On the decisional problem based on matrix power function defined over non-commutative group

Aleksejus Mihalkovich[1], Jokubas Zitkevicius[2]
Department of Applied Mathematics, Kaunas University of Technology, Kaunas, Lithuania
[1]Corresponding author
E-mail: [1]*aleksejus.michalkovic@ktu.lt*, [2]*jokubas.zitkevicius@ktu.edu*

Received 11 March 2024; accepted 11 April 2024; published online 9 May 2024
DOI https://doi.org/10.21595/mme.2024.24071

Abstract. In this paper, we perform statistical analysis for the decisional problem which is fundamental for the security of the key exchange protocol based on matrix power function. We have proven previously that the considered decisional problem is NP-complete and hence our proposal could potentially be quantum-safe. However, we did not explore the dependence of the complexity of the considered problem on the security parameters. Here we show that for small matrices certain information could be gained from the distribution of the entries of the public key matrices. On the other hand, we show that as the size of the matrices grows, the public key matrices are indistinguishable from truly random matrices.

Keywords: non-commuting cryptography, statistical cryptanalysis, uniform distribution.

1. Introduction

A novel idea presented by W. Diffie and M. Hellman in [1] of using a pair of keys to agree on a shared secret gave birth to the branch of public-key cryptography. Since then, much research has been performed in this field and widely known cryptosystems such as RSA and many others were proposed. However, these cryptosystems mostly relied on the security of the discrete logarithm problem (DLP) defined in some multiplicative group (a version of DLP for additive groups e.g. elliptic curves can also be defined) or integer factorization problem [2]. While these problems do provide a decent challenge, due to the findings published by P. Shorr in [3] these problems could be solved by quantum computers.

For some time, quantum computers were viewed as a mostly theoretical threat. However, due to the rapid development of quantum technologies, by the mid-2010s quantum cryptanalysis could no longer be viewed as purely theoretic. In 2016 the National Institute of Standards and Technology (NIST) announced a call for post-quantum algorithms for standardization [4]. As of now the finalists of round 3 have been announced [5]. Furthermore, the development of quantum-safe cryptographic schemes continues due to the increasing practical demand of such algorithms in the near future.

The proposed cryptographic schemes rely on hard problems e.g. defined in lattices or using multivariate quadratic equations. Alternatively error correction codes, hash-based cryptography or elliptic curves isogenies could be used to construct quantum-safe algorithms [6,7]. The security of such algorithms relies on NP-hard computational problems, i.e. they are in the hardest class of problems which cannot be solved by a deterministic Turing machine in polynomial time. Moreover, decisional versions of some of these problems are known to be NP-complete, e.g. closest vector problem used in lattice-based cryptography [8]. It is widely believed that such problems can withstand quantum cryptanalysis.

In this paper, we consider one of such problems which is fundamental for the security of the cryptographic protocols presented in [9] and [10]. The objective of this problem is to recover the secret key of the legitimate user based on his public key [9]. Our goal is to show that the produced key is statistically indistinguishable from a truly random matrix if the public parameters of the protocol are appropriately chosen. We think that our results pose an interest from the practical

implementation point of view, since the choice of the security parameters influences the memory requirements to store the private and public data and hence can be fundamental to determining if our proposal can be implemented in memory-restricted devices.

The rest of this paper is organized as follows: in Section 2 we revise the mathematical background of our research; in Section 3 we define the considered problem in the form of the security game and present the main results of this paper. As usual, conclusions are presented at the end of the paper.

2. Mathematical background

Our approach is related to multivariate cryptography. Specifically, we focus on a certain mapping called the matrix power function (MPF) first introduced in [11]. The idea of this mapping is somewhat similar to the classical matrix multiplication. However, since MPF is defined for matrices with entries chosen from multiplicative (semi)group $\mathbb{S}$, we use multiplication as the operation in $\mathbb{S}$ and exponentiation as the scalar multiplication. Hence, we obtain the following expressions defining the one-sided MPFs [11]:

$$^{\mathbf{X}}\mathbf{W} = \mathbf{A}, \qquad a_{ij} = \prod_{k=1}^{m} \left(w_{kj}\right)^{x_{ik}}, \tag{1}$$

$$\mathbf{W}^{\mathbf{Y}} = \mathbf{B}, \qquad b_{ij} = \prod_{k=1}^{m} \left(w_{ik}\right)^{x_{kj}}. \tag{2}$$

