mathematics

MDPI

Article

Matrix Power Function Based Block Cipher Operating in CBC Mode

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

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

* Correspondence: aleksejus.michalkovic@ktu.lt

† These authors contributed equally to this work.

Abstract: In our previous study, we proposed a perfectly secure Shannon cipher based on the so-called matrix power function. There we also introduced a concept of single round symmetric encryption, i.e., we used the matrix power function together with some rather simple operations to define a three-step encryption algorithm that needs no additional rounds. Interestingly enough, the newly proposed Shannon cipher possesses the option of parallelization—an important property of efficiently performing calculations using several processors. Relying on our previous proposal, in this study we introduce a concept of a one round block cipher, which can be used to encrypt an arbitrary large message by dividing it into several blocks. In other words, we construct a block cipher operating in cipher block chaining mode on the basis of the previously defined Shannon cipher. Moreover, due to the perfect secrecy property of the original algorithm, we show that our proposal is able to withstand the chosen plaintext attack.

Keywords: chosen plaintext attack; CBC mode; symmetric encryption; matrix power function; perfect secrecy

MSC: 94A60

Citation: Dindiene, L.; Mihalkovich, A.; Luksys, K.; Sakalauskas, E. Matrix Power Function Based Block Cipher Operating in CBC Mode. *Mathematics* **2022**, *10*, 2123. https://doi.org/10.3390/math10122123

Academic Editor: Sergey Bezzateev

Received: 18 March 2022
Accepted: 21 April 2022
Published: 18 June 2022

1. Introduction

Since ancient times, people have used symmetric cryptography to encrypt data. Over many centuries, this branch of modern cryptography has greatly evolved. Nowadays, all the symmetric ciphers either operate on fixed-length blocks of bits or create a keystream to be combined with the initial plaintext. These approaches to data encryption are called block ciphers and stream ciphers, respectively.

The concept of a symmetric cipher is generally defined as a triplet $(Gen(), Enc(), Dec())$, where $Gen()$ is a key generation function, $Enc()$ and $Dec()$ are encryption and decryption functions, respectively [1]. The major requirement of a symmetric encryption scheme is the following:

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

i.e., decryption function correctly restores the message μ using the same key k. Any properly working symmetric cipher must satisfy this requirement. Proving the correctness of any symmetric cipher relies on verifying identity (1).

So far, the majority of the widely used block ciphers use at least several rounds to encrypt the secret data. Usually, operations used in these ciphers (e.g., AES) are fairly simple (some of them even linear) and could be easily inverted if a single round was executed. Hence, the security of these algorithms relies on the combination of fairly simple steps performed multiple times.

There are two common approaches to the design of symmetric block cipher. One of them is the Feistel network developed in the last quarter of the 20th century [2]. Noticeable ciphers, such as DES, Camelia, Blowfish, and CAST-128, were constructed using this technique. The general idea behind the Feistel network is to divide the block to be encrypted into two equal parts L_0, R_0 and manipulate them using some round function F and round sub-keys $K_0, K_1, \ldots, K_n$ to calculate the ciphertext, which is usually defined as a concatenation of R_{n+1} and L_{n+1}. Depending on the complexity of the scheme the number of rounds is chosen carefully and can vary from being quite small (e.g., 8) to several dozens (e.g., 64 or 72). The more rounds the greater security—that is the general rule.

An alternative approach is designing the substitution-permutation (SP) network. The Rijndael block cipher known as the AES is perhaps the most popular example of this type. It superseded the DES and became the standard recommended by NIST for data encryption in 2002 [3]. The most common version of AES uses a 128-bit block and 10, 12, or 14 rounds depending on the key size. Another example is the Kuznyechik symmetric block cipher developed in 2015 [4]. It was later standardized by the Russian government and replaced the previously used scheme based on the Feistel network. The SP network is usually designed by defining the so-called substitution boxes (S-boxes) and permutation boxes (P-boxes). These boxes are commonly introduced via mathematical functions and logical operations, e.g., shifting operation and the bitwise addition (XOR).

