{V}) &= \left({}^{\mathbf{X}}\mathbf{W}\right)^{\mathbf{V}}. \end{aligned} \tag{18}$$

Note that this system is symmetric, i.e., by switching the pairs $(\mathbf{X}, \mathbf{Y})$ and $(\mathbf{U}, \mathbf{V})$, we obtain the following result:

$$\begin{aligned} \mathbf{A}(\mathbf{U}, \mathbf{V}, \mathbf{X}, \mathbf{Y}) &= \mathbf{C}_0(\mathbf{X}, \mathbf{Y}, \mathbf{U}, \mathbf{V}), \\ \mathbf{C}_0(\mathbf{U}, \mathbf{V}, \mathbf{X}, \mathbf{Y}) &= \mathbf{A}(\mathbf{X}, \mathbf{Y}, \mathbf{U}, \mathbf{V}), \\ \mathbf{C}_1(\mathbf{U}, \mathbf{V}, \mathbf{X}, \mathbf{Y}) &= \mathbf{C}_2(\mathbf{X}, \mathbf{Y}, \mathbf{U}, \mathbf{V}), \\ \mathbf{C}_2(\mathbf{U}, \mathbf{V}, \mathbf{X}, \mathbf{Y}) &= \mathbf{C}_1(\mathbf{X}, \mathbf{Y}, \mathbf{U}, \mathbf{V}). \end{aligned}$$

Due to this symmetry, Lemma 1 also works in the reverse direction. Hence, we have:

Lemma 2. *Assume that the pair of matrices* $(\mathbf{U}, \mathbf{V})$ *such that* $\mathbf{U} \in Sp(\mathbf{L})$ *and* $\mathbf{V} \in Sp(\mathbf{R})$ *is fixed and the Heuristic 1 holds. Then there is a unique pair* $(\mathbf{X}, \mathbf{Y})$ *such that* $\mathbf{X} \in Sp(\mathbf{L})$ *and* $\mathbf{Y} \in Sp(\mathbf{R})$*, which corresponds to the fixed commitment vector* $\vec{\mathbf{C}}$*, where* $\mathbf{C}_0 = \left({}^{\mathbf{U}}\mathbf{W}\right)^{\mathbf{V}}$*, and a fixed public key* $\mathbf{A}$*.*

The proof of this lemma is similar to the one presented above. Evidently, we only consider such fixed matrices in Lemmas 1 and 2, where at least one set $(\mathbf{X}, \mathbf{Y}, \mathbf{U}, \mathbf{V})$ satisfying all four relations exists in the first place.

These lemmas establish a one-to-one link between the private key and matrices $(\mathbf{U}, \mathbf{V})$ provided that four relations (18) are fixed. This link can be summarized by the following corollary of Lemmas 1 and 2:

Corollary 1. *Let the commitment vector* $\vec{\mathbf{C}}$ *and safe public key* $\mathbf{A}$ *be fixed. Assume also that Heuristic 1 holds. Then the number of pairs* $(\mathbf{U}, \mathbf{V})$ *resulting in the commitment* $\vec{\mathbf{C}}$ *is equal to the number of solutions of the Equation* (11)*.*

Relying on the latter corollary and our assumption regarding the solutions of (11), we can see that there are exactly four quadruples $(\mathbf{X}, \mathbf{Y}, \mathbf{U}, \mathbf{V})$ that give us the same values of $\mathbf{A}$ and all $\mathbf{C}_i$s.

Before we consider the property of knowledge soundness, let us denote the binary matrices obtained by reducing all the power matrices modulo 2 by a lower index $\oplus$, i.e., $\mathbf{X}_{\oplus} \equiv \mathbf{X} \bmod 2$, etc. Note that this affects the template (8) so that the matrix $\mathbf{R}_{\oplus}$ contains a c-th row of zeros. Additionally, for simplicity, we assume that the initial matrices $\mathbf{L}$ and $\mathbf{R}$ are contained in the representations of $\mathbf{L}^m$ and $\mathbf{R}^m$ with odd coefficients, i.e.,

$$\mathbf{L}^m = \sum_{i=1}^{m-1} l_i \mathbf{L}^i; \tag{19}$$

$$\mathbf{R}^m = \sum_{i=1}^{m-1} r_i \mathbf{R}^i, \tag{20}$$

where l_1 and r_1 are odd.