The matrix $\mathbf{W}$ in Eq. (1) and Eq. (2) is called the *base matrix* with its entries chosen from the multiplicative (semi)group $\mathbb{S}$. We refer to $\mathbb{S}$ as the *platform (semi)group*. The matrices $\mathbf{X}$ and $\mathbf{Y}$ in Eq. (1) and Eq. (2) respectively are referred to as *power matrices*. Their entries are chosen from a ring of scalars $\mathbb{Z}_{ord(\mathbb{S})}$, where $ord(\mathbb{S})$ denotes the multiplicative order of $\mathbb{S}$, i.e. the smallest natural number satisfying the relation $w^{ord(\mathbb{S})} = e$ for any $w \in \mathbb{S}$, and e is the identity of $\mathbb{S}$.

In our early research related to MPF we considered various commuting platform groups [12–14]. It was shown in [12] that is this case MPF is associative, i.e. the following identity holds:

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

Hence, we obtain the definition of the two-sided MPF. Unfortunately, our early proposals presented in [12] and [14] were attacked in [15] using tools of linear algebra together with discrete logarithm mapping. Though we fixed the flaw in our paper [16], and investigated this enhanced version in [17], partly due to the presented attack, our attention turned to non-commuting platform groups, where Eq. (3) does not hold in general, and hence the order of actions must be taken into consideration. In [9] and [18] we have shown that we can define hard decisional problems based on MPF defined over non-commuting platform groups thus demonstrating that MPF is a possible candidate for the so-called one-way function – easy to calculate, hard to invert.

In this paper, we consider a family of the so-called modular-maximal cyclic groups generally denoted by $\mathbb{M}_{2^t}$ and defined as follows [19-21]:

$$\mathbb{M}_{2^t} = \langle a, b | a^{2^{t-1}} = e, b^2 = e, bab^{-1} = a^{2^{t-2}+1} \rangle, \tag{4}$$

where a and b are two non-commuting generators of the group and e is the identity of the group. Note that the parameter t defines the size of $\mathbb{M}_{2^t}$, i.e. $|\mathbb{M}_{2^t}| = 2^t$, and hence we refer to it as the group-defining parameter. All the elements of $\mathbb{M}_{2^t}$ can be represented in two ways: either $a^{\alpha}b^{\beta}$ or $b^{\beta}a^{\alpha}$, where $\alpha \in \mathbb{Z}_{2^{t-1}}$ and $\beta \in \mathbb{Z}_2$. Since both these representations are equivalent, in this paper, we use the representation $a^{\alpha}b^{\beta}$ for the elements of $\mathbb{M}_{2^t}$.

Basic operations in this group are presented below [9].

Multiplication of two elements:

$$\left(a^{\alpha_1}b^{\beta_1}\right)\cdot\left(a^{\alpha_2}b^{\beta_2}\right)=\begin{cases}a^{\alpha_1+\alpha_2}b^{\beta_2}, & \beta_1=0,\\ a^{\alpha_1+\alpha_2}b^{1+\beta_2}, & \beta_1=1,\quad \alpha_2 \text{ is even},\\ a^{\alpha_1+\alpha_2+2^{t-2}}b^{1+\beta_2}, & \beta_1=1,\quad \alpha_2 \text{ is odd}.\end{cases} \tag{5}$$

Exponentiation to the power k:

$$\left(a^{\alpha}b^{\beta}\right)^{k}=\begin{cases}a^{k\alpha}, & \beta=0,\\ a^{k\alpha}b^{k}, & \beta=1,\quad \alpha_2 \text{ is even},\\ a^{k\alpha+2^{t-2}\left\lfloor\frac{k}{2}\right\rfloor}b^{1+\beta_2}, & \beta=1,\quad \alpha_2 \text{ is odd}.\end{cases} \tag{6}$$

An important corollary of these expressions is the fact that there are two cyclic subgroups of $\mathbb{M}_{2^t}$ of size 2^{t-1}. These subgroups are generated by elements a and ab. We denote them by $\langle a\rangle$ and $\langle ab\rangle$ respectively. Their explicit presentations are given below:

$$\langle a\rangle=\left\{e,a,a^2,\dots,a^{2^{t-1}-1}\right\}, \tag{7}$$

$$\langle ab\rangle=\left\{e,ab,a^2,a^3b,\dots,a^{2^{t-1}-1}b\right\}. \tag{8}$$

It is important to note that in general elements from $\langle a\rangle$ and $\langle ab\rangle$ do not commute. This fact plays a major role in the application of $\mathbb{M}_{2^t}$ in our research. Specifically, we defined the form of the base matrix **W** as well as the forms of the secret key matrices.