However, since the operations themselves are rather simple, the cryptanalysis of these block ciphers is a non-stopping field of research. Over recent years many attacks on the developed ciphers were published, e.g., [5–7], one of the more notable ones was proposed by Courtois whose goal was to break the AES cipher [8]. It was later proven to be impractical.

In the most general form any good cipher should act as a one-way function (OWF), i.e., calculating the argument x of the function f given its value $f(x)$ without knowing some secret key should be an impossible task. To put it simply the ciphertext c should look completely random to any adversary even if he knows the original message μ. In fact, a fundamental relation between OWFs and pseudorandom generators was revealed by Yao in [9], where he proved that OWFs exist if, and only if, the pseudorandom generators exist.

In the realm of the symmetric ciphers, one particular example stands out. This simple technique developed by Vernam in 1917 is now commonly referred to as the one-time pad. The reason behind this is the property of perfect secrecy, which guarantees that no information about the encrypted plaintext is leaked by the ciphertext. Formally perfect secrecy can be defined as follows (however, there are other equivalent definitions) [1,10]:

Definition 1. *The symmetric cipher $\varepsilon = (Enc(k, \mu), Dec(k, c))$ is perfectly secure if for any fixed values μ_0, c_0 the following probabilities are equal:*

$$\Pr(c = c_0 | \mu = \mu_0) = \Pr(c = c_0).$$

This definition is due to Shannon who has also shown that the one-time pad is perfectly secure [11]. Together the result by Yao and this definition explain why it is essential for a secure cipher to possess good properties of randomness. Notably, the link between OWF and pseudorandom generators is reflected in the avalanche effect and the bit independence criterion. Some work in this area was previously performed in [12] for our scheme.

Interestingly enough, the one-time pad uses a single round and a simple XOR operation to encrypt a plaintext μ. Though the idea of using this technique is theoretical (at least for the most part) we can see that the keys of modern symmetric block cipher are no shorter than the block size, thus staying true to the original idea by Vernam. For example, AES encrypts 128-bit block using 128, 192, or 256-bit keys [3]. Our cipher follows the same pattern, i.e., the secret key is longer than the size of a block.

The main goal is to propose a symmetric cipher based on the conjectured one-way function (OWF). During our previous research, we proved that a certain realization of asymmetric

encryption based on our function is NP-complete [13]. It is conjectured that such cryptographic primitives could be resistant to algebraic analysis and quantum cryptanalysis.

Despite the fact that we are currently working on a symmetric encryption scheme we think that its security may prove to be a hard nut to crack. In particular, we aim to make our block cipher perfectly secure while also achieving several other important properties which allow our proposal to be used as a basis for the cipher block chaining (CBC) mode. At the same time in Section 3, we introduce modifications of the initial cipher making it more flexible. Furthermore, by generalizing algebraic structures we gain a higher encryption speed of our proposal. We prove the perfect secrecy property of our block cipher in Section 5.

In Section 6 we prove that our block cipher is secure against CPA. As demonstrated by Boneh and Shoup in [10] this fact is directly linked to the perfect secrecy property of the presented Shannon cipher. Due to made modifications we also inspect their influence on the perfect secrecy property. We end our paper by presenting conclusions and a list of references.

2. Our Previous Work

Our first attempt at designing a symmetric block cipher was made in 2007 when our research group published a paper [14]. There we have proposed a technique to construct an S-box based on at that time newly defined matrix power function (MPF)—a non-linear matrix mapping $Mat_m(\mathbb{R}) \times Mat_m(\mathbb{R}) \mapsto Mat_m(\mathbb{S})$, where $\mathbb{S}$ is a multiplicative semigroup, $\mathbb{R}$ is a ring of integers and $Mat_m(\cdot)$ denotes a ring of $m \times m$ matrices with entries selected from the specified algebraic structure. We denote the MPF in the following way:

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

where $\mathbf{X}, \mathbf{Y} \in Mat_m(\mathbb{R})$ and $\mathbf{W}, \mathbf{E} \in Mat_m(\mathbb{S})$. Usually, in our research, we refer to $\mathbf{X}, \mathbf{Y}$ as power matrices. We also refer to $\mathbf{W}$ as a base matrix and to $\mathbf{E}$ as the matrix exponent. Furthermore, we call $Mat_m(\mathbb{S})$ a platform semigroup and $Mat_m(\mathbb{R})$ a power ring. Each entry of matrix exponent $\mathbf{E}$ is calculated in the following way:

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

We can see from the latter expression that MPF bears a strong resemblance to classical matrix multiplication. In fact, explicit expressions of the entries of matrix $\mathbf{E}$ in the case of 2×2 matrices are presented below:

$$\begin{aligned}
e_{11} &= w_{11}^{x_{11}y_{11}} w_{12}^{x_{11}y_{21}} w_{21}^{x_{12}y_{11}} w_{22}^{x_{12}y_{21}};\\
e_{12} &= w_{11}^{x_{11}y_{12}} w_{12}^{x_{11}y_{22}} w_{21}^{x_{12}y_{12}} w_{22}^{x_{12}y_{22}};\\
e_{21} &= w_{11}^{x_{21}y_{11}} w_{12}^{x_{21}y_{21}} w_{21}^{x_{22}y_{11}} w_{22}^{x_{22}y_{21}};\\
e_{22} &= w_{11}^{x_{21}y_{12}} w_{12}^{x_{21}y_{22}} w_{21}^{x_{22}y_{12}} w_{22}^{x_{22}y_{22}}.
\end{aligned}$$

Properties similar to the ones of matrix multiplication also hold for MPF if the platform semigroup $\mathbb{S}$ is commuting. However, this may not be the case for the non-abelian platform semigroups.

Note that here and onwards all the matrices are denoted by uppercase bold letters whereas all the scalars and bitstrings are denoted by lowercase italic letters. All the sets are denoted by uppercase blackboard bold letters, e.g., $\mathbb{S}, \mathbb{R}$, etc.

However, we had to apply restrictions on the plaintext matrix form to avoid the potentially harmful property of MPF, i.e., the base matrix $\mathbf{W}$ cannot contain any zero entries, since otherwise the MPF value matrix E is a zero matrix. Here, we plan to eliminate this constraint while also avoiding zero entries in the base matrix. Furthermore, we use a more general approach to construct a valid block cipher.

Recently in our paper [15] we introduced a new block cipher and proposed a concept of single round symmetric encryption based on the MPF mapping. However, there we used low cardinality algebraic structures. For this reason, our cipher lacked the flexibility necessary for the implementation of our scheme in practice. Furthermore, our investigation in [12] has shown that the statistical properties of the proposed scheme leave much to be desired for the parameters introduced in [15]. However, that very same investigation revealed that extra flexibility in the main parameters significantly improves the statistical properties of our scheme. As such we consider the paper [15] a first draft for constructing a symmetric block cipher. To be self-contained we present the encryption and decryption algorithms of our original proposal.

Let $\mathbf{M}$ be the initial message converted to matrix form. To encrypt the initial message we use a secret key—a pair of matrices $(\mathbf{X}, \mathbf{Y})$, where $\mathbf{X}, \mathbf{Y} \in Mat_m(\mathbb{Z}_3)$, $\mathbf{X}$ does not contain any zero entries and $\mathbf{Y}$ is invertible. The encryption algorithm consists of the following steps:

$$\begin{aligned} \mathbf{S_1} &= \mathbf{X} + \mathbf{M}; \\ \mathbf{S_2} &= F(\mathbf{X}) \odot {}^{\mathbf{Y}}F(\mathbf{S_1})^{\mathbf{Y}}; \\ \mathbf{S} = \mathbf{S_3} &= F^{-1}(\mathbf{S_2}) + \mathbf{X}, \end{aligned} \tag{1}$$

where $F(\mathbf{X}) : Mat_m(\mathbb{Z}_3) \mapsto Mat_m(\mathbb{G}_3)$ is a publicly known one-to-one mapping which replaces entries of matrix $\mathbf{X}$ with elements from $\mathbb{G}_3$—a Sylow subgroup of $\mathbf{Z}_7$. Clearly, $F^{-1}(\mathbf{S_2})$ is the inverse transformation. We use $\odot$ to denote Hadamard product of two matrices.