We now prove the following result:

Theorem 2. *Assume we have two accepting conversations* $(\vec{\mathbf{C}}, \vec{\mathbf{H}}, \vec{\mathbf{S}})$ *and* $(\vec{\mathbf{C}}, \vec{\mathbf{H}}', \vec{\mathbf{S}}')$ *for the same public key* $\mathbf{A}$*. Assume also that Heuristic 1 holds. Then the witness* $(\mathbf{X}, \mathbf{Y})$ *can be extracted with probability* $1 - 2^{2-m} + 2^{-2(m-1)}$.

Proof. Due to Lemma 1, matrices $\mathbf{U}$ and $\mathbf{V}$ are unique, and hence, we can perform the following calculations:

$$\mathbf{S}_1 - \mathbf{S}'_1 = (\mathbf{U} + \mathbf{H}_1\mathbf{X}) - (\mathbf{U} + \mathbf{H}'_1 X) = (\mathbf{H}_1 - \mathbf{H}'_1)\mathbf{X};$$
$$\mathbf{S}_2 - \mathbf{S}'_2 = (\mathbf{V} + \mathbf{Y}\mathbf{H}_2) - (\mathbf{V} + Y\mathbf{H}'_2) = \mathbf{Y}(\mathbf{H}_2 - \mathbf{H}'_2).$$

Denoting $\Delta\mathbf{S}_1 = \mathbf{S}_1 - \mathbf{S}'_1$, $\Delta\mathbf{S}_2 = \mathbf{S}_2 - \mathbf{S}'_2$, $\Delta\mathbf{H}_1 = \mathbf{H}_1 - \mathbf{H}'_1$, $\Delta\mathbf{H}_2 = \mathbf{H}_2 - \mathbf{H}'_2$, we obtain the following matrix equations defined over the ring $\mathbb{Z}_8$:

$$\Delta\mathbf{S}_1 = \Delta\mathbf{H}_1\mathbf{X}; \quad \Delta\mathbf{S}_2 = \mathbf{Y}\Delta\mathbf{H}_2. \tag{21}$$

However, all the matrices in the presented equations are contained in the appropriate linear spans $Sp(\mathbf{L})$ or $Sp(\mathbf{R})$. Hence, they can be expressed as linear combinations of the public matrices $\mathbf{L}$ of $\mathbf{R}$. Let us first focus on the right-hand sides of Equation (21). We have:

$$\Delta\mathbf{S}_1 = \Big(\sum_{i=1}^{m-1} \Delta h_{1i}\mathbf{L}^i\Big) \cdot \Big(\sum_{i=1}^{m-1} x_i\mathbf{L}^i\Big); \quad \Delta\mathbf{S}_2 = \Big(\sum_{i=1}^{m-1} y_i\mathbf{R}^i\Big) \cdot \Big(\sum_{i=1}^{m-1} \Delta h_{2i}\mathbf{R}^i\Big), \tag{22}$$

where $\Delta h_{1i} = h_{1i} - h'_{1i}$ and $\Delta h_{2i} = h_{2i} - h'_{2i}$ are coefficients of the polynomial representations of matrices $\Delta\mathbf{H}_1$ and $\mathbf{H}_2$, respectively. Evidently, $h_{1i}, h'_{1i}, h_{2i}, h'_{2i}$ are coefficients of polynomial representations of matrices $\mathbf{H}_1, \mathbf{H}'_1, \mathbf{H}_2, \mathbf{H}'_2$, respectively. Expanding the obtained expressions, we get the following double sums:

$$\Delta\mathbf{S}_1 = \sum_{i=1}^{m-1}\sum_{j=1}^{m-1} \Delta h_{1i}x_j\mathbf{L}^{i+j}; \quad \Delta\mathbf{S}_2 = \sum_{i=1}^{m-1}\sum_{j=1}^{m-1} \Delta h_{2i}y_j\mathbf{R}^{i+j}. \tag{23}$$