Template 1. The base matrix **W** is chosen randomly to fit the following form [9]:

$$\mathbf{W}=\begin{pmatrix}a^{2k_{11}+1}b & a^{k_{12}} & \dots & a^{2k_{c1}+l_{c1}}b^{l_{c1}} & \dots & a^{k_{1(m-1)}} & a^{2k_{1m}+1}b\\ a^{2k_{21}} & a^{k_{22}} & \dots & a^{2k_{c2}+l_{c2}}b^{l_{c2}} & \dots & a^{k_{2(m-1)}} & a^{2k_{2m}}\\ \dots & \dots & \dots & \dots & \dots & \dots & \dots\\ a^{2k_{m1}+1}b & a^{k_{m2}} & \dots & a^{2k_{cm}+l_{cm}}b^{l_{cm}} & \dots & a^{k_{m(m-1)}} & a^{2k_{mm}+1}b\end{pmatrix}. \tag{9}$$

The main idea behind this template is to choose the entries of the columns in such a way that in each of the individual column entries are in the same cyclic subgroup either $\langle a\rangle$ or $\langle ab\rangle$. This way we ensure that each individual column contains commuting entries. However, we still have to make sure that the exponentiation from the right is also performed with commuting entries. To achieve this goal, we define the following templates for power matrices [9]:

Template 2. The left power matrix **X** is chosen at random to satisfy the following condition:

$$x_{i1}+x_{im}\equiv 0 \bmod 2. \tag{10}$$

Template 3. The right power matrix **Y** is chosen at random to satisfy the following condition:

$$y_{cj}\equiv 0 \bmod 2. \tag{11}$$

Previously in [9] we proposed a key exchange protocol where we used $\mathbb{M}_{2^t}$ as a platform group for the MPF with similar templates for matrices. Also, using the ideas presented in that paper we proposed a sigma identification protocol in [10]. Here we focus on these ideas presented in a more general way, i.e. we consider the MPF with additional constraints given by the Templates 1, 2 and 3 defined above to keep the results obtained here applicable for future research in this area.

3. Decisional problem based on MPF

In this section we consider the following security game aimed at distinguishing an MPF value from a truly random matrix:

Security Game. Let $\mathbf{W}$ be a matrix satisfying Template 1. For a given adversary $\mathcal{A}$ and its challenger $\mathcal{C}$ we define the following game:

1) $\mathcal{C}$ chooses at random two matrices $\mathbf{X}$ and $\mathbf{Y}$ satisfying Templates 2 and 3 respectively and computes $\mathbf{K}_0 = ({}^{\mathbf{X}}\mathbf{W})^{\mathbf{Y}}$.

2) $\mathcal{C}$ generates a random matrix $\mathbf{K}_1$ with entries $(k_1)_{ij} \in \mathbb{Z}_{2^{t-1}}$.

3) $\mathcal{C}$ gives the pair $(\mathbf{W}, \mathbf{K}_\beta)$, where $\beta \in \{0,1\}$ to $\mathcal{A}$.

4) $\mathcal{A}$ outputs $\hat{\beta}$.

The adversary $\mathcal{A}$ wins the game if $\hat{\beta} = \beta$.

To put it simpler, the aim of the game is to answer YES/NO to the following question: is there a pair of matrices $(\mathbf{X}, \mathbf{Y})$ satisfying Templates 2 and 3 respectively, such that $\mathbf{K}_\beta = ({}^{\mathbf{X}}\mathbf{W})^{\mathbf{Y}}$. Hence, we obtain a decisional problem based on MPF defined over a non-commutative platform group. Here we refer to this problem as *MPF decisional problem.*

Previously in [9] we used Schaefer's dichotomy theorem to show that a special case of this problem when matrices $\mathbf{X}$ and $\mathbf{Y}$ are generated as polynomials of pre-fixed matrices $\mathbf{L}$ and $\mathbf{R}$ with coefficients from $\mathbb{Z}_{2^{t-1}}$ is NP-complete. However, we did not explore the dependence of the complexity of this problem on the order of the matrices or the size of the platform group $\mathbb{M}_{2^t}$. Here we focus on these dependencies, i.e. we are interested in determining how difficult it is to solve the considered decisional problem for distinct values of the group size-defining parameter t and the matrix order m.

