mathematics

MDPI

Article

# Counter Mode of the Shannon Block Cipher Based on MPF Defined over a Non-Commuting Group

**Aleksejus Mihalkovich** *,†, **Matas Levinskas** † and **Eligijus Sakalauskas** †

Faculty of Mathematics and Natural Sciences, Kaunas University of Technology, 44249 Kaunas, Lithuania
* Correspondence: aleksejus.michalkovic@ktu.lt
† These authors contributed equally to this work.

**Abstract:** In this paper, we present a counter mode of a Shannon block cipher based on the matrix power function. We make use of the matrix power function to define a single round symmetric cipher. Continuing our previous research, we implement a non-commuting group the order of which is a power of two in order to define a CTR mode in its most classic interpretation. We explore the security of the newly defined scheme, first, by showing that our block cipher is perfectly secure and does not leak any information about the initial plaintext based on the ciphertext. Then, we define a sequence of security games that show how the CTR mode of our cipher can resist all passive attacks.

**Keywords:** counter mode; symmetric cryptography; perfect secrecy

**MSC:** 94A60

**Citation:** Mihalkovich, A.; Levinskas, M.; Sakalauskas, E. Counter Mode of the Shannon Block Cipher Based on MPF Defined over a Non-Commuting Group. *Mathematics* **2022**, *10*, 3363. https://doi.org/10.3390/math10183363

Academic Editors: Antanas Cenys and Daniel-Ioan Curiac

Received: 5 July 2022
Accepted: 13 September 2022
Published: 16 September 2022

## 1. Introduction

Symmetric ciphers are widely used in the modern digital world. The general idea of hiding secret information using mathematics can be described as a triplet $(Gen(), Enc(), Dec())$, where $Gen()$ is the key generation algorithm, $Enc()$ is the encryption function, and $Dec()$ is the decryption function [1,2]. A major requirement of any symmetric cipher is the ability to correctly restore the original message $\mu$ encrypted by the function $Enc()$ using the same secret key $k$. In other words, the following property should hold:

$$Dec(k, Enc(k, \mu)) = \mu.$$

Symmetric ciphers are commonly classified into block ciphers and stream ciphers depending on their structure. Block ciphers are deterministic and can be used to encrypt fixed-length groups of bits. Hence, the application of this type of ciphers is limited by the size of a block, e.g., 128 bits. On the other hand, a stream cipher takes a message as input and combines it with the keystream, usually by applying an exclusive-or (XOR) operation.

Notably, it is possible to obtain a stream cipher by linking together encrypted blocks in specific ways. This is exactly how block ciphers are currently implemented in the real world. The general methodology behind this approach is to define a mode of encryption for a block cipher. The descriptions of these various modes can be found in [3].

Due to the topic of this paper, we focus on the counter mode (CTR) of symmetric encryption. As far as the implementation of the various modes of encryption, the use of this mode is a common practice. CTR was originally proposed in [4] to create a stream of encrypted blocks, as shown in Figure 1.

The authors of [5] point out the following advantages of the CTR mode:

1. **Software efficiency:** As opposed to the cipher block chaining (CBC) mode, subsequent ciphertext blocks are computationally independent. This fact greatly contributes to the performance speed of CTR mode.

2. **Hardware efficiency**: Subsequent blocks can be computed separately, allowing parallelization of calculations.
3. **Preprocessing**: As the message is used only in the last step of CTR mode, calculations can be made in advance to make the encryption process resemble the one-time pad (OTP) technique, i.e., simple XOR of the original message and a bit string obtained long before the input.
4. **Random-access**: It is not necessary to encrypt previous blocks to obtain the ciphertext of the upcoming ones; hence, encryption can start at any block.
5. **Provable security**: The above advantages do not affect the security of the CTR mode, which relies on the pseudorandom nature of the encryption function $Enc()$.

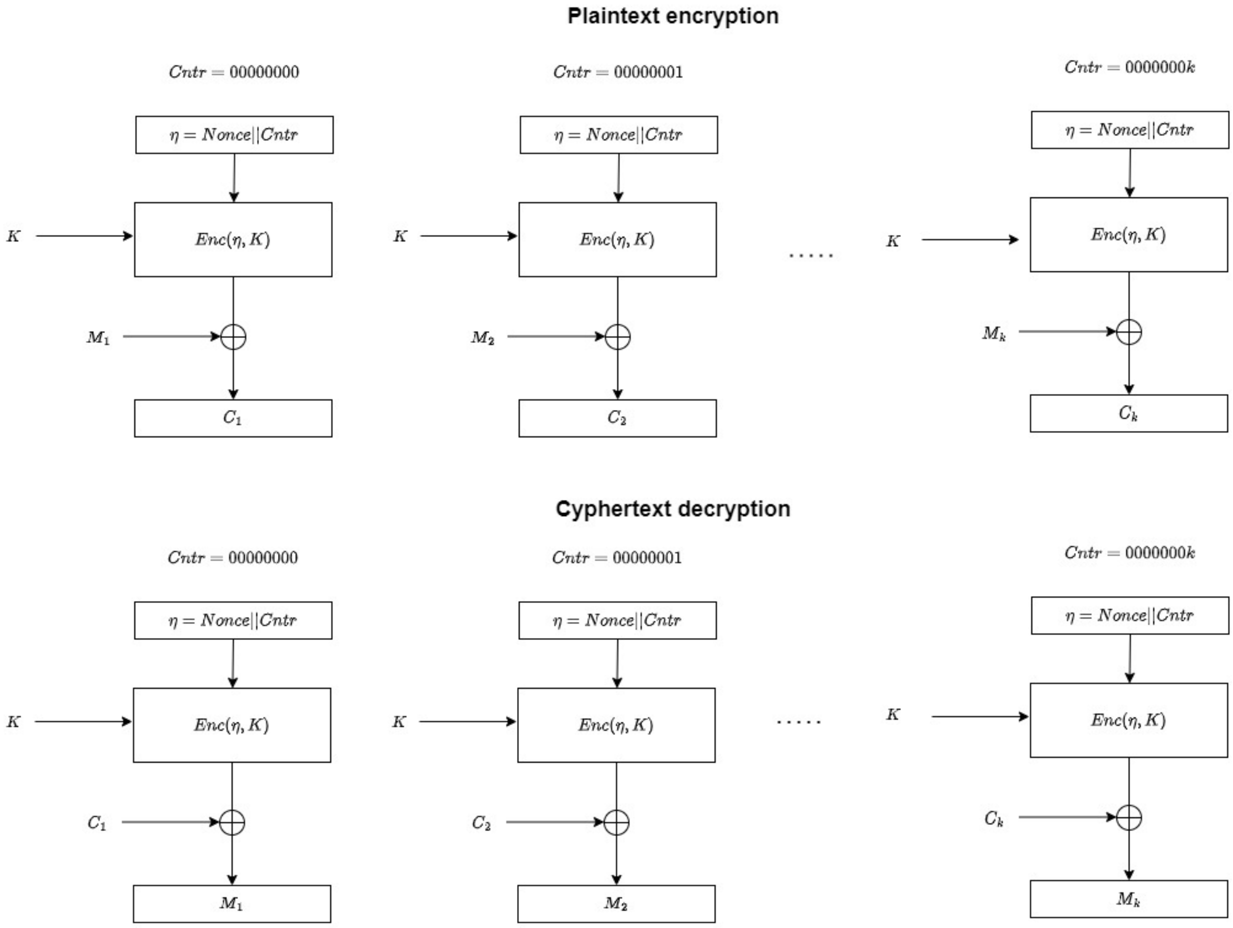

**Figure 1.** Encryption and decryption procedures of CTR mode.

An enhancement of this mode called the Galois counter mode was published in [6]. This mode was designed for use with AES cipher and was later standardized by NIST [7]. Another enhancement was proposed in [8]. Whether the block cipher presented in this paper can be implemented in these modes remains an open question thus far.

However, as pointed out in [9], applications of CTR mode in practice commonly require some means of authentication. For this reason, in [8], the authors introduced additional tags to deal with this issue.

It is worth mentioning that the current implementation of CTR mode and its enhancements usually makes use of the AES algorithm [10–14]. Due to its structure, AES uses rather simple functions, most of which are linear. For this reason, depending on the size of the key 10, 12, or 14 rounds of encryption are performed. The CTR mode of AES is widely applied in such modern technologies as blockchain, cryptocurrency, and encrypted search. Recent applications of AES CTR mode for blockchain technology can be found in [11,12]. Here, the CTR mode is used to ensure data integrity and confidentiality. The authors of [12] evaluated their approach by realizing a real implementation of their idea in the Ethereum blockchain by adding an extra layer to it. This change allowed the authors of [12] to transform the permissionless blockchain into a permessionned one, which is useful for applications in wireless networks. In [14], the authors used CTR mode to preserve the privacy of data during substring search.