We can now collect like terms and obtain the $(2m-2) \times (m-1)$ temporary matrix of coefficients, where the i-th row corresponds to the coefficient of $\mathbf{L}^i$ (or $\mathbf{R}$) and the j-th column corresponds to the coefficient of x_j (or y_j). For simplicity, we consider only the first double sum. Denoting this temporary matrix by $\mathbf{T}$, we have:

$$\mathbf{T} = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ \Delta h_{11} & 0 & 0 & \cdots & 0 & 0 & 0 \\ \Delta h_{12} & \Delta h_{11} & 0 & \cdots & 0 & 0 & 0 \\ \Delta h_{13} & \Delta h_{12} & \Delta h_{11} & \cdots & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \Delta h_{1(m-1)} & \Delta h_{1(m-2)} & \Delta h_{1(m-3)} & \cdots & \Delta h_{13} & \Delta h_{12} & \Delta h_{11} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & \Delta h_{1(m-1)} & \Delta h_{1(m-2)} & \Delta h_{1(m-3)} \\ 0 & 0 & 0 & \cdots & 0 & \Delta h_{1(m-1)} & \Delta h_{1(m-2)} \\ 0 & 0 & 0 & \cdots & 0 & 0 & \Delta h_{1(m-1)} \end{pmatrix} \tag{24}$$

The key moment in this proof is the rank of matrix $\mathbf{T}$. It is important to note that if at least one of $\Delta h_{1i} \not\equiv 0 \bmod 2$, then the rank of binary matrix $\mathbf{T}_{\oplus}$ is equal to $(m-1)$, i.e., $\mathbf{T}_{\oplus}$ is a full rank matrix.

However, since the basis of the linear span $Sp(\mathbf{L})$ consists of the first $(m-1)$ powers of matrix $\mathbf{L}$, then each subsequent power of $\mathbf{L}$ can be represented by a linear combination of the basis matrices. Then, we can use row additions to transform the temporary matrix $\mathbf{T}_{\oplus}$ to obtain a square matrix of coefficients $\hat{\mathbf{T}}_{\oplus}$ for the following system of linear equations:

$$\vec{\mathbf{\Delta s}}_{\mathbf{1}\oplus} = \hat{\mathbf{T}}_{\oplus}\vec{\mathbf{x}}_{\oplus},$$

where $\hat{\mathbf{T}}_{\oplus}$ consists of the first $(m-1)$ rows of the transformed matrix $\mathbf{T}_{\oplus}$. Then, due to assumption (19), $\hat{\mathbf{T}}_{\oplus}$ is a full rank matrix, and hence, $\hat{\mathbf{T}}$ is a full rank matrix as well. For this reason, both equation in (21) can be solved in polynomial time, and the witness $(\mathbf{X}, \mathbf{Y})$ can be restored.

Lastly, we note that if $\Delta h_{1i} \equiv 0 \bmod 2$ or $\Delta h_{2i} \equiv 0 \bmod 2$ for all $i = 1, 2, \ldots, m-1$, then $\mathbf{T}_{\oplus}$ is a zero matrix, and hence, the witness $(\mathbf{X}, \mathbf{Y})$ cannot be restored. The probability of this happening is 2^{1-m} for each matrix $\Delta\mathbf{H}_1$ and $\Delta\mathbf{H}_2$. It is now easy to show using basic laws that the probability of successful restoration is $1 - 2^{2-m} + 2^{-2(m-1)}$. □

For the reader to better understand the essential moment of the latter proof, let us consider a toy example.