Our results are based on the statistical analysis of the distribution of the entries of the MPF value matrix $\mathbf{K}_0$. Our goal is to show that the entries of $\mathbf{K_0}$ are distributed uniformly in $\mathbb{Z}_{2^{t-1}}$ as a truly random matrix $\mathbf{K}_1$ has uniformly distributed entries.

The statistical analysis was performed as follows:

1) We generate a matrix $\mathbf{W}$ that satisfies Template 1.

2) We select a natural number k that defines the total number of iterations executed.

3) Within the l-th iteration, where $1 \le l \le k$, a new pair of matrices $(\mathbf{X}_l, \mathbf{Y}_l)$ is generated such that the matrix $\mathbf{X}_l$ satisfies Template 2 and the matrix $\mathbf{Y}_l$ satisfies Template 3. For each pair we calculate the matrix exponent $\mathbf{V}_l = ({}^{\mathbf{X}_l}\mathbf{W})^{\mathbf{Y}_l}$.

4) We store the frequencies of powers of the generator a two different ways: an array $\mathbf{q}$ stores the overall frequencies of powers, and a tensor $\mathbf{Q}$ keeps track of frequencies in each individual position in the matrix exponent, i.e. we obtain m^2 separate samples, where m is the size of the matrices. Denote by $f(z, \mathbf{V}_l)$ the frequency of the element a^z in the matrix exponent $\mathbf{V}_l$ and denote by $f_{ij}(z, \mathbf{V}_l)$ the frequency of the element a^z in the (i,j)-th position of matrix exponent $\mathbf{V}_l$. Then we have:

$$\mathbf{q} = \left(\sum_{l=1}^{k} f(0, \mathbf{V}_l) \quad \sum_{l=1}^{k} f(1, \mathbf{V}_l) \quad \dots \quad \sum_{l=1}^{k} f(2^{t-1}-1, \mathbf{V}_l) \right), \tag{12}$$

$$\mathbf{Q} = \begin{pmatrix} \mathbf{q}_{11} & \dots & \mathbf{q}_{1m} \\ \dots & \ddots & \dots \\ \mathbf{q}_{m1} & \dots & \mathbf{q}_{mm} \end{pmatrix}, \qquad \mathbf{q}_{ij} = \left(\sum_{l=1}^{k} f_{ij}(0, \mathbf{V}_l) \quad \dots \quad \sum_{l=1}^{k} f_{ij}(2^{t-1}-1, \mathbf{V}_l) \right). \tag{13}$$

5) After all k iterations have been executed, we perform Pierson chi-squared test for uniform distribution for $\mathbf{q}$ and each sample $\mathbf{q}_{ij} \in \mathbf{Q}$ separately at a 0.05 significance level and calculate p-value for all of the obtained values of the chi-squared statistics.

If the null hypothesis is rejected for the sample $\mathbf{q}$, then there may exist patterns in the structure of the key matrix $\mathbf{K}_0$ distinguishing it from a truly random matrix, i.e. some values of $\mathbf{K}_0$ might

be more likely than others. Hence an adversary has a non-negligible chance of winning the security game defined above. Moreover, if the null hypothesis is rejected for multiple samples $\mathbf{q}_{ij}$ of the tensor $\mathbf{Q}$ then there is a potential threat of pattens for some individual positions and the adversary may use this partial information leak to win the considered security game with non-negligible probability, if these patterns are stable under repeats of the experiment.

Let us consider an example of the performed experiment consisting of $k = 1000$ iterations. Assume the parameter values $t = 4$ and $m = 8$. The following base matrix $\mathbf{W}$ was generated:

$$\mathbf{W} = \begin{pmatrix} a^3b & a^3 & a^4 & a & e & a^7 & a^5 & a^5b \\ a^4 & a^4 & a^6 & a^5 & a^7b & a^5 & a^7 & a^6 \\ a^2 & a & a & a^5 & e & a^2 & a & a^2 \\ a^4 & a^2 & a^2 & a^5 & e & e & a^4 & a^2 \\ a^4 & e & a^6 & a^7 & ab & a^4 & a^6 & a^6 \\ a^6 & e & a^7 & a^5 & e & a^7 & a^5 & a^2 \\ a^6 & a^7 & e & a & a^6 & a^2 & a^7 & a^6 \\ a^3b & a^5 & a & a^3 & ab & a^2 & a^3 & a^5b \end{pmatrix}. \tag{14}$$

Note that for this choice of $\mathbf{W}$ we have $c = 5$ in Eq. (11).