It can be seen from Figure 1 that CTR uses the idea of the nonce. This information is publicly known and, much like the OTP secret key, cannot be reused. The author of [9] suggested splitting the nonce into two equal parts to achieve additional flexibility of CTR mode, thus making it applicable to longer messages. Interestingly enough, in our scheme the nonce is split to fit our goals; however, the obtained parts are not equal. Furthermore, we think that we can achieve the flexibility of our proposal by manipulating the main parameters of the block cipher. Hence, we believe that our idea can be used to encrypt short and long messages (of course, with distinct parameter values). In other words, by manipulating the block size, we think that we can maintain the speed of encryption for both types of messages.

In our research, we suggest trading multiple rounds of encryption for a single round of highly non-linear transformation. Furthermore, because we use matrix operations in our research, a significant boost in speed is possible within the single block encryption by applying parallelization of computations using several processors.

Previously, we published a paper [15] in which we defined a CBC mode of the Shannon block cipher proposed in [16]. In those papers, we implemented a mapping called the matrix power function (MPF) defined over a commuting platform, specifically, a Sylow group of prime cardinality $p$. Based on the properties of the platform group, we defined power matrices over the ring of integers $\mathbb{Z}_p$. A key feature we used in our construction is a non-homomorphic mapping $f$, which uniquely assigned an element of the Sylow group to an integer in $\mathbb{Z}_p$.

Interestingly enough, the newly defined block cipher was proven to be perfectly secure (a feature proven for the OTP technique by Shannon himself). However, a comparison of our block cipher to OTP has shown that in our case the same key can be used multiple times without revealing the secret data. Furthermore, in [17] we presented a comparison of the performance of our cipher to AES-128 and TDES. The results of that paper have shown that by varying the main parameters of our proposal, we can encrypt roughly the same amount of data about 1.5 times faster than AES-128 and 47 times faster than TDES.

Following the path laid out in this paper, we propose the CTR mode of the Shannon block cipher based on MPF. Seeking to keep our proposal closer to the classic definition of this mode, we use a certain non-commuting group containing $2^t$ elements as a platform for MPF. In this way, it is possible to apply the XOR operation at the last step of CTR mode, which was not possible with the structures used in our previous publication. Moreover, we assume that by switching to a non-commuting group we contribute to the overall security of our scheme as well.

The rest of this paper is organized as follows: in Section 2, we revise the basic definitions and algebraic structures used in our previous research; in Section 3, we propose a block cipher based on MPF mapping and explore its basic properties; in Section 4, we introduce the CTR mode of the proposed block cipher and in Section 5 we explore its resistance against passive attacks. Finally, we present our conclusions at the end of the paper.

## 2. Our Previous Work and Preliminaries

To be self-contained, let us revise the notion of MPF. As the name of this mapping states, it is defined for matrices with their entries chosen from appropriate algebraic structures. Moreover, for cryptographic purposes, we use square matrices of order $m$. Hence, in total, each matrix contains $m^2$ entries.

Let us assume that $\mathbb{S}$ is some multiplicative semigroup where each element has a maximum possible order of $ord(\mathbb{S})$. This semigroup does not need to be cyclic and can even be non-commuting. We call $\mathbb{S}$ a platform semigroup and denote the set of matrices with entries in $\mathbb{S}$ by $Mat_m(\mathbb{S})$. Let

**W** be a matrix in $Mat_m(\mathbb{S})$. We use this matrix as a base of MPF.

Due to the maximal order of elements in $\mathbb{S}$, it is clear that raising any arbitrary element of this semigroup makes sense modulo $ord(\mathbb{S})$, as larger powers can be reduced. Hence, we consider the ring $\mathbb{Z}_{ord(\mathbb{S})}$, which contains non-negative integers less than $ord(\mathbb{S})$. We refer to it as the power ring and denote the set of matrices with entries in $\mathbb{Z}_{ord(\mathbb{S})}$ by $Mat_m(\mathbb{Z}_{ord(\mathbb{S})})$. Matrices $\mathbf{X}, \mathbf{Y} \in Mat_m(\mathbb{Z}_{ord(\mathbb{S})})$ are inputs of the MPF, and we call them power matrices because their entries are used as powers.

Let us first assume that $\mathbb{S}$ is a commuting semigroup. Formally, we can then define one-sided mappings called the left-sided MPF (LMPF) and the right-sided MPF (RMPF), respectively, in the following way:

**Definition 1.** *Let* $\mathbf{W} \in Mat_m(\mathbb{S})$ *be a publicly known matrix. Then, LMPF is a mapping* $F(\mathbf{X}) : Mat_m(\mathbb{Z}_{ord(\mathbb{S})}) \to Mat_m(\mathbb{S})$ *denoted as*

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

*where* $\mathbf{E}_L \in Mat_m(\mathbb{S})$ *is the LMPF value with entries calculated in the following way:*

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

**Definition 2.** *Let* $\mathbf{W} \in Mat_m(\mathbb{S})$ *be a publicly known matrix. Then, RMPF is a mapping* $F(\mathbf{Y}) : Mat_m(\mathbb{Z}_{ord(\mathbb{S})}) \to Mat_m(\mathbb{S})$ *denoted as*

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

*where* $\mathbf{E}_R \in Mat_m(\mathbb{S})$ *is the RMPF value with entries calculated in the following way:*

$$\{e_R\}_{ij} = \prod_{k=1}^{m} w_{ik}^{y_{kj}}.$$

Notably, if the platform semigroup $\mathbb{S}$ is commuting, the two-sided MPF can be defined as a mapping $F(\mathbf{X}, \mathbf{Y}) : Mat_m(\mathbb{Z}_{ord(\mathbb{S})}) \times Mat_m(\mathbb{Z}_{ord(\mathbb{S})}) \to Mat_m(\mathbb{S})$ due to the following associativity property:

$$^{\mathbf{X}}(\mathbf{W}^{\mathbf{Y}}) = (^{\mathbf{X}}\mathbf{W})^{\mathbf{Y}}. \tag{1}$$

However, if $\mathbb{S}$ is non-commuting, property (1) does not hold in general, and the two-sided MPF cannot be defined. As such, based on the order of actions, we can define the left-to-right (LR) and right-to-left (RL) MPF.

**Definition 3.** *Let* $\mathbf{W} \in Mat_m(\mathbb{S})$ *be a publicly known matrix. Then, LRMPF is a mapping* $F(\mathbf{X}, \mathbf{Y}) : Mat_m(\mathbb{Z}_{ord(\mathbb{S})}) \times Mat_m(\mathbb{Z}_{ord(\mathbb{S})}) \to Mat_m(\mathbb{S})$ *denoted as*

$$\mathbf{E}_{LR} = \left({}^{\mathbf{X}}\mathbf{W}\right)^{\mathbf{Y}},$$

*where* $\mathbf{E}_{LR} \in Mat_m(\mathbb{S})$ *is the LRMPF value with entries calculated in the following way:*

$$\{e_{LR}\}_{ij} = \prod_{k=1}^{m} \{e_L\}_{ik}^{y_{kj}}$$

*and* $\{e_L\}_{ik}$ *are the appropriate entries of the LMPF value matrix* $\mathbf{E}_L$.

**Definition 4.** *Let* $\mathbf{W} \in Mat_m(\mathbb{S})$ *be a publicly known matrix. Then, RLMPF is a mapping* $F(\mathbf{X}, \mathbf{Y}) : Mat_m(\mathbb{Z}_{ord(\mathbb{S})}) \times Mat_m(\mathbb{Z}_{ord(\mathbb{S})}) \to Mat_m(\mathbb{S})$ *denoted as*

$$\mathbf{E}_{RL} = {}^{\mathbf{X}}\left(\mathbf{W}^{\mathbf{Y}}\right),$$

*where* $\mathbf{E}_{RL} \in Mat_m(\mathbb{S})$ *is the LRMPF value with entries calculated in the following way:*

$$\{e_{RL}\}_{ij} = \prod_{k=1}^{m} \{e_R\}_{kj}^{x_{ik}}$$

*and* $\{e_R\}_{kj}$ *are the appropriate entries of the RMPF value matrix* $\mathbf{E}_R$.

In this paper, we use the LRMPF, although similar results can be obtained by switching the order of actions.

Now, we present a brief reminder of the non-commuting group used as a platform group for MPF construction.

Set $a$ and $b$ to be two non-commuting generators and let $e$ denote the identity element of a group defined by the following relations:

$$\begin{aligned} &R_1 : a^{2^{t-1}} = e; \\ &R_2 : b^2 = e; \\ &R_3 : bab^{-1} = a^{2^{t-2}+1}, \end{aligned} \tag{2}$$

where $t$ is some positive integer which determines the cardinality of the obtained group. Explicit presentation of the so-called modular group via its generators and the defined relations is provided below:

$$\mathbb{M}_{2^t} = \langle a, b \mid R_1, R_2, R_3 \rangle \tag{3}$$

The inspiration for this group comes from several papers on the theory of indecomposable non-commuting groups. In [18], the authors discuss the realizability of seven examples of non-commuting groups which cannot be decomposed into the Cartesian product of any smaller groups. Each of the presented examples contains 16 elements in total. One of the briefly mentioned groups is a special case of the definition (3) which is called a modular group of size 16, or $\mathbb{M}_{16}$ for short. The explicit presentation of this group is

$$\mathbb{M}_{16} = \left\langle a, b \mid a^8 = e, b^2 = e, bab^{-1} = a^5 \right\rangle.$$

To remain self-contained, we present the expressions for basic operations in $\mathbb{M}_{16}$. However, we leave the proofs of these expressions outside of this paper, as they can be found in [19].