Example 1. *Let us assume that $m = 4$. Furthermore, let public matrix $\mathbf{L}$ be chosen such that $\mathbf{L}^4_{\oplus} = \mathbf{L}_{\oplus} + \mathbf{L}^2_{\oplus}$. Then, the temporary matrix $\mathbf{T}$ for restoring $\mathbf{X}$ is:*

$$\mathbf{T} = \begin{pmatrix} 0 & 0 & 0 \\ \Delta h_{11} & 0 & 0 \\ \Delta h_{12} & \Delta h_{11} & 0 \\ \Delta h_{13} & \Delta h_{12} & \Delta h_{11} \\ 0 & \Delta h_{13} & \Delta h_{12} \\ 0 & 0 & \Delta h_{13} \end{pmatrix}.$$

Limiting ourselves to the binary matrix $\mathbf{T}_{\oplus}$ to suppress coefficients and observing that:

$$\mathbf{L}^5_{\oplus} = \mathbf{L}^2_{\oplus} + \mathbf{L}^3_{\oplus},$$
$$\mathbf{L}^6_{\oplus} = \mathbf{L}^3_{\oplus} + \mathbf{L}^4_{\oplus} = \mathbf{L}^3_{\oplus} + \mathbf{L}_{\oplus} + \mathbf{L}^2_{\oplus}$$

we can perform the following transformations of the matrix $\mathbf{T}_{\oplus}$*:*

$$\mathbf{T}_{\oplus} = \begin{pmatrix} 0 & 0 & 0 \\ \Delta h_{11} & 0 & 0 \\ \Delta h_{12} & \Delta h_{11} & 0 \\ \Delta h_{13} & \Delta h_{12} & \Delta h_{11} \\ 0 & \Delta h_{13} & \Delta h_{12} \\ 0 & 0 & \Delta h_{13} \end{pmatrix} \sim \begin{pmatrix} \Delta h_{13} & \Delta h_{12} & \Delta h_{11} \\ \Delta h_{11} + \Delta h_{13} & \Delta h_{12} & \Delta h_{11} \\ \Delta h_{12} & \Delta h_{11} & 0 \\ \Delta h_{13} & \Delta h_{12} & \Delta h_{11} \\ 0 & \Delta h_{13} & \Delta h_{12} \\ 0 & 0 & \Delta h_{13} \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} \Delta h_{13} & \Delta h_{12} & \Delta h_{11} \\ \Delta h_{11} + \Delta h_{13} & \Delta h_{12} + \Delta h_{13} & \Delta h_{11} + \Delta h_{12} \\ \Delta h_{12} & \Delta h_{11} + \Delta h_{13} & \Delta h_{12} \\ \Delta h_{13} & \Delta h_{12} & \Delta h_{11} \\ 0 & \Delta h_{13} & \Delta h_{12} \\ 0 & 0 & \Delta h_{13} \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} \Delta h_{13} & \Delta h_{12} & \Delta h_{11} + \Delta h_{13} \\ \Delta h_{11} + \Delta h_{13} & \Delta h_{12} + \Delta h_{13} & \Delta h_{11} + \Delta h_{12} + \Delta h_{13} \\ \Delta h_{12} & \Delta h_{11} + \Delta h_{13} & \Delta h_{12} + \Delta h_{13} \\ \Delta h_{13} & \Delta h_{12} & \Delta h_{11} \\ 0 & \Delta h_{13} & \Delta h_{12} \\ 0 & 0 & \Delta h_{13} \end{pmatrix}.$$

Hence, the binary matrix $\hat{\mathbf{T}}_{\oplus}$ *has the following form:*

$$\hat{\mathbf{T}}_{\oplus} = \begin{pmatrix} \Delta h_{13} & \Delta h_{12} & \Delta h_{11} + \Delta h_{13} \\ \Delta h_{11} + \Delta h_{13} & \Delta h_{12} + \Delta h_{13} & \Delta h_{11} + \Delta h_{12} + \Delta h_{13} \\ \Delta h_{12} & \Delta h_{11} + \Delta h_{13} & \Delta h_{12} + \Delta h_{13} \end{pmatrix}.$$

The matrix $\hat{\mathbf{T}}$ *has a similar structure. The only difference is that extra coefficients from elementary row operations may appear.*