Since there are a total of 1000 pairs $(\mathbf{X}_i, \mathbf{Y}_i)$ generated and matrix exponents $\mathbf{V}_i$ calculated, here we present only the matrices obtained during the first iteration as the example:

$$\mathbf{X_1} = \begin{pmatrix} 1 & 0 & 2 & 3 & 6 & 1 & 2 & 7 \\ 4 & 0 & 2 & 4 & 3 & 4 & 4 & 6 \\ 6 & 3 & 4 & 6 & 3 & 1 & 1 & 2 \\ 0 & 4 & 7 & 5 & 7 & 1 & 3 & 4 \\ 7 & 1 & 6 & 6 & 5 & 2 & 4 & 5 \\ 5 & 0 & 6 & 6 & 1 & 3 & 2 & 1 \\ 0 & 3 & 3 & 6 & 4 & 2 & 7 & 4 \\ 1 & 4 & 4 & 5 & 4 & 2 & 6 & 1 \end{pmatrix}, \quad \mathbf{Y_1} = \begin{pmatrix} 3 & 5 & 4 & 4 & 1 & 2 & 1 & 4 \\ 7 & 3 & 4 & 7 & 1 & 2 & 2 & 1 \\ 1 & 2 & 7 & 2 & 5 & 1 & 0 & 0 \\ 4 & 7 & 1 & 4 & 2 & 1 & 0 & 7 \\ 4 & 6 & 4 & 2 & 2 & 2 & 2 & 0 \\ 1 & 0 & 7 & 2 & 5 & 0 & 0 & 0 \\ 0 & 1 & 7 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 3 & 0 & 3 & 6 & 5 \end{pmatrix},$$

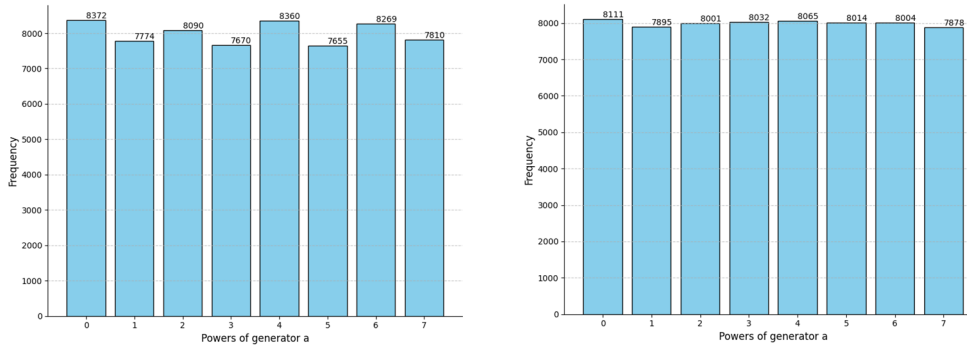
$$\mathbf{V_1} = \begin{pmatrix} e & a^7 & a^3 & a & a^6 & a^4 & e & e \\ e & a^5 & a & a^4 & a^4 & a^5 & e & a^3 \\ a^4 & a^6 & a^2 & a^2 & a^6 & a^3 & a^2 & a^7 \\ a^5 & a^2 & a & a^7 & a & a^7 & e & a^7 \\ a^3 & a^7 & a^6 & a^3 & a & a^7 & a^2 & a^4 \\ e & a^3 & a^7 & a^3 & a^4 & e & a^4 & a^2 \\ e & e & a^6 & a^7 & a^4 & a^4 & a^2 & a \\ a^2 & a & a^5 & a^2 & a^6 & a^4 & a^4 & a^7 \end{pmatrix}. \tag{15}$$

The histogram after 1000 iterations is presented below. Also, for comparison we have generated 1000 random matrices with entries uniformly chosen from $\mathbb{Z}_8$.

Due to the low p-value of the obtained results the null hypothesis is rejected in case of Fig. 1(a) and hence the tensor $\mathbf{Q}$ was not considered. We could explain this result by inspecting the elements of the given $\mathbf{W}$: since in the first and last columns even-degree powers must dominate due to Template 1 and we only have 8 columns in total, the impact of even powers is crucial when exponentiating to left and right power matrices in Eq. (1) and Eq. (2) respectively. Hence, we see that the even powers of the generator a are more likely in this case.