Because the group $\mathbb{M}_{16}$ is multiplicative, we can define the product of two elements. Assume the indices $\alpha, \alpha_1, \alpha_2 \in \{0, 1, \ldots, 7\}$, whereas $\beta, \beta_1, \beta_2 \in \{0, 1\}$. Then, given two elements of $\mathbb{M}_{16}$ $w_1 = b^{\beta_1}a^{\alpha_1}$ and $w_2 = b^{\beta_2}a^{\alpha_2}$, their product is calculated in the following way:

$$w_1 \cdot w_2 = \begin{cases} b^{\beta_1+\beta_2}a^{\alpha_1+\alpha_2} \text{ if } \alpha_1 \text{ is even;} \\ b^{\beta_1}a^{\alpha_1+\alpha_2} \text{ if } \alpha_1 \text{ is odd and } \beta_2 = 0; \\ b^{\beta_1+1}a^{\alpha_1+\alpha_2+4} \text{ if } \alpha_1 \text{ is odd and } \beta_2 = 1. \end{cases} \tag{4}$$

Moreover, given an element of $\mathbb{M}_{16}$ $w = b^\beta a^\alpha$, its $n$-th power is calculated in the following way:

$$w^n = \begin{cases} a^{\alpha n}, \text{ if } \beta = 0; \\ b^n a^{\alpha n}, \text{ if } \beta = 1 \text{ and } \alpha \text{ is even;} \\ b^n a^{\alpha n + 4\left[\frac{n}{2}\right]}, \text{ if } \beta = 1 \text{ and } \alpha \text{ is odd,} \end{cases} \tag{5}$$

where the notation $\left[\frac{n}{2}\right]$ stands for the integer part of $\frac{n}{2}$. We note that calculating an inverse of an element of $\mathbb{M}_{16}$ is equivalent to raising it to the seventh power; hence, we have

$$w^{-1} = \begin{cases} a^{-\alpha}, \text{ if } \beta = 0; \\ ba^{-\alpha}, \text{ if } \beta = 1 \text{ and } \alpha \text{ is even}; \\ ba^{4-\alpha}, \text{ if } \beta = 1 \text{ and } k \text{ is odd}. \end{cases} \quad (6)$$

In other papers [20,21], authors have considered non-commuting groups of sizes 32 and 64, respectively. Interestingly enough, special cases of definition (3) were mentioned in those papers as well.

In a previous paper [19], we explored the basic properties of $\mathbb{M}_{16}$ seeking implementations of this group in cryptography. The results of this paper showed that $\mathbb{M}_{16}$ can be used as a platform for MPF, and over the following years we published several papers in which we proposed various symmetric and asymmetric cryptographic primitives based on an MPF defined over $\mathbb{M}_{16}$. Moreover, we considered the complexity of the algebraic problem behind a key exchange protocol defined using the aforementioned tools. Using Schaeffer's criteria, we were able to prove that a certain MPF problem is NP-complete if $\mathbb{M}_{16}$ is used as a platform. This fact brings us one step closer to the branch of post-quantum cryptography, as it is conjectured that NP-complete problems are thus far uncrackable by quantum computers.

Even though the research presented in this paper belongs to the field of symmetric cryptography, there are similarities between the computational problems our primitives are based on. Hence, we claim that the CTR mode of our block cipher can be considered computationally safe. We define this feature formally in Section 5 and prove it in Proposition 3.

In general, the group $\mathbb{M}_{16}$ contains words of the types $a^\alpha b^\beta$ or $b^\beta a^\alpha$, where $\alpha \in \{0, 1, \ldots, 7\}$ and $\beta \in \{0, 1\}$. However, due to relations $R_1, R_2$, and $R_3$, every word can be written in the form $b^\beta a^\alpha$, which we consider a canonical representation. Hence, the cardinality of this group is $|\mathbb{M}_{16}| = 16$ . This fact is indicated by the index in its notation. A similar idea is true for the general case, i.e., $|\mathbb{M}_{2^t}| = 2^t$.

Recently, we have considered applications of MPF defined over $\mathbb{M}_{2^t}$ in symmetric cryptography. Based on our previous findings, in the upcoming section we present a symmetric block cipher, i.e., we show how to encrypt and decrypt a message using MPF defined over $\mathbb{M}_{2^t}$.

## 3. Shannon Block Cipher Based on MPF

Let us consider a message of $m^2t$ bits which can be represented by a matrix $M$ with entries in $\mathbb{M}_{2^t}$. Such a message is viewed as a single block for our cipher. The transformation of the initial message to its matrix representation is performed by splitting it into $m^2$ chunks of size $t$. The most significant bit of each piece is interpreted as the power of generator $b$ whereas the rest of the bits represent the power of generator $a$. As such, we can define two matrices $M_b$ and $M_a$ which consist of the mentioned powers of generators $b$ and $a$, respectively. Moreover, we use this index notation for other matrices as well, thus separating the powers of generators into appropriate matrices. We use the extra notations $a^{\mathbf{A}}, b^{\mathbf{B}}$ to define matrices with entries $a^{\alpha_{ij}}$ and $b^{\beta_{ij}}$, respectively, where $\mathbf{A} = \{\alpha_{ij}\}$ and $\mathbf{B} = \{\beta_{ij}\}$.

Furthermore, in our research we make use of the following extra mappings which help us to separate the powers of generators $a$ and $b$. We denote these mappings by $\phi(w)$ and $\psi(w)$, where $w \in \mathbb{M}_{2^t}$, and define them as follows:

$$\phi(b^\beta a^\alpha) = \beta, \quad \psi(b^\beta a^\alpha) = \alpha.$$

At first, it may seem that the pair $(\phi(w), \psi(w))$ is a kind of analogue to the discrete logarithm mapping. However, because $\mathbb{M}_{2^t}$ is a non-commuting and indecomposable group, the basic properties that the discrete logarithm should satisfy are invalid in the general case. Hence, the use of these mappings is not harmful to our scheme. Instead, we use them to hide the output of the LRMPF value.

More specifically, we define the matrix analogues of the mappings $\phi(w)$ and $\psi(w)$ by simply applying them entry-wise to the entries of the matrix $b^{\mathbf{B}} \odot a^{\mathbf{A}}$, where $\odot$ denotes the Hadamard product of two matrices. Denoting them by the appropriate uppercase letters, we have:

$$\Phi(b^{\mathbf{B}} \odot a^{\mathbf{A}}) = \mathbf{B}, \quad \Psi(b^{\mathbf{B}} \odot a^{\mathbf{A}}) = \mathbf{A}.$$

Now, we are ready to describe our proposal in greater detail. Prior to executing the proposed scheme, the parameters $t$ and $m$ and the shifting parameter $\kappa$, defined below in Equation (7), are published online. In addition, note that each time something is chosen at random we assume that the choice is uniform in the appropriate set of possibilities.

### 3.1. Key Generation Procedure

The result of the following key generation procedure is a symmetric key $\vec{\mathbf{K}} = (\mathbf{X}, \mathbf{Y}, \mathbf{\Delta})$.

1. Generate a binary matrix $\mathbf{\Delta}$
2. Generate a matrix $\mathbf{X}$ with random entries from $\mathbb{Z}_{2^{t-1}}$;
3. Generate a temporary matrix $\mathbf{Y}'$ with random entries from $\mathbb{Z}_{2^{t-2}}$
4. Choose a permutation matrix $\mathbf{P}$ from the set of permutation matrices
5. Define $\mathbf{Y} = 2\mathbf{Y}' + \mathbf{P}$; using Gauss–Jordan algorithm, calculate its inverse $\mathbf{Y}^{-1}$.

Note that no additional restrictions are applied each time the matrix is generated at Steps 1–3 of the presented process. In addition, because $\mathbf{P} = \mathbf{Y} \bmod 2$ is a permutation matrix, the last step of the presented algorithm is always successful, i.e., $\mathbf{Y}$ is invertible. Hence, all the steps of this procedure are executed exactly once, as none of them can result in a failure. It can be seen that due to the definition of matrix $\mathbf{Y}$, both even and odd entries of $\mathbf{Y}$ are distributed uniformly in the subsets of even and odd elements of $\mathbb{Z}_{2^{t-1}}$, respectively. This fact is important in establishing the perfect secrecy property in Section 4.