Recall that the Hadamard product is simply the entry-wise multiplication of two matrices, much like the addition operation. As such the properties of the Hadamard product are similar to the regular matrix addition with the neutral element equal to the unit matrix $\mathbf{1}$, i.e., each entry of this matrix is equal to 1. Moreover, we can define the inverse of a matrix $\mathbf{A}$ in Hadamard sense as a matrix $\mathbf{B}$, such that $\mathbf{A} \odot \mathbf{B} = \mathbf{1}$. We denote $\mathbf{B} = \mathbf{A}^H$.

Let us also briefly revise the notion of the Sylow subgroup. For simplicity, let us focus on the multiplicative ring of integers $\mathbb{Z}_p$, where $p = kq + 1$, p and q are primes and $\gcd(k, q) = 1$. Then, the group $\mathbb{G}_q$ is called a Sylow subgroup if the multiplicative order of its generator g equals q, i.e., $g^q \equiv 1 \bmod p$. In fact, due to the Lagrange theorem since q is prime, every element of $\mathbb{G}_q$ generates the whole group apart from 1. Sylow subgroups can also be defined in a more general case as well, but our research does not require considering it.

The decryption algorithm is simply a reversal of each presented step and is as follows:

$$\begin{aligned} \mathbf{D_1} &= \mathbf{S} - \mathbf{X}; \\ \mathbf{D_2} &= {}^{\mathbf{Y}^{-1}}\left(F(\mathbf{D_1}) \odot F(\mathbf{X})^H\right)^{\mathbf{Y}^{-1}}; \\ \mathbf{M} = \mathbf{D_3} &= F^{-1}(\mathbf{D_2}) - \mathbf{X}, \end{aligned} \tag{2}$$

where $F(\mathbf{X})^H$ is the inverse matrix in a Hadamard sense. It can be easily shown that $\mathbf{D_1} = \mathbf{S_2}$ and $\mathbf{D_2} = F(\mathbf{S_1})$. Hence, the proposed cipher works correctly. Explicit proof of correctness is presented in [15].

A beneficial feature of MPF which distinguishes our scheme from others is that it is a highly non-linear function. For this reason, differential and linear cryptanalysis is assumed to be inefficient.

In our previous publication, we proved that the proposed Shannon cipher is perfectly secure; hence, it does not leak any information about the secret data.

In this paper we take the second major step, i.e., we present a block cipher based on our previous scheme which operates in CBC mode.

3. Modifications of the Initial Cipher

In this section, we consider some important modifications of the cipher presented in [15]. The first major change we make is the introduction of a prime integer q which

denotes the size of the Sylow group $\mathbb{G}_q$. Recall that the essential property of this group is that every element $g \in \mathbb{G}_q$ such that $g \neq 1$ generates the whole group. This property of the Sylow group $\mathbb{G}_q$ means that for a uniformly chosen $\alpha \in \mathbb{Z}_q$ and a fixed element $a \in \mathbb{G}_q$ we have:

$$\Pr(g^\alpha = a) = \frac{1}{q},$$

where we used the notation $\Pr(x = x_0)$ to denote the probability that a random variable x equals a fixed value x_0.

We use $\mathbb{G}_q$ as a platform group and $\mathbb{Z}_q$ as a power ring of the MPF. Consequently, we define a one-to-one mapping $f : \mathbb{Z}_q \mapsto \mathbb{G}_q$ and its matrix analogue F as an entry-wise application of f. Then by our construction, we have:

$$\Pr(x = x_0) = \Pr(f(x) = f(x_0)),$$

where $x \in \mathbb{Z}_q$ is a random variable and $x_0 \in \mathbb{Z}_q$ is a fixed value. Obviously $f(x)$ and $f(x_0)$ are respectively a random variable and a fixed value in a Sylow group $\mathbb{G}_q$. Hence the mapping f as well as its inverse $f^{-1} : \mathbb{G}_q \mapsto \mathbb{Z}_q$ preserves all the probabilities.