After performing a couple of extra experiments with the same parameters, the p-value did not increase, so we assume that repeating the experiment does not significantly change the p-value. Hence, relying on the obtained results we see that the MPF decisional problem is solvable for this case. In other words, due to the observed pattern of the even powers being more frequent, we see a significant difference between the MPF value $\mathbf{K}_0$ and a truly random matrix $\mathbf{K}_1$ as presented in Fig. 1. Hence, the matrix order is too small to obtain a complex MPF decisional problem.

On the other hand, based on the presented results we make a conjecture that the observed parity effect becomes less noticeable or even disappears as the size of the matrix increases, since the matrix **W** contains more free columns and the impact of the three specific columns reduces.



a) Histogram for the experiment data: p-value for sample **q**: $3.5 \cdot 10^{-15}$

b) Histogram for truly random matrices: p-value for sample **q**: 0.60

Fig. 1. Comparison of the results of the experiment to truly random data for security parameters $t = 4$ and $m = 8$

Let us now present our findings for the parameter values: $t = 4$ and $m = 12$. The idea of the experiment stays the same and the total number of iterations is $k = 1000$. We suppress the explicit presentation of the matrix **W** to shorten the paper. For better comparison we repeat the experiment three times each time changing the matrix **W**. Also, we have generated 1000 truly random 12×12 matrices. The results are presented in Fig. 2.

Evidently, the p-values differ in all cases, but all of them are greater than the selected threshold of 0.05. Interestingly enough, the p-value of the truly random data was less than the p-value of the Experiment 3 and comparable to other obtained p-values. Moreover, we can see that even for truly random data the null hypothesis was rejected for several positions of the matrix. However, there are no recognizable patterns in the positions where the uniformness was rejected. Neither the number of such positions nor their locations in the matrices are stable. Hence the adversary cannot acquire any valuable information by studying these positions which could potentially increase the probability of winning the considered security game. Relying on these observations we claim that for these parameter values the MPF value $\mathbf{K}_0$ is indistinguishable from a truly random matrix $\mathbf{K}_1$.

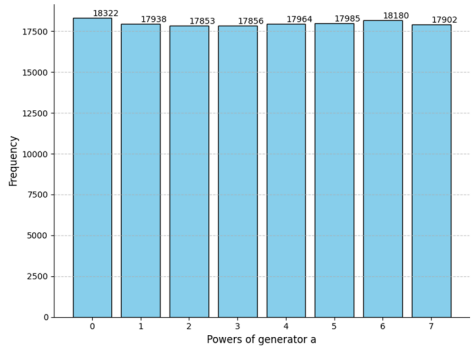
Additionally, we performed experiments with other values of the security parameters. Since p-values for the experiments greatly vary and sometimes become lower than the considered threshold. For this reason, for each platform group $\mathbb{M}_{16}$, $\mathbb{M}_{32}$, $\mathbb{M}_{64}$ and $\mathbb{M}_{128}$ we performed the search for the smallest m such that the null hypothesis could not be rejected for all the experiments. We started at 8×8 matrices and increased m by 1 until all 25 experiments produced p-values greater than 0.05. Based on the obtained results we make a conjecture that considered security game could not be won in the average case for the following parameter values shown in Table 1.

Table 1. Minimal matrix size dependence on the platform group

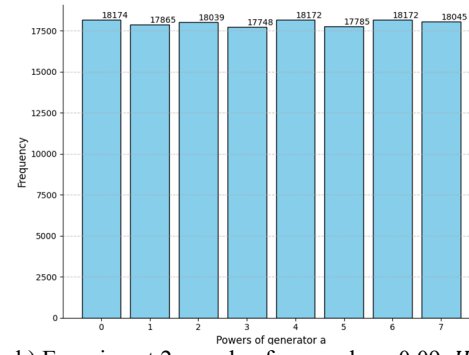
Platform group	$\mathbb{M}_{16}$	$\mathbb{M}_{32}$	$\mathbb{M}_{64}$	$\mathbb{M}_{128}$
m	14	14	14	> 16

We can see from the presented results that as the cardinality of the platform group increases, the impact of even degrees becomes more noticeable. Hence, for practical implementation of our KEP it may be reasonable to consider a balance between the cardinality of the platform group and the matrix size, since large matrices require more available memory space. For example, for the platform group $\mathbb{M}_{16}$ and 14×14 matrices 490 bytes of memory are needed to store matrices **W**, **L**,