### 3.2. Encryption Function

Assuming that the original message has been converted into its matrix representation, the encryption is performed as follows:

1. The obtained matrix representation of the message is split into separate matrices $\mathbf{M}_a$ and $\mathbf{M}_b$, where each leading bit of an entry of the message matrix $\mathbf{M}$ is used to form binary matrix $\mathbf{M}_b$, whereas the rest of bits are used to form $\mathbf{M}_a$. Notably, entries of $\mathbf{M}_b$ are interpreted as powers of generator $b$. Similarly, $\mathbf{M}_a$ contains powers of generator $a$.
2. The encryption algorithm is as follows:

$$\begin{aligned} \mathbf{C}_1 &= b^{\mathbf{M}_b + \mathbf{\Delta}} \odot a^{\mathbf{M}_a + \mathbf{X}}; \\ \mathbf{C}_2 &= \left({}^{\mathbf{Y}}\mathbf{C}_1\right)^{\mathbf{Y}}; \\ \mathbf{C} &= \mathrm{Shift}_\kappa(\Phi(\mathbf{C}_2) \parallel \Psi(\mathbf{C}_2)) + (\mathbf{\Delta} \parallel \mathbf{X}), \end{aligned} \tag{7}$$

   where $\parallel$ denotes the concatenation of two matrices, $\mathrm{Shift}_\kappa$ is the entry-wise shifting by $\kappa$ bits (e.g., to the right) operator, and the addition is performed with respect to the appropriate modulo (i.e., matrices $\mathbf{M}_b$ and $\mathbf{\Delta}$ are summed modulo 2, $\mathbf{M}_a$ and $\mathbf{X}$ modulo $2^{t-1}$, and finally modulo $2^t$). In all cases, we omit moduli of addition, as their values are usually clear from the context.
3. The matrix $\mathbf{C}$ is converted into a string of bits by concatenating its entries in the following way:

$$c = c_{11} \parallel c_{12} \parallel \ldots \parallel c_{1m} \parallel c_{21} \parallel c_{22} \parallel \ldots \parallel c_{2m} \parallel c_{mm}.$$

   The obtained string $c$ is the ciphertext of the initial message.

Due to the discussed steps, the encryption function is provided by

$$\mathrm{Enc}(\vec{\mathbf{K}},\mathbf{M}) = \mathrm{Shift}_{\kappa}(\Phi(({}^{\mathbf{Y}}\mathbf{C}_1)^{\mathbf{Y}}) \parallel \Psi(({}^{\mathbf{Y}}\mathbf{C}_1)^{\mathbf{Y}}) + (\mathbf{\Delta} \parallel \mathbf{X}), \tag{8}$$

where $\mathbf{M} = \mathbf{M}_b \parallel \mathbf{M}_a$ is the original message represented in matrix form and $\mathbf{C}_1$ is defined as in Equation (7).

### 3.3. Decryption Function

Let us assume that the received ciphertext $c$ has been transformed into a matrix in the same way as the original message. The following procedure is performed to decrypt the encrypted message using the symmetric key $\vec{\mathbf{K}} = (\mathbf{X}, \mathbf{Y}, \mathbf{\Delta})$.

1. The decryption algorithm is as follows:

$$\begin{aligned}
\mathbf{D}_1 &= \mathrm{Shift}_{t-\kappa}(\mathbf{C} - \mathbf{\Delta} \parallel \mathbf{X}).\\
\mathbf{D}_2 &= b^{\mathbf{D}_{1b}} a^{\mathbf{D}_{1a}}\\
\mathbf{D}_3 &= \left({}^{\mathbf{Y}^{-1}}\mathbf{D}_2\right)^{\mathbf{Y}^{-1}};\\
\mathbf{D}_a &= \Psi(\mathbf{D}_3) - \mathbf{X},\\
\mathbf{D}_b &= \Phi(\mathbf{D}_3) - \mathbf{\Delta}
\end{aligned} \tag{9}$$

where $\mathbf{D}_{1b}$ is a binary matrix obtained by splitting the first bits of $\mathbf{D}_1$ and $\mathbf{D}_{1a}$ consists of the leftover bits. Subtraction is to be treated as an inverse of addition in the encryption algorithm (7).
2. Matrices $\mathbf{D}_a$ and $\mathbf{D}_b$ are concatenated together entry-wise, producing matrix $\mathbf{D} = \mathbf{D}_b \parallel \mathbf{D}_a$.
3. The obtained matrix $\mathbf{D}$ undergoes the procedure of transformation to a string of bits by concatenating entries of the matrix.
4. Junk symbols are removed (if any). The output of this step is the initial message.

We can summarize the steps presented above by defining the decryption function as follows:

$$\mathrm{Dec}(\vec{\mathbf{K}},\mathbf{C}) = \left(\Phi\left(\left({}^{\mathbf{Y}^{-1}}\mathbf{D}_2\right)^{\mathbf{Y}^{-1}}\right) - \mathbf{\Delta}\right) \parallel \left(\Psi\left(\left({}^{\mathbf{Y}^{-1}}\mathbf{D}_2\right)^{\mathbf{Y}^{-1}}\right) - \mathbf{X}\right), \tag{10}$$

where $\mathbf{C}$ is the ciphertext represented in matrix form and $\mathbf{D}_2$ is defined as in Equation (9).

### 3.4. Proof of the Validity

Looking at the presented encryption and decryption algorithms, we can clearly see that $\mathbf{D}_2 = \mathbf{C}_2$ due to definitions of these matrices.

Let us consider an intermediate result $\mathbf{H} = {}^{\mathbf{Y}}\mathbf{C}_1$. Note that entries of matrix $T$ are provided by

$$h_{ij} = \prod_{k=1}^{m} \{c_1\}_{kj}^{y_{ik}}. \tag{11}$$

An important restriction, which helps us to prove the validity of our protocol, is the structure of the key matrix $\mathbf{Y}$. Obviously, due to $\mathbf{Y}$ being a permutation matrix modulo 2, it is invertible over $\mathbb{Z}_{2^{t-1}}$, as its determinant is always odd and hence is relatively prime with $2^{t-1}$ for any value of $t$. Furthermore, because exactly one entry is odd in each row and each column of $\mathbf{Y}$, exactly one of the multipliers in the product (11) can contain generator $b$, and hence it can never be cancelled unless raised to an even power.

It is clear that the restoration of the matrix $\mathbf{C}_1 \in Mat_m(\mathbb{M}_{2^t})$ is successful modulo $2^{t-1}$, as in this case the non-commutative nature of the platform group is gone, i.e., $\mathbf{C}_1 \equiv \mathbf{H}^{\mathbf{Y}^{-1}} \bmod 2^{t-1}$. Hence, only the extra summands of $2^{t-1}$ can affect the final result. However, the structure of matrix $\mathbf{Y}$ helps to control extra summands in the powers of generator $a$ as well. More precisely, if the extra summand appears when calculating $h_{ij}$, then it appears when restoring $\{c_1\}_{ij}$ as well, cancelling the original effect. Similarly, if the extra summand does not appear in the first place, then it does not appear during decryption. Hence, we have $\mathbf{C}_1 = \mathbf{H}^{\mathbf{Y}^{-1}}$. This is due to the fact that the parity of the powers of generator $a$ is preserved during decryption calculations thanks to the structure of matrices $\mathbf{Y}$ and $\mathbf{Y}^{-1}$. For this reason, and due to the successful restoration of the powers of generator $b$ using Formulas (4) and (5), we obtain the desired result. Hence, the matrix $\mathbf{Y}^{-1}$, which has the same structure as $\mathbf{Y}$, successfully restores the initial matrix $\mathbf{C}_1$ when applied to $\mathbf{H}$, i.e., we have $\mathbf{C}_1 = \mathbf{H}^{\mathbf{Y}^{-1}}$.

We now consider the matrix $\mathbf{C}_2 = \mathbf{H}^{\mathbf{Y}} = {}^{\mathbf{Y}}\mathbf{C}_1^{\mathbf{Y}}$. Due to the properties established in this proof, the matrix $\mathbf{Y}^{-1}$ successfully restores matrix $\mathbf{H}$, i.e., $\mathbf{H} = \mathbf{C}_2^{\mathbf{Y}^{-1}}$.

Combining these two observations, we gain the following result:

$$\mathbf{D}_2 = {}^{\mathbf{Y}^{-1}}\mathbf{D}_1^{\mathbf{Y}^{-1}} = {}^{\mathbf{Y}^{-1}}\mathbf{C}_2^{\mathbf{Y}^{-1}} = {}^{\mathbf{Y}^{-1}}\left({}^{\mathbf{Y}}\mathbf{C}_1^{\mathbf{Y}}\right)^{\mathbf{Y}^{-1}} = \mathbf{C}_1.$$

Moreover, applying the mappings $\Phi$ and $\Psi$ and subtracting the appropriate matrices yields the matrix form $\mathbf{M}$ of the initial message, i.e., $\mathbf{D} = \mathbf{M}$.

Matrix $\mathbf{D}$ now undergoes a transformation to obtain a string of bits $d$ by concatenating its entries as follows:

$$d = d_{11} \parallel d_{12} \parallel \ldots \parallel d_{1m} \parallel d_{21} \parallel d_{22} \parallel \ldots \parallel d_{2m} \parallel d_{mm}.$$

Relying on the discussed observations, we conclude that $d$ is the bit string representing the initial message with junk symbols at the end. These can now be dropped to leave us with the initial message.