Furthermore, in step 2 of our cipher we introduce an extra matrix $\mathbf{Z}$ with entries randomly chosen from the platform group $\mathbb{G}_q$. In other words, Step 2 of our cipher now looks as follows:

$$\mathbf{S_2} = \mathbf{Z} \odot {}^{\mathbf{Y}}F(\mathbf{S_1})^{\mathbf{Y}},$$

where matrices $\mathbf{S_1}$ and $\mathbf{Y}$ as well as mapping F are defined as above. Hence, the secret key is now $\vec{\mathbf{K}} = \{\mathbf{X}, \mathbf{Y}, \mathbf{Z}\}$.

By applying these modifications we are able to enlarge the set of possible messages while keeping the matrix order m fairly small. However, for practical purposes we may want to limit the entries of matrix $\mathbf{M}$ by the number $2^{\lfloor \log_2 q \rfloor}$, i.e., by the largest power of 2, which does not exceed q. We do not consider this limitation here and leave the investigation of its effect for our future research.

Furthermore, because matrix $\mathbf{Z}$ is chosen independently from other matrices, the reintroduced matrix $\mathbf{S_2}$ sufficiently contributes to the proof of perfect secrecy property of the block cipher.

It is also important to note that it is possible to implement extra precautions which can contribute to the overall security of our block cipher. One of these precautions is the procedure of transformation of the initial message to its matrix form. Although important, this procedure does not in any way affect the proof we present in Section 5.

4. CBC Mode of Our Cipher

Using the previously defined scheme for a single message in this section, we present the CBC mode of our cipher. Because we can encrypt at most $m^2 \cdot t$ bits, where $t = \lfloor \log_2 q \rfloor$, we split the giant bit string into parts of length $m^2 \cdot t$. We also add junk symbols at the end of the last part, if needed. Moreover, we split each of the obtained parts into smaller chunks as discussed above to perform a transformation of the original plaintext to its matrix form.

Let us denote the matrix form of each plaintext part by $\mathbf{M}_i$ and the obtained ciphertext matrix by $\mathbf{C}_i$ with $\mathbf{C}_0$ denoting the publicly known initialization matrix. Each block $\mathbf{M}_i$ is encrypted using the key $\vec{\mathbf{K}} = \{\mathbf{X}, \mathbf{Y}, \mathbf{Z}\}$, where $\mathbf{X} \in Mat_m(\mathbb{Z}_{q\setminus 0})$, $\mathbf{Y} \in Mat_m(\mathbb{Z}_q)$ and $\mathbf{Z} \in Mat_m(\mathbb{G}_q)$. We can encrypt the whole message μ divided into blocks by executing the following scheme:

$$\begin{aligned} \mathbf{S}_{1i} &= \mathbf{M}_i + \mathbf{C}_{i-1}; \\ \mathbf{S}_{2i} &= \mathbf{Z} \odot {}^{\mathbf{Y}}F(\mathbf{S}_{1i})^{\mathbf{Y}}; \\ \mathbf{C}_i = \mathbf{S}_{3i} &= F^{-1}(\mathbf{S}_{2i}) + \mathbf{X}, \end{aligned} \tag{3}$$

where $\mathbf{S}_{1i}, \mathbf{S}_{2i}$ and $\mathbf{S}_{3i}$ are intermediate matrices obtained during the encryption of the i-th block $\mathbf{M}_i$. Hence the encryption function is:

$$Enc(\mathbf{M}_i, (\mathbf{X}, \mathbf{Y}, \mathbf{Z})) = F^{-1}(\mathbf{Z} \odot {}^{\mathbf{Y}}F(\mathbf{M}_i + \mathbf{C}_{i-1})^{\mathbf{Y}}) + \mathbf{X}.$$

Each encrypted block $\mathbf{C}_i$ is converted to a bit string by concatenating the obtained entries in their bit representations. Hence, the final result, i.e., the ciphertext of the original massive message, is the following bit string:

$$\begin{aligned} c = c_{011} \parallel c_{012} \parallel \ldots \parallel c_{01m} \parallel c_{021} \parallel c_{022} \parallel \ldots \parallel c_{0mm} \parallel \\ \parallel c_{111} \parallel \ldots \parallel c_{1mm} \parallel \ldots \parallel c_{Nmm}, \end{aligned} \tag{4}$$

where N is the number of blocks and $\parallel$ stands for the concatenation operation. Hence we see that the obtained ciphertext consists of $N + 1$ blocks of size $m^2 t$ each.