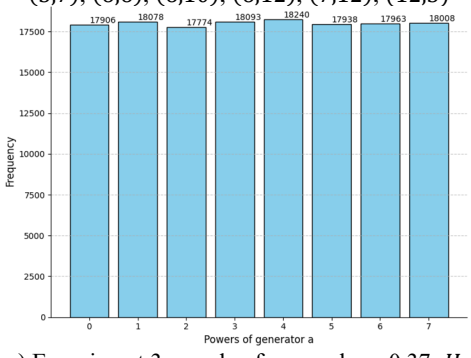
R, **X**, **Y** and **A**, whereas for the platform group $\mathbb{M}_{128}$ and 16×16 matrices 1216 bytes of memory are required to store this data and the protocol is potentially less secure in the statistical sense. Also, memory is required to store a vector of coefficients. Moreover, it may be a good idea to store tables for mathematical operations in the platform group as well as powers of **L** and **R** to speed up the execution of the protocol in exchange for memory.



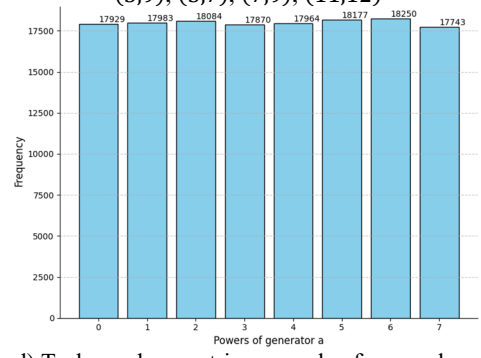
a) Experiment 1: p-value for sample q: 0.15; H_0 rejected for the following positions of Q: (2,9), (4,6), (5,7), (6,6), (6,10), (6,12), (7,12), (12,5)



b) Experiment 2: p-value for sample q: 0.09; H_0 rejected for the following positions of Q: (2,4), (3,9), (5,7), (7,9), (11,12)



c) Experiment 3: p-value for sample q: 0.37; H_0 rejected for the following positions of Q: (1,9), (4,8), (4,9), (4,10), (6,3), (8,1), (8,10), (10,9), (11,4), (11,6), (12,3), (12,10)



d) Truly random matrices: p-value for sample q: 0.16; H_0 rejected for the following positions of Q: (1,11), (1,12), (2,1), (2,5), (6,11)

Fig. 2. Comparison of the results of the experiment to truly random data for security parameters $t = 4$ and $m = 12$

In conclusion we note that due to the sporadic changes of the p-value the obtained results should be viewed as recommendations based purely on statistical results. In other words, these result must be viewed as minimal recommendations for the values of public parameters. Algebraic analysis must also be taken into consideration. Such methods as the linearization technique, or the faithful matrix representation of the elements of the group $\mathbb{M}_{2^t}$ were not considered in this work. Should these methods provide the adversary with some useful information about private keys, we must evaluate the dangers caused by them and hopefully avoid them by appropriately increasing the values the public parameters of the system.

4. Conclusions

In this paper, we have presented the results of the statistical analysis aimed at distinguishing the public key of the legit user from a truly random matrix. We have shown that for small matrices the adversary can gain a significant advantage in winning the security game defined in Section 3 based on the distribution of the entries of the public key matrix. However, this advantage vanishes

as matrices become larger. Hence, based on the presented results we could recommend considering matrices of size 14 at the very least. Additional experiments are needed to find the optimal size of matrices for large groups, i.e. when the group-defining parameter $t \geq 7$.

Notably, the security of our protocol relies on a hard decisional problem. However, the latter result means that to implement our protocol in practice, we need to find the balance between the choice of public parameter values and the required memory for data storage. Furthermore, unreasonably large values of the public parameters can also negatively affect the execution time of the protocol thus making it less attractive to the designers of cryptographic software.

The obtained results will serve as a basis for our future research of other cryptographic primitives based on the MPF defined over modular-maximal cyclic groups.

Acknowledgements

The authors have not disclosed any funding.

Data availability

The datasets generated during and/or analyzed during the current study are available from the corresponding author on reasonable request.

Author contributions

Aleksejus Mihalkovich: conceptualization, formal analysis, investigation, methodology, project administration, supervision, writing and visualization. Jokubas Zitkevicius: data curation, formal analysis, investigation, software, writing and visualization.

Conflict of interest

The authors declare that they have no conflict of interest.

References

[1] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, Vol. 22, No. 6, pp. 644–654, Nov. 1976, https://doi.org/10.1109/tit.1976.1055638

[2] D. Boneh and V. A. Shoup, *Graduate Course in Applied Cryptography*. 2020.