### *3.5. The Main Properties of the Proposed Block Cipher*

In our previous paper [16], we have shown that all the intermediate steps of the similarly designed block cipher operating in CBC mode produce values uniformly distributed in the appropriate algebraic structures. Moreover, the block cipher proposed in that paper has the perfect secrecy property. Here, we revise the appropriate proofs and adapt them to fit our proposal.

Due to the similarities between the two ciphers, we claim that the following statements are true.

**Proposition 1.** *Assume that the secret key $\vec{\mathbf{K}}$ is uniformly chosen from the set of all possible keys $\mathcal{K}$. Then, in Step 2 of the counter mode, the intermediate matrices $\mathbf{C}_1, \mathbf{C}_2$ are distributed uniformly in $Mat_m(\mathbf{M}_{2^t})$ and the matrix $\mathbf{C}$ is distributed uniformly in $Mat_m(\mathbf{Z}_{2^t})$.*

**Proof.** Let us apply the previously defined mappings $\Phi(\cdot)$ and $\Psi(\cdot)$ to the matrix $\mathbf{C}_1 = b^{\mathbf{B}} \odot a^{\mathbf{A}}$, where $\mathbf{B} = \mathbf{N}_b + \mathbf{\Delta}$ and $\mathbf{A} = \mathbf{N}_a + \mathbf{X}$. Recall that due to the statement of the proposition and the properties of matrix summation, the entries $\Phi(\mathbf{C}_1) = \mathbf{B}$ and $\Psi(\mathbf{C}_1) = \mathbf{A}$ are uniformly distributed in $\mathbb{Z}_2$ and $\mathbb{Z}_{2^{t-1}}$, respectively.

Because $\mathbf{Y}$ is a permutation matrix modulo 2, it mixes up the entries of $\mathbf{A}$ without changing them. For this reason, the entries of $\Phi(\mathbf{C}_2)$ are uniformly distributed in $\mathbb{Z}_2$. Hence, powers of generator $b$ in matrix $\mathbf{C}_2$ are uniformly distributed in $\mathbb{Z}_2$.

We now consider the distribution of the powers of generator $a$ in matrix $\mathbf{C}_2$. Keeping in mind the properties of permutation matrices, without loss of generality, we henceforth consider a special case of identity permutation, i.e., we assume that odd entries of matrix $\mathbf{Y}$ are located on its main diagonal. We make a remark regarding the general case of permutation matrices later in this proof.

Let us focus on the intermediate result $\mathbf{V} = {}^{\mathbf{Y}}\mathbf{C}_1$ and apply the mapping $\Psi(\cdot)$ to this matrix. We can express every entry $\psi(v_{ij})$ as follows:

$$\psi(v_{ij}) = \sum_{k=1}^{m} \psi(\{c_1\}_{kj}) y_{ik} + \gamma_{ij}, \tag{12}$$

where $\gamma_{ij} \in \{0, 2^{t-2}\}$ can be one of two possible values depending on the number of times the extra summand $2^{t-2}$ was added. We split the sum (12) into two parts based on the parity of entries of matrix $\mathbf{Y}$. Then, for even values of $\mathbf{Y}$, we have

$$s_{ij} = \sum_{k=1, k\neq i}^{m} \psi(\{c_1\}_{kj}) y_{ik} + \gamma_{ij} \tag{13}$$

Due to the special structure of matrix $\mathbf{Y}$, we have a single summand of the sum (12) containing an odd entry $y_{ii}$. Hence, we denote

$$u_{ij} = \psi(\{c_1\}_{ij}) y_{ii}. \tag{14}$$

Note that if $\mathbf{Y}$ is a permutation matrix other than identity modulo 2, then the column index changes in the extracted summand. The omitted index in sum (13) changes as well. These are the only two differences in the general case.

Due to construction, all possible values of the sum (13) lie in the subset of even elements of $\mathbb{Z}_{2^{t-1}}$, and hence we claim that

$$\sum_{r=0}^{2^{t-2}-1} \Pr(s_{ij} = 2r) = 1, \tag{15}$$

which is obviously true, as these probabilities form a total probability. The exact values of these probabilities are irrelevant.

Considering the only odd summand, we can calculate the following probability:

$$\Pr(u_{ij} = u_0) = \Pr(\psi(\{c_1\}_{ij}) y_{ii} = u_0) = \Pr(\psi(\{c_1\}_{ij}) = u_0 y_{ii}^{-1}) = \frac{1}{2^{t-1}}, \tag{16}$$

where $u_0 \in \mathbb{Z}_{2^{t-1}}$ is fixed. This comes from the fact that $\gcd(y_{ii}, 2^{t-1}) = 1$, and hence $y_{ii}^{-1}$ exists. Moreover, $\psi(\{c_1\}_{ij})$ is uniformly distributed due to the statement of the lemma.

Meshing facts (15) and (16) together, we obtain the following result:

$$\begin{aligned} \Pr(\psi(v_{ij}) = z_0) = \Pr(s_{ij} + u_{ij} = z_0) = \Pr(u_{ij} = z_0 - 2r)\cdot \\ \cdot \Pr(s_{ij} = 2r) = \frac{1}{2^{t-1}} \sum_{r=0}^{2^{t-2}-1} \Pr(s_{ij} = 2r) = \frac{1}{2^{t-1}}. \end{aligned} \tag{17}$$

This result means that powers of generator $a$ in an intermediate matrix $\mathbf{V}$ are distributed uniformly in $\mathbb{Z}_{2^{t-1}}$. Note that because the term $\gamma_{ij}$ does not play a major part in this calculation, distributions of power of both generators are independent of each other, i.e., powers of generator $b$ do not in any way affect the distribution of powers of generator $a$.

Similar calculations of probabilities can be performed for the powers of generator $a$ in the matrix $\mathbf{V}^{\mathbf{Y}} = \left({}^{\mathbf{Y}}\mathbf{C}_1\right)^{\mathbf{Y}} = \mathbf{C}_2$. Relying on the uniform distribution of entries of matrix $\mathbf{V}$ and properties of matrix $\mathbf{Y}$, we draw a conclusion that powers of generator $a$ in matrix $\mathbf{C}_2$ are distributed uniformly.

Lastly, the powers of both generators in matrix $\mathbf{C}_2$ are distributed uniformly. Then, due to the properties of the matrix summation and uniform distribution of concatenated matrices, the final output $\mathbf{C}$ is distributed uniformly in $Mat_m(\mathbb{Z}_{2^t})$. The shifting operation does not play any part in this distribution, as it only performs an additional mix of bits. □

**Proposition 2.** *Assume that the secret key $\vec{\mathbf{K}}$ is uniformly chosen from the set of all possible keys $\mathcal{K}$. Then, the block cipher presented in Step 2 is perfectly secure.*

**Proof.** Let us consider encryption algorithm (7). First, we turn our attention to matrix $\mathbf{C}_1$ and focus on the powers of generator $a$. Denoting $\mathbf{N}_a + \mathbf{X} = \mathbf{U}$, we rewrite each entry of matrix $U$ in the following form:

$$u_{ij} = x_{ij} + n_{aij}, i, j \in \{1, \dots, m\}. \tag{18}$$

Due to the statement of the theorem, entries $x_{ij}$ are chosen at random and are uniformly distributed in $\mathbb{Z}_{2^{t-1}}$, whereas entries $n_{aij}$ are random arbitrary distributed values in $\mathbb{Z}_{2^{t-1}}$. For any fixed matrix $\mathbf{U}_0$ with entries $u_{0ij} \in \mathbb{Z}_{2^{t-1}}$, we have

$$\begin{aligned} \Pr(u_{ij} = u_{0ij}) = &\Pr(x_{ij} = u_{0ij} - n_{aij}) = \\ &= \frac{1}{2^{t-1}} \sum_{n_{0ij} \in \mathbb{Z}_{2^{t-1}}} \Pr(n_{aij} = n_{0ij}) = \frac{1}{2^{t-1}}, \end{aligned} \tag{19}$$

where $n_{0ij}$ are fixed elements of $\mathbb{Z}_{2^{t-1}}$.

We now calculate the conditional probabilities of the entries of matrix $\mathbf{U}$:

$$\Pr(u_{ij} = u_{0ij} \mid n_{aij} = n_{0ij}) = \Pr(x_{ij} = u_{0ij} - n_{0ij}) = \frac{1}{2^{t-1}}, \tag{20}$$

because the entries $x_{ij}$ and $n_{aij}$ are independent, and the difference $u_{0ij} - n_{0ij} \in \mathbb{Z}_{2^{t-1}}$.