Despite the fact that the obtained result is weaker than the original definition of knowledge soundness, we view it as a good alternative since the probability of success tends to 100% remarkably fast. Specifically, if $m = 6$, it surpasses 90%, and for $m = 16$, it approximately equals 99.99%. Moreover, even if, say, $\Delta h_{1i} = 2\Delta\hat{h}_{1i}$, the hopes of restoring a witness are not completely lost since the following cancellation is possible:

$$2\Delta\hat{\mathbf{S}}_1 \equiv 2\Delta\hat{\mathbf{H}}_1\mathbf{X} \bmod 8 \Rightarrow \Delta\hat{\mathbf{S}}_1 \equiv \Delta\hat{\mathbf{H}}_1\mathbf{X} \bmod 4,$$

and one can hopefully restore the matrix $\mathbf{X}$ modulo 4. However, to restore the original matrix in this case, the witness extractor needs to browse through a set of possible values of $\vec{\mathbf{x}}$ until one finds the correct value of $\mathbf{X}$. This comes from the fact that the solution of (21) is not unique. In fact, the parity-defining bits of $\vec{\mathbf{x}}$ are lost, and the witness extractor needs more time to restore them. As such, the witness extractor becomes inefficient. For the sake of the original notion, we based our proof on the assumption that the witness extractor is efficient.

Now we consider the resistance of our sigma identification protocol against eavesdropping and active attacks. Our proofs are inspired by the approach presented in [1], which relies on the notions of special HVZK and knowledge soundness. Specifically, we consider Attack Games 18.1–18.3 and Theorems 19.15 and 19.22.

Theorem 3. *MPF-based SIP presented above is secure against eavesdropping attacks.*

Proof. Let $\mathcal{A}$ be an eavesdropping attacker. He can request a maximum of $8^{2(m-1)}$ conversations between the Prover and the Verifier. This number comes from counting all the possible pairs of matrices $(\mathbf{U}, \mathbf{V})$. Then, due to Lemma 1, all the commitments are distinct, and the identity of the legit user cannot be obtained, as shown in the proof of Theorem 2. Moreover, since the proposed SIP is a special HVZK, the received queries have identical distributions, i.e., they are all equally likely. Hence, to impersonate another user, the adversary has to find a solution to Equation (11) under the setup presented in this paper. However, this is an NP-complete problem, as shown in our previous paper [7]. Furthermore, based on Theorem 19.15 and Attack Games 18.1 and 18.2 of [1], we can see that any adversary who can successfully impersonate a legit user can also efficiently perform a direct attack on our SIP. For these reasons, any impersonation attempts of $\mathcal{A}$ result in failure. □

As we have shown, the initial notion of knowledge soundness is not satisfied in our case. However, due to the negligibly small knowledge error, this fact does not affect the following result:

Theorem 4. *MPF-based SIP presented above is secure against active attacks.*

Proof. Let $\mathcal{A}$ be an active attacker whose goal is to impersonate a legal user by generating an accepting conversation without knowing the private key $\mathbf{PrK} = (\mathbf{X}, \mathbf{Y})$.

The adversary $\mathcal{A}$ interacts with a challenger, who plays the role of a Prover and sends his public key $\mathbf{A}$ defined by (11) to the adversary while keeping $\mathbf{PrK} = (\mathbf{X}, \mathbf{Y})$ for himself. An attacker $\mathcal{A}$ now plays the role of the Verifier and, hence, can generate challenge $\vec{\mathbf{H}}$ as he desires. However, due to the fact that $\mathcal{A}$ is not in control of the generation of $\mathbf{U}$ and $\mathbf{V}$, he fails to gain any information from this active probing phase due to Theorem 1. Note that since the attacker $\mathcal{A}$ can choose $\vec{\mathbf{H}}$ at his will, he can control knowledge soundness and hence make the private key of the challenger unrestorable, as mentioned in our previous proof. However, this is not his goal, since he was only able to hide the challenger's ID rather than learning how to impersonate him. Notably, $\mathcal{A}$ can interact with more than one challenger at this stage.