The decryption algorithm is similar to the previously presented encryption procedure and consists of the following steps:

$$\begin{aligned} \mathbf{D}_{1i} &= \mathbf{C}_i - \mathbf{X}; \\ \mathbf{D}_{2i} &= {}^{\mathbf{Y}^{-1}}(F(\mathbf{D}_{1i}) \odot \mathbf{Z}^H)^{\mathbf{Y}^{-1}}; \\ \mathbf{D}_i = \mathbf{D}_{3i} &= F^{-1}(\mathbf{D}_{2i}) - \mathbf{C}_{i-1}, \end{aligned}$$

where $\mathbf{D}_{1i}, \mathbf{D}_{2i}$ and $\mathbf{D}_{3i}$ are intermediate matrices obtained during the decryption of the i-th block $\mathbf{C}_i$. Hence the decryption function is:

$$Dec(\mathbf{C}_i, (\mathbf{X}, \mathbf{Y}, \mathbf{Z})) = F^{-1}({}^{\mathbf{Y}^{-1}}(F(\mathbf{C}_i - \mathbf{X}) \odot \mathbf{Z}^H)^{\mathbf{Y}^{-1}}) - \mathbf{C}_{i-1}.$$

Now we prove the correctness of the decryption algorithm.

Clearly, all the blocks (i.e., $\mathbf{C}_i$'s) can be obtained from the ciphertext (4) by splitting it into N parts of length $m^2 \cdot t$. Then, it is easy to see that by subtracting $\mathbf{X}$ from the i-th block $\mathbf{C}_i$ we obtain matrix $F^{-1}(\mathbf{S}_{2i})$. Because $F(F^{-1}(\mathbf{S}_{2i}))$ is clearly equal to $\mathbf{S}_{2i}$, we can multiply this matrix by $\mathbf{Z}^H$ in the Hadamard sense to cancel matrix $\mathbf{Z}$ and hence we have:

$$\begin{aligned} F(\mathbf{D}_{1i}) \odot \mathbf{Z}^H = F(F^{-1}(\mathbf{S}_{2i})) \odot \mathbf{Z}^H = \mathbf{S}_{2i} \odot \mathbf{Z}^H = \\ = \mathbf{Z} \odot {}^{\mathbf{Y}}F(\mathbf{S}_{1i})^{\mathbf{Y}} \odot \mathbf{Z}^H = {}^{\mathbf{Y}}F(\mathbf{S}_{1i})^{\mathbf{Y}} \odot \mathbf{1} = {}^{\mathbf{Y}}F(\mathbf{S}_{1i})^{\mathbf{Y}}. \end{aligned}$$

Because $F(\mathbf{D}_{1i}) = F(F^{-1}(\mathbf{S}_{2i})) = \mathbf{S}_{2i}$. However, due to properties of MPF, by raising the obtained result to power matrix $\mathbf{Y}^{-1}$ on both sides we obtain:

$${}^{\mathbf{Y}^{-1}}({}^{\mathbf{Y}}F(\mathbf{S}_{1i})^{\mathbf{Y}})^{\mathbf{Y}^{-1}} = {}^{\mathbf{Y}^{-1}\mathbf{Y}}F(\mathbf{S}_{1i})^{\mathbf{Y}\mathbf{Y}^{-1}} = {}^{I}F(\mathbf{S}_{1i})^{I} = F(\mathbf{S}_{1i}).$$

Therefore, we see that:

$$\mathbf{D}_{2i} = {}^{\mathbf{Y}^{-1}}(F(\mathbf{D}_{1i}) \odot \mathbf{Z}^H)^{\mathbf{Y}^{-1}} = F(\mathbf{S}_{1i}).$$

Then, Because $F^{-1}(F(\mathbf{S}_{1i})) = \mathbf{S}_{1i}$, by subtracting $\mathbf{C}_{i-1}$ we obtain the block $\mathbf{M}_i$—a matrix form of a part of the original plaintext as desired.