Another important property of matrix $\mathbf{U}$ is the independence of its entries. Because all $x_{ij}, i, j = 1, \dots, m$, are independent, for all $u_{0ij} \in \mathbb{Z}_{2^{t-1}}$ we have

$$\begin{aligned} &\Pr(\cap_{i,j=1}^{m}\{u_{ij} = u_{0ij}\}) = \Pr(\cap_{i,j=1}^{m}\{x_{ij} + n_{aij} = u_{0ij}\}) = \\ &= \sum_{n \in \mathbb{Z}_{2^{t-1}}} \Pr(\cap_{i,j=1}^{m}\{x_{ij} = u_{0ij} - n_{0ij}\}, \cap_{i,j=1}^{m}\{n_{aij} = n_{0ij}\}) = \\ &= \frac{1}{2^{m^2(t-1)}} \sum_{n_{0ij} \in \mathbb{Z}_{2^{t-1}}} \Pr(\cap_{i,j=1}^{m}\{n_{aij} = n_{0ij}\}) = \frac{1}{2^{m^2(t-1)}}. \end{aligned} \tag{21}$$

In the last step, we use the fact that the sum $\sum_{n_{0ij} \in \mathbb{Z}_{2^{t-1}}} \Pr(\cap_{i,j=1}^{m}\{n_{aij} = n_{0ij}\})$ is the total probability, and hence is equal to 1.

Relying on the obtained Equalities (19)–(21), we claim that

$$\Pr(\mathbf{U} = \mathbf{U}_0) = \Pr(\mathbf{U} = \mathbf{U}_0 \mid \mathbf{N}_a = \mathbf{N}_{a0}) = \frac{1}{2^{m^2(t-1)}}, \tag{22}$$

where $\mathbf{N}_{a0} \in Mat_m(\mathbb{Z}_{2^{t-1}})$ is a fixed matrix.

Similarly, matrix $\mathbf{\Delta}$ is chosen uniformly from $\mathbb{Z}_2$. For this reason, analogous observation holds for the matrix sum $\mathbf{N}_b + \mathbf{\Delta}$, with probability $2^{-m^2}$. However, both sums in the expression of $\mathbf{C}_1$ are independent of each other, and hence we have:

$$\Pr(\mathbf{C}_1 = \mathbf{C}_{10}) = \Pr(\mathbf{C}_1 = \mathbf{C}_{10} \mid \mathbf{N} = \mathbf{N}_0) = \frac{1}{2^{m^2}} \cdot \frac{1}{2^{m^2(t-1)}} = \frac{1}{2^{tm^2}}, \tag{23}$$

where $\mathbf{C}_{10}$ is a fixed matrix defined over $\mathbb{M}_{2^t}$ and $\mathbf{M}_0$ is a fixed matrix defined over $\mathbb{Z}_{2^t}$. Hence, we have shown that the entries of matrix $\mathbf{C}_1$ are uniformly distributed in $\mathbb{M}_{2^t}$.

Let us denote the set of all possible values of key matrix $\mathbf{Y}$ by $\mathbb{K}_{\mathbf{Y}}$. Note that each matrix from this set reduced modulo 2 is a permutation matrix, and hence the cardinality of this set is $|\mathbb{K}_{\mathbf{Y}}| = n! \cdot 2^{m^2(t-2)}$.

We now consider the second step of the encryption algorithm (7), i.e., matrix $\mathbf{C}_2$. Due to Proposition 1, entries of MPF value are uniformly distributed in $\mathbb{M}_{2^t}$. All that is left is to explore the conditional probabilities of its entries, expressed as follows:

$$\Pr(\mathbf{C}_2 = \mathbf{C}_{20} \mid \mathbf{N} = \mathbf{N}_0) = \frac{\Pr(\mathbf{C}_2 = \mathbf{C}_{20}, \mathbf{N} = \mathbf{N}_0)}{\Pr(N = \mathbf{N}_0)} \tag{24}$$

Explicit calculations of probability $\Pr(\mathbf{C}_2 = \mathbf{C}_{20}, \mathbf{N} = \mathbf{N}_0)$ are presented below in matrix form for simplicity:

$$\begin{aligned} &\Pr(\mathbf{C}_2 = \mathbf{C}_{20}, \mathbf{N} = \mathbf{N}_0) = \Pr({}^{\mathbf{Y}}(\mathbf{C}_1)^{\mathbf{Y}} = \mathbf{C}_{20}, \mathbf{N} = \mathbf{N}_0) = \\ &= \Big( \sum_{\mathbf{Y}_0 \in \mathbb{K}_{\mathbf{Y}}} \Pr(\mathbf{C}_1 = {}^{\mathbf{Y}_0^{-1}}(\mathbf{C}_{20})^{\mathbf{Y}_0^{-1}}) \cdot \Pr(\mathbf{Y} = \mathbf{Y}_0) \Big) \Pr(\mathbf{N} = \mathbf{N}_0) = \\ &= \frac{1}{2^{tm^2}} \cdot \Big( \sum_{\mathbf{Y}_0 \in \mathbb{K}_{\mathbf{Y}}} \Pr(\mathbf{Y} = \mathbf{Y}_0) \Big) \cdot \Pr(\mathbf{N} = \mathbf{N}_0) = \frac{1}{2^{tm^2}} \cdot \Pr(\mathbf{N} = \mathbf{N}_0), \end{aligned} \tag{25}$$

where $\mathbf{Y}_0 \in \mathbb{K}_{\mathbf{Y}}$ is a fixed matrix. Here, we use the fact that the entries of $\mathbf{C}_1$ are identically uniformly distributed and are independent of matrix $\mathbf{N}$. Furthermore, keeping with our notation, the sum $\sum_{\mathbf{Y}_0 \in \mathbb{K}_{\mathbf{Y}}} \Pr(\mathbf{Y} = \mathbf{Y}_0)$ represents a total probability, and hence is equal to 1. Note that we use the notation $\Pr(\mathbf{N} = \mathbf{N}_0)$ to indicate the probability of a certain fixed message, which is then split into two parts $\mathbf{N}_a$ and $\mathbf{N}_b$.

We limit ourselves to the matrix form of these calculations, as the expression of probability for a single entry of $\mathbf{C}_2$ is much more complicated due to restriction on matrix $\mathbf{Y}$.

Because Expression (25) is a numerator of conditional probability (24), we obtain the following result:

$$\Pr(\mathbf{C}_2 = \mathbf{C}_{20} \mid \mathbf{N} = \mathbf{N}_0) = \frac{\frac{1}{2^{tm^2}} \cdot \Pr(\mathbf{N} = \mathbf{N}_0)}{\Pr(\mathbf{N} = \mathbf{N}_0)} = \frac{1}{2^{tm^2}}. \tag{26}$$

It can be seen from the obtained result that the distributions of $\mathbf{C}_2$ and $\mathbf{N}$ match, and we can hence draw the conclusion that entries of matrix $\mathbf{C}_2$ are independent of plaintext matrix $\mathbf{N}$.

The proof for the last step of the encryption algorithm is analogous to the proof of the first step, as the matrix $\mathbf{\Delta} \parallel \mathbf{X}$ consists of uniformly distributed entries in $\mathbb{Z}_{2^t}$, whereas the shifting function does not have an impact on the distribution of the entries of the other matrix summand. □

However, it is important to note that for Proposition 2 to take place we have to apply restriction on matrix $\mathbf{Y}$, i.e., we must have $\mathbf{Y} = P \bmod 2$, where $P$ is a permutation matrix. Otherwise, there is no way to ensure that the encryption function is one-to-one, and hence there is a second nonce $\eta$, which can be used to decrypt the ciphertext. For these reasons, the conditional probabilities for the matrix $\mathbf{C}_2$ do not grant us the desired independence from the nonce if the constraint on $\mathbf{Y}$ is neglected.

We should emphasize that in Proposition 2 we have established perfect secrecy for the encryption of a single block only. Obviously, as the plaintext grows in size it must be split into several blocks, and due to the fixed length of the secret key the CTR mode cannot possibly possess the perfect secrecy property, as it trivially contradicts Shannon theorem.

## 4. Counter Mode of Our Cipher

In this section, we introduce the main idea of this paper, i.e., the counter mode of our cipher. Due to the general scheme of this mode presented in Figure 1, we consider only the encryption function (8) of our original idea. Note that the restriction on matrix $\mathbf{Y}$ is required in order to ensure that the encryption function is one-to-one, which, as we show in this section, plays an important role in establishing the perfect secrecy property of our block cipher. Moreover, according to [1], despite the fact that the nonce is never decrypted, the original plaintext has to be restored using the same nonce and no other such nonces should exist. This condition implies the one-to-one nature of the encryption function. Hence, for now we leave this restriction intact and present our thoughts on the matter at the end of this paper.