After the active probing phase, the challenger and the attacker switch places: now the challenger is the Verifier, whereas the attacker plays the role of the Prover, except for the lack of a private key $\mathbf{PrK}$. However, due to the one-wayness of MPF mapping, the adversary $\mathcal{A}$ cannot recover $\mathbf{PrK}$ from the public key $\mathbf{A}$. For this reason, he cannot generate a working conversation, since by using a random pair of matrices $\hat{\mathbf{X}}$ and $\hat{\mathbf{Y}}$, the protocol falls apart during the verification phase, i.e., checking the validity of (15).

Another important fact is that the Verifier is now in control of challenges $\vec{\mathbf{H}}$. Due to the presented probability of success, an honest Verifier can generate the challenge simply by picking the coefficients h_{1i} and h_{2i} at random. By doing so, he is almost always able to identify a suspicious user should the need arise.

In other words, if $\mathcal{A}$ is able to impersonate a legit user, then he is able to solve an NP-complete problem, as proven in [7]. Moreover, if $\mathcal{A}$ uses his own private and public keys, the challenger is able to identify him with probability $1 - 2^{2-m} + 2^{-2(m-1)}$. □

To sum up the findings presented in this section, our proposal can withstand both eavesdropping and active attacks. Moreover, due to negligibly small knowledge error, our protocol does not require a large number of parallel rounds to achieve a NIST security level, as opposed to Shamir's approach presented in [6].

5. Conclusions

In this paper, we proposed a SIP based on the MPF defined over a non-commuting modular group $\mathtt{M}_{16}$. Due to the fact that this group is not decomposable into a product of cyclic low-order groups, discrete logarithm mapping cannot be defined. For this reason, the proposed SIP is resistant to the linear algebra attack presented in [12].

Since the platform group $\mathtt{M}_{16}$ is non-commuting, MPF mapping is non-associative in general. To overcome this fact, we used templates previously defined in [8]. Furthermore, due to the main result of [7], we think that the proposed SIP could belong to the post-quantum cryptography field, since the MPF problem with precisely the setup presented in this paper was proven to be NP-complete.

Using properties of one-sided MPFs, we have shown that the presented protocol is special HVZK, and therefore, according to the assumption that the proposed MPF is conjectured one-way function, this protocol is resistant against eavesdropping adversary attacks [1].

Despite the fact that the multiplicative order of $\mathtt{M}_{16}$ is not a prime number, we have shown that our protocol provides asymptotic knowledge soundness. In other words, the recovery of private key **PrK** of a suspicious user is possible with overwhelming probability if two accepting conversations with identical commitment vectors $\vec{\mathbf{C}}$ are known. In fact, the growth of this probability is exponential as the order of the square matrices m increases. As such, we can view m as the security parameter. Notably, if $m = 16$, then the identity of a suspicious user can be recovered with a probability of 99.99%.

Relying on the proven properties of our SIP and the attack games presented in [1], we proved that the proposed protocol is asymptotically secure against active adversary attacks.