[3] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *35th Annual Symposium on Foundations of Computer Science*, pp. 124–134, Apr. 2024, https://doi.org/10.1109/sfcs.1994.365700

[4] "Post-Quantum Cryptography," Computer Security Division, https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/call-for-proposals

[5] "NIST Announces First Four Quantum-Resistant Cryptographic Algorithms," NIST, 2022.

[6] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, Vol. 549, No. 7671, pp. 188–194, Sep. 2017, https://doi.org/10.1038/nature23461

[7] R. Badhwar, "The need for post-quantum cryptography," in *The CISO's Next Frontier*, Cham: Springer International Publishing, 2021, pp. 15–30, https://doi.org/10.1007/978-3-030-75354-2_2

[8] D. Micciancio and S. Goldwasser, *Complexity of Lattice Problems*. Boston, MA: Springer US, 2002, https://doi.org/10.1007/978-1-4615-0897-7

[9] A. Mihalkovich, E. Sakalauskas, and K. Luksys, "Key exchange protocol defined over a non-commuting group based on an NP-complete decisional problem," *Symmetry*, Vol. 12, No. 9, p. 1389, Aug. 2020, https://doi.org/10.3390/sym12091389

[10] A. Mihalkovich, K. Luksys, and E. Sakalauskas, "Sigma identification protocol construction based on MPF defined over non-commuting platform group," *Mathematics*, Vol. 10, No. 15, p. 2649, Jul. 2022, https://doi.org/10.3390/math10152649

[11] E. Sakalauskas and K. Luksys, "Matrix power S-box construction," *Cryptology ePrint Archive*, 2007.

[12] E. Sakalauskas, N. Listopadskis, and P. Tvarijonas, "Key agreement protocol (KAP) based on matrix power function," in *6th International Conference on Information Research and Applications*, 2008.

[13] A. Mihalkovič and E. Sakalauskas, "Asymmetric cipher based on MPF and its security parameters evaluation," *Proceedings of The Lithuanian Mathematical Society*, Vol. 53, pp. 72–77, 2012.

[14] E. Sakalauskas and A. Mihalkovich, "New asymmetric cipher of non-commuting cryptography class based on matrix power function," *Informatica*, Vol. 25, pp. 283–298, 2014.

[15] J. Liu, H. Zhang, and J. Jia, "A linear algebra attack on the non-commuting cryptography class based on matrix power function," in *Information Security and Cryptology*, pp. 343–354, Mar. 2017, https://doi.org/10.1007/978-3-319-54705-3_21

[16] E. Sakalauskas, A. Mihalkovich, and A. Venčkauskas, "Improved asymmetric cipher based on matrix power function with provable security," *Symmetry*, Vol. 9, No. 1, Jan. 2017, https://doi.org/10.3390/sym9010009

[17] A. Mihalkovich and M. Levinskas, "Investigation of matrix power asymmetric cipher resistant to linear algebra attack," in *Information and Software Technologies*, pp. 197–208, Oct. 2019, https://doi.org/10.1007/978-3-030-30275-7_16

[18] E. Sakalauskas and A. Mihalkovich, "MPF problem over modified medial semigroup is NP-complete," *Symmetry*, Vol. 10, No. 11, p. 571, Nov. 2018, https://doi.org/10.3390/sym10110571

[19] H. Grundman and T. Smith, "Automatic realizability of Galois groups of order 16," *Proceedings of the American Mathematical Society*, Vol. 124, No. 9, pp. 2631–2640, Jan. 1996, https://doi.org/10.1090/s0002-9939-96-03345-x

[20] H. G. Grundman and T. L. Smith, "Realizability and automatic realizability of Galois groups of order 32," *Central European Journal of Mathematics*, Vol. 8, No. 2, pp. 244–260, Apr. 2010, https://doi.org/10.2478/s11533-009-0072-x

[21] H. G. Grundman and T. L. Smith, "Galois realizability of groups of order 64," *Central European Journal of Mathematics*, Vol. 8, No. 5, pp. 846–854, Aug. 2010, https://doi.org/10.2478/s11533-010-0052-1

Aleksejus Mihalkovich received a Ph.D. degree in Kaunas University of Technology, in 2015. Since 2019 he is an Assist. Professor in the Department of Applied Mathematics and a member of Cryptography and Blockchain Technology research group. His current research interests include the cryptanalysis of symmetric and asymmetric cryptographic primitives.

Jokubas Zitkevicius is currently pursuing a bachelor's degree of Applied Mathematics at Kaunas University of Technology. A member of Cryptography and Blockchain Technology research group.