Prior to performing encryption of the plaintext limited by $2^l$ blocks, the sender generates the nonce as a bit string, which for now can be interpreted as a number $\eta \in \{0, 1, \ldots, 2^{m^2 t} - 1\}$. This is done by randomly choosing an integer $\eta' \in \{0, 2^{m^2 t - l}\}$ and setting $\eta = 2^l \eta'$. The counter mode is executed as follows:

1. For the $j$-th block, we define a bit string $n = \eta + (j - 1)$ of size $m^2 t$ and convert it into a matrix by splitting off $t$-bit chunks $n_1, n_2, \ldots, n_{m^2}$ and interpreting them as entries of the matrix $\mathbf{N}$ row-wise, i.e., the matrix $\mathbf{N}$ is as follows:

$$\mathbf{N} = \begin{pmatrix} n_1 & n_2 & \ldots & n_m \\ n_{m+1} & n_{m+2} & \ldots & n_{2m} \\ \ldots & \ldots & \ldots & \ldots \\ n_{m(m-1)+1} & n_{m(m-1)+2} & \ldots & n_{m^2} \end{pmatrix} \tag{27}$$

2. The matrix $\mathbf{N}$ is encrypted using the secret key $\vec{\mathbf{K}} = \{\mathbf{X}, \mathbf{Y}, \mathbf{\Delta}\}$ using the encryption function $Enc(\vec{\mathbf{K}}, \mathbf{N})$ to obtain a ciphertext matrix $\mathbf{C}$.
3. The matrix $\mathbf{C}$ is transformed into a bit string $c_j$ of size $m^2 t$ by concatenating its entries, i.e., $c_j = c_{11} \parallel c_{12} \parallel \ldots \parallel c_{1m} \parallel c_{21} \parallel \ldots \parallel c_{mm}$;
4. The plaintext is split into separate disjoint parts $\mu_j$ of $m^2 t$ bits (with junk at the end if required), where $j = 1, 2, \ldots \lfloor \frac{|\mu|}{m^2} \rfloor$. Each part is XORed with an appropriate bit string $c_j$.

The output of this algorithm is the ciphertext $(\eta, c)$, where $c$ is obtained by concatenating chunks $c_1 \oplus \mu_1, c_2 \oplus \mu_2, \ldots$ into a single string.

The decryption works similarly, with the plaintext replaced by the ciphertext in the last step.

However, the perfect secrecy property does not mean that our block cipher is impervious to other kinds of attacks. The widely known one-time pad technique is easily broken if the secret key is ever reused. This is something CTR mode and one-time pad have in common. The major difference in the CTR mode, as opposed to the one-time pad, is the fact that nonces must not be reused. However, it is much easier to ensure this restriction, and casual solutions for this issue are known.

## 5. Security Analysis

In this section, we take another step towards the security of our block cipher. Following the technique presented in [1], we use the notion of an Attack Game played between an adversary $\mathcal{A}$, an effective algorithm aimed at the disruption of communication by extracting hidden data (e.g., private key of some other relations) given the publicly available information, and a challenger, a machine excepting inputs from the adversary and generating outputs based on a certain sequence of actions.

The purpose of the attack game we consider in this section is to somehow tell apart the encryption function from other random functions. In other words, we aim to show that the encryption function can be viewed as a secure pseudorandom permutation (PRP). Note, however, that at the moment we assume that the messages to be encrypted are chosen at random. Hence, for now we adapt the notion of weak PRP security from [1].

**Attack Game 1.** *Consider the encryption function $Enc(\vec{\mathbf{K}}, \mathbf{M})$, where the $\mathbf{M}$ is the encrypted plaintext in its matrix representation. For an index $\beta \in \{0, 1\}$, we define the following Experiment $\beta$ between the challenger and the adversary $\mathcal{A}$:*

1. *The challenger randomly selects a function F in a following way:*

$$F(\mathbf{M}) = \begin{cases} Enc(\vec{\mathbf{K}}, \mathbf{M}) & \text{if } \beta = 0; \\ Rand(\mathbf{M}) & \text{if } \beta = 1, \end{cases} \tag{28}$$

   *where $Rand(\mathbf{M}) : Mat_m(\mathbb{Z}_{2^t}) \to Mat_m(\mathbb{Z}_{2^t})$ is a truly random permutation.*
2. *The adversary requests a sequence of Q queries from the challenger consisting of plaintext matrices matrices $\mathbf{M}_q$, where $q = 1, 2, \ldots, Q$ is the index of the queries and ciphertext matrices $\mathbf{C}_q = F(\vec{\mathbf{K}}, \mathbf{M})$.*
3. *The challenger generates random matrices $\mathbf{M}_q$ distributed uniformly in $Mat_m(\mathbb{Z}_{2^t})$ and computes $\mathbf{C}_q = F(\mathbf{M}_q)$. He sends the obtained pairs to the adversary.*
4. *Relying on the obtained responses, the adversary outputs an experiment indicator $\hat{\beta} \in \{0, 1\}$ and wins the game if $\hat{\beta} = \beta$.*

*Denote by $\Pr(W_\beta)$ the probability of the random event $W_\beta$ that $\mathcal{A}$ outputs the value $\beta$. The advantage in winning the above game is then provided by*

$$wPRPadv[\mathcal{A}, Enc(\vec{\mathbf{K}}, \mathbf{M})] = |\Pr(W_1) - \Pr(W_0)|.$$

Note that in this Attack Game the adversary remains passive and can only request queries one at a time. Extra investigations of possible enhancements of our proposal are needed to fully understand whether the adversary can be active in the presented Attack Game.

Relying on the uniform distribution of the ciphertext matrix in $Mat_m(\mathbb{Z}_{2^t})$ established in the previous section, we claim the following.

**Proposition 3.** *The encryption function $Enc(\vec{\mathbf{K}}, \mathbf{M})$ is a weakly secure pseudorandom permutation, i.e., the probability of winning the Attack Game 1 $wPRPadv[\mathcal{A}, Enc(\vec{\mathbf{K}}, \mathbf{M})]$ is negligible if messages are chosen at random with uniform distribution.*

**Proof.** Let us first note that the adversary $\mathcal{A}$ can gain control of all the possible messages $\mathbf{M}$ by expressing them as a linear combination of the basis elements of the message space $\mathcal{M}$. All the adversary needs to do is to request $m^2$ queries and check matrices $\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_{m^2}$ for linear independence. Every subsequent query $\mathbf{M}_q$, where $q > m^2$ can be expressed in the following way:

$$\mathbf{M}_q = \sum_{i=1}^{m^2} \alpha_{qi} \mathbf{M}_i$$

for some coefficients vector $\vec{\alpha}_q$. Conveniently, the co-domain of the function $Enc(\vec{\mathbf{K}}, \mathbf{M})$ matches the domain, and hence every output can be expressed as a linear combination of the same basis elements, i.e.,

$$\mathbf{C}_q = \sum_{i=1}^{m^2} \gamma_{qi} \mathbf{M}_i$$

for some coefficients vector $\vec{\gamma}_q$.

If $\beta = 0$, i.e., the original encryption function is used to encrypt the messages $\mathbf{M}_q$, then due to the constraint on the parameter $\mathbf{Y}$ the encryption function is a one-to-one mapping. Hence, all of the outputs $\mathbf{C}_q$ are distinct. Furthermore, given a random vector uniformly distributed $\vec{\alpha}_q$, the probability $Pr(\vec{\gamma}_q = \vec{\gamma}_q^0) = 2^{-m^2 t}$, where $\vec{\gamma}_q^0$ is a fixed vector. For the first query, we can simply use Proposition 1. For subsequent queries, we rely on the uniform distribution of message matrices, as in this case the ciphertext matrices preserve this distribution.

On the other hand, if $\beta = 1$, then because $Rand(\mathbf{M})$ is a random permutation it affects the matrix $\mathbf{M}$ in a way indistinguishable from the one presented above, i.e., the output is distributed uniformly in $Mat_m(\mathbb{Z}_{2^t})$, and hence the probability $Pr(\vec{\gamma}_q = \vec{\gamma}_q^0) = 2^{-m^2 t}$ is the same for all queries $q$.

To summarize, regardless of the value of $\beta$, all the values of the coefficients vector $\vec{\gamma}_q$ are equally possible, and hence the distribution of the outputs $F(\mathbf{M}_q)$ is indistinguishable from the uniform in $Mat_m(\mathbb{Z}_{2^t})$. For this reason, $PRPadv[\mathcal{A}, Enc(\vec{\mathbf{K}}, \mathbf{M})]$ is negligible. □

Hence, relying on the proven result, we claim that the function $Enc(\vec{\mathbf{K}}, \mathbf{M})$ can be considered a weakly secure pseudorandom permutation. We use this fact in Section 5 to prove the resistance of our main idea against passive adversaries.

Note that as of now we cannot do any better than Proposition 3. This is due to the fact that hidden correlations arise between the ciphertexts when the adversary is allowed to choose the message matrices at will. We believe that this issue can be fixed using additional actions to mix the entries of the message matrices prior to applying the MPF mapping. However, this is a topic for future research.

As we proven that the encryption function is a weakly secure pseudorandom permutation, we only consider passive attacks at the moment. We formalize the resistance of of the presented CTR mode against passive adversaries in the following Attack Game aimed at relating each obtained ciphertext to the original plaintext given two choices. This means that the adversary can obtain useful information, based on which he can choose the original plaintext with a probability significantly different from the coin toss experiment.