Author Contributions: Conceptualization, A.M. and E.S.; methodology, A.M.; software, A.M.; validation, A.M., K.L. and E.S.; formal analysis, A.M.; investigation, A.M. and K.L.; writing—original draft preparation, A.M.; writing—review and editing, A.M.; visualization, A.M.; supervision, E.S.; project administration, K.L.; funding acquisition, K.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: This article does not contain any studies with human participants or animals performed by any of the authors.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Boneh, D.; Shoup, V. A Graduate Course in Applied Cryptography. Version 0.5. 2020. Available online: http://toc.cryptobook.us/book.pdf (accessed on 14 April 2022).
2. Schnorr, C.P. Efficient Signature Generation by Smart Cards. *J. Cryptol.* **1991**, *4*, 161–174. [CrossRef]
3. Okamoto, T. Authenticated Key Exchange and Key Encapsulation in the Standard Model. In *Advances in Cryptology, Proceesings of the ASIACRYPT 2007, Kuching, Sarawak, Malaysia, 2–6 December 2007*; Kurosawa, K., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2007; Volume 4833, pp. 474–484. ISBN 978-3-540-76899-9.
4. Chaum, D.; Pedersen, T.P. Wallet Databases with Observers. In *Advances in Cryptology—CRYPTO' 92, Proceesings of the 12th Annual International Cryptology Conference, Santa Barbara, CA, USA, 16–20 August 1992*; Brickell, E.F., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1993; Volume 740, pp. 89–105. ISBN 978-3-540-57340-1.
5. Beullens, W. Sigma Protocols for MQ, PKP and SIS, and Fishy Signature Schemes. In *Advances in Cryptology—EUROCRYPT 2020, Proceesings of the 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, 10–14 May 2020*; Canteaut, A., Ishai, Y., Eds.; Lecture Notes in Computer Science; Springer International Publishing: Cham, Germany, 2020; Volume 12107, pp. 183–211. ISBN 978-3-030-45726-6.
6. Shamir, A. An Efficient Identification Scheme Based on Permuted Kernels (Extended Abstract). In *Advances in Cryptology—CRYPTO' 89 Proceedings, Proceedings of the 9th Annual International Cryptology Conference, Santa Barbara, CA, USA, 20–24 August 1989*; Brassard, G., Ed.; Lecture Notes in Computer Science; Springer: New York, NY, USA, 1990; Volume 435, pp. 606–609. ISBN 978-0-387-97317-3.
7. 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]
8. Mihalkovich, A.; Sakalauskas, E.; Levinskas, M. Key Exchange Protocol Based on the Matrix Power Function Defined Over $\mathtt{M}_{16}$. In Proceedings of the Intelligent Computing, London, UK, 14–15 July 2022; Arai, K., Ed.; Springer International Publishing: Cham, Germany, 2022; pp. 511–531.

9. Sakalauskas, E.; Timofejeva, I.; Kilciauskas, A. Sigma Identification Protocol Construction Based on MPF. *Symmetry* **2021**, *13*, 1683. [CrossRef]
10. Sakalauskas, E.; Luksys, K. The Matrix Power Function and Its Application to Block Cipher S-Box Construction. *Int. J. Innov. Comput. Inf. Control.* **2012**, *8*, 2655–2664.
11. Sakalauskas, E.; Mihalkovich, A. Candidate One-Way Function Based on Matrix Power Function with Conjugation Constraints. *Proc. Bulg. Cryptogr. Days* **2012**, *15*, 29–37.
12. 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 Information Security and Cryptology, Beijing, China, 4–6 November 2016; Chen, K., Lin, D., Yung, M., Eds.; Springer International Publishing: Cham, Germany, 2017; pp. 343–354.
13. Sakalauskas, E.; Listopadskis, N.; Tvarijonas, P. Key Agreement Protocol (KAP) Based on Matrix Power Function. In *Advanced Studies in Software and Knowledge Engineering*; International Book Series "Information Science and Computing"; Institute of Information Theories and Applications FOI ITHEA: Sofia, Bulgaria, 2018; pp. 92–96.
14. Mihalkovič, A.; Sakalauskas, E. Asymmetric Cipher Based on MPF and Its Security Parameters Evaluation. *Liet. Mat. Rink.* **2012**, *53*, 72–77. [CrossRef]
15. Grundman, H.; Smith, T. Automatic Realizability of Galois Groups of Order 16. *Proc. Am. Math. Soc.* **1996**, *124*, 2631–2640. [CrossRef]
16. Grundman, H.G.; Smith, T.L. Realizability and Automatic Realizability of Galois Groups of Order 32. *Centr. Eur. J. Math.* **2010**, *8*, 244–260. [CrossRef]
17. Grundman, H.G.; Smith, T.L. Galois Realizability of Groups of Order 64. *Centr. Eur. J. Math.* **2010**, *8*, 846–854. [CrossRef]
18. Mihalkovich, A. On the Associativity Property of MPF over M16. *Liet. Mat. Rink. Liet. Mat. Draugijos Darbai. Ser. A* **2018**, *59*, 7–12. [CrossRef]