**Attack Game 2.** *Consider the nonce-based encryption scheme $\varepsilon(\vec{\mathbf{K}}, \mathbf{M}, \mathbf{N})$, where the ciphertext matrix $\mathbf{C} = Enc(\vec{\mathbf{K}}, \mathbf{N}) \oplus \mathbf{M}$. For an index $\beta \in \{0, 1\}$, we define the following Experiment $\beta$ between the challenger and the adversary $\mathcal{A}$:*

1. *The challenger randomly selects a key $\vec{\mathbf{K}} \in \mathcal{K}$.*
2. *The adversary requests  a sequence of queries to the challenger consisting of the pair of equal length messages $(\mathbf{M}_{q0}, \mathbf{M}_{q1})$, the nonces $\eta_q \in \mathcal{N} \setminus \{\eta_1, \eta_2, \dots, \eta_{q-1}\}$, where $\mathcal{N}$ denotes the space of all possible nonces, and the ciphertexts $\mathbf{C}_q = Enc(\vec{\mathbf{K}}, \mathbf{N}_q) \oplus \mathbf{M}_{q\beta}$.*
3. *The challenger generates messages and nonces at random. Furthermore, he computes the ciphertext as presented above. He sends these values to the adversary.*
4. *Relying on the obtained responses, the adversary outputs an experiment indicator $\hat{\beta} \in \{0, 1\}$ and wins the game if $\hat{\beta} = \beta$.*

*We denote by $\Pr(W_\beta)$ the probability of the random event $W_\beta$ that $\mathcal{A}$ outputs the value $\beta$. The advantage in winning the above game is provided by:*

$$wPAadv[\mathcal{A}, \varepsilon] = |\Pr(W_1) - \Pr(W_0)|.$$

Based on the properties of our scheme, we claim the following.

**Proposition 4.** *For any efficient adversary $\mathcal{A}$, his advantage $wPAadv[\mathcal{A}, \varepsilon]$ in Attack Game 2 is negligible.*

**Proof.** This result follows directly from the fact that $Enc(\vec{\mathbf{K}}, \mathbf{N})$ is a weakly secure pseudorandom permutation and from Theorem 5.6 of [1]. □

From the results of this paper, it can be seen that our proposed CTR mode of the block cipher based on MPF can resist all passive attacks.

From the point of view of implementation of our CTR mode, the practical advantage of winning Attack Games 1 and 2 must be taken into the consideration to determine the safe values of the main parameters of our block cipher, namely, the order of the square matrices $m$ and the group size determining parameter $t$. Though more investigations may be required in this area, we think that the link between the number of queries sent by the adversary in Attack Game 2 can be estimated by the following inequality:

$$wPAadv[\mathcal{A}, \varepsilon] \leq \frac{Q^2}{2^{m^2 t}}, \tag{29}$$

which comes from Theorems 4.4 and 5.6 of [1].

Here, we should make another important observation. Due to the general structure of the CTR mode, the decryption function is never used. This fact grants us an opportunity to discard the restriction on the power matrix $Y$, thus making the encryption function irreversible. A further investigation of this change may be required to fully understand the effect it has on the proposed CTR mode.

## 6. Conclusions and Discussion

In this paper, we have presented a CTR mode of the original block cipher based on matrices. Interestingly enough, instead of using multiple rounds to obtain a ciphertext, we propose a strongly nonlinear MPF mapping. Our previous results together with our current findings show a promising future for the presented ciphers, as they are perfectly secure, which had previously been proven only for the OTP technique. In this paper, we have explored the resistance of our proposal to passive attacks; however, there is a great deal of work yet to be done. At the moment, we have introduced the basic idea of MPF application for the counter mode of encryption. It now makes sense to work towards enhancements of the original idea to make our proposal impervious to active attacks.

Interestingly, in the present paper we have demonstrated a way to construct a working block cipher using a non-commuting platform group. Despite the fact that the associativity property (1) is not satisfied, we were able to define a suitable template for the power matrix $\mathbf{Y}$, which allowed us to overcome this feature of MPF. Note, however, that if the defined constraints on matrix $\mathbf{Y}$ are neglected, the decryption function of the presented block cipher cannot be successfully used to restore the original plaintext.

The latter fact creates a rather interesting opportunity for our proposal, as discarding (or greatly loosening) the restrictions of the power matrix $\mathbf{Y}$ would make the encryption irreversible. Even though, as pointed out in [22], this change could be advantageous due to the PRP/PRF switching lemma, it is necessary to analyze the complexity of nonce collision problem, i.e., whether it is possible to effectively find two nonces which produce the same ciphertext matrix. If this problem can be easily solved, it would have a dire effect on the resistance of our proposal to all kinds of attacks.

**Author Contributions:** Conceptualization, A.M.; methodology, A.M. and M.L.; software, M.L.; validation, A.M., M.L. and E.S.; formal analysis, A.M.; investigation, M.L.; resources, A.M.; writing—original draft preparation, A.M.; writing—review and editing, A.M.; visualization, M.L.; supervision, E.S. 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. Katz, J.; Lindell, Y. *Introduction to Modern Cryptography*; CRC Press: London, UK, 2020.
3. Stallings, W. NIST Block Cipher Modes of Operation for Confidentiality. *Cryptologia* **2010**, *34*, 163–175. [CrossRef]
4. Diffie, W.; Hellman, M.E. Privacy and Authentication: An Introduction to Cryptography. *Proc. IEEE* **1979**, *67*, 397–427. [CrossRef]
5. Lipmaa, H.; Rogaway, P.; Wagner, D. Comments to NIST Concerning AES-Modes of Operations: CTR-Mode Encryption. 2000. Available online: https://csrc.nist.rip/groups/ST/toolkit/BCM/documents/proposedmodes/ctr/ctr-spec.pdf (accessed on 15 September 2022).
6. McGrew, D.A.; Jose, S.; Viega, J. The Galois/Counter Mode of Operation (GCM). Available online: https://csrc.nist.rip/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-spec.pdf (accessed on 15 September 2022).
7. Dworkin, M.J. *Sp 800-38d. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*; NIST: Gaithersburg, MD, USA, 2007.
8. Gueron, S.; Jha, A.; Nandi, M. Comet: Counter Mode Encryption with Authentication Tag. Submission to NIST Lightweight Cryptography Project. 2019. Available online: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/comet-spec.pdf (accessed on 15 September 2022).
9. Gueron, S. Counter Mode for Long Messages and a Long Nonce. In Proceedings of the Cyber Security, Cryptology, and Machine Learning, Virtual, 30 June–1 July 2022; Dolev, S., Katz, J., Meisels, A., Eds.; Springer International Publishing: Cham, Switzerland, 2022; pp. 224–231.
10. Ahmad, N.; Wei, L.M.; Hairol Jabbar, M. Advanced Encryption Standard with Galois Counter Mode Using Field Programmable Gate Array. *J. Phys. Conf. Ser.* **2018**, *1019*, 012008. [CrossRef]
11. Marsalek, A.; Kollmann, C.; Zefferer, T.; Teufl, P. Unleashing the Full Potential of Blockchain Technology for Security-Sensitive Business Applications. In Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea, 14–17 May 2019; pp. 394–402.
12. Hammi, M.T.; Bellot, P.; Serhrouchni, A. BCTrust: A Decentralized Authentication Blockchain-Based Mechanism. In Proceedings of the 2018 IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, Spain, 15–18 April 2018; pp. 1–6.
13. Khaing, M.T.; Aye, Z.M. Image Encryption Based on AES Stream Cipher in Counter Mode. Ph.D. Thesis, University of Computer Studies, Mawlamyine, Myanmar, 2009.
14. Mahdi, M.S.R.; Aziz, M.M.A.; Mohammed, N.; Jiang, X. Privacy-Preserving String Search on Encrypted Genomic Data Using a Generalized Suffix Tree. *Inform. Med. Unlocked* **2021**, *23*, 100525. [CrossRef]
15. Dindiene, L.; Mihalkovich, A.; Luksys, K.; Sakalauskas, E. Matrix Power Function Based Block Cipher Operating in CBC Mode. *Mathematics* **2022**, *10*, 2123. [CrossRef]
16. Sakalauskas, E.; Dindienė, L.; Kilčiauskas, A.; Lukšys, K. Perfectly Secure Shannon Cipher Construction Based on the Matrix Power Function. *Symmetry* **2020**, *12*, 860. [CrossRef]
17. Mihalkovich, A.; Levinskas, M.; Makauskas, P. MPF Based Symmetric Cipher Performance Comparison to AES and TDES. *Math. Model. Eng.* **2022**, *8*, 15–25. [CrossRef]
18. Grundman, H.; Smith, T. Automatic Realizability of Galois Groups of Order 16. *Proc. Amer. Math. Soc.* **1996**, *124*, 2631–2640. [CrossRef]
19. Mihalkovich, A. On the Associativity Property of MPF over M16. *Liet. Mat. Rinkinys Liet. Mat. Draugijos Darbai. Ser. A* **2018**, *59*, 7–12. [CrossRef]
20. 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]
21. Grundman, H.G.; Smith, T.L. Galois Realizability of Groups of Order 64. *Centr. Eur. J. Math.* **2010**, *8*, 846–854. [CrossRef]
22. Bellare, M.; Rogaway, P. Introduction to Modern Cryptography. Available online: http://almuhammadi.com/sultan/crypto_books/BR.2005.pdf (accessed on 11 August 2022).