5. Perfect Secrecy of the Block Cipher

Referencing the definition of the perfect secrecy property proposed by Boneh and Shoup (2), we formulate the following important result:

Proposition 1. *The block cipher with the proposed Algorithm (3) is perfectly secure, i.e., the following properties hold:*

$$\begin{aligned}
\Pr(\mathbf{S}_{1i} = \mathbf{S}_{1i}^0) &= \Pr(\mathbf{S}_{1i} = \mathbf{S}_{1i}^0 | \mathbf{M}_i = \mathbf{M}_i^0) = \left(\tfrac{1}{q}\right)^{m^2}; \\
\Pr(\mathbf{S}_{2i} = \mathbf{S}_{2i}^0) &= \Pr(\mathbf{S}_{2i} = \mathbf{S}_{2i}^0 | \mathbf{M}_i = \mathbf{M}_i^0) = \left(\tfrac{1}{q}\right)^{m^2}; \\
\Pr(\mathbf{S}_{3i} = \mathbf{S}_{3i}^0) &= \Pr(\mathbf{S}_{3i} = \mathbf{S}_{3i}^0 | \mathbf{M}_i = \mathbf{M}_i^0) = \left(\tfrac{1}{q}\right)^{m^2}.
\end{aligned} \tag{5}$$

Note that because there are many lower indices involved in notation, throughout this section we use an upper index 0 to indicate some fixed value (matrix or a single entry) defined in the appropriate set or an algebraic structure as was performed in expression (5).

As mentioned previously, the matrix X does not contain any zero entries. We use notation $\mathbb{Z}_{q\setminus 0}$ to denote a set of integers between 1 and $q-1$, i.e., $\mathbb{Z}_{q\setminus 0} = \mathbb{Z}_q \setminus \{0\}$. Note that we do not perform any operations with the elements of $\mathbb{Z}_{q\setminus 0}$. Hence, our motivation for the chosen notation is to distinguish this set from a widely known multiplicative group of integers $\mathbb{Z}_q^*$, i.e., we do not confuse the reader with the multiplicative or any other nature of the set $\mathbb{Z}_{q\setminus 0}$.

Before elaborating the main proof, we emphasize some initial relationships between matrices of the cipher (3). Initialization matrix $\mathbf{C}_0$ is independent of key and message matrices, with mutually independent entries. Key matrices $\mathbf{X}$, $\mathbf{Y}$, $\mathbf{Z}$ and their entries are mutually independent. Entries of $\mathbf{C}_0$ and $\mathbf{X}$ are uniformly distributed in $\mathbb{Z}_q$. Entries of $\mathbf{Y}$ are uniformly distributed in $\mathbb{Z}_{q\setminus 0}$. Entries of $\mathbf{Z}$ are uniformly distributed in $\mathbb{G}_q$.

Proof. The proof of the proposition is essentially based on the idea presented in [15]. We split the proof into three steps. We show that entries of matrices $\mathbf{S_1}, \mathbf{S_2}$ and $\mathbf{S_3}$ of each block are uniformly distributed in an appropriate structure, that they are independent of message matrix $\mathbf{M}$ and that all the entries are mutually independent.

All initial assumptions and proved statements on the independence of matrices are used without explicit emphasis to avoid lots of repetitive statements. The proof of each matrix's independence is presented in a separate subsection to retain the structure of the section.

Proving the independence, we rely on one of the main formula of probabilities: if two variables X and Y are independent, then $\Pr(X|Y) = \frac{\Pr(X,Y)}{\Pr(Y)} = \Pr(X)$, i.e., $\Pr(X,Y) = \Pr(X) \cdot \Pr(Y)$. In a further proof of independence, we refer to the latter formula.

For the simplicity of proving the above-listed independence, let us take the first block of the cipher (3). The proof of its independence is closely related to the proof of Theorem 1 in [15], but in our case, we have an extended structure from the set of three elements to the set which consists of q elements. Probabilities of the first block are used in the proof of further blocks. Therefore, we present the detailed proof here.

Rewrite Equation (3) of the first (initial) block for each entry of matrices $(i, j = 1, \ldots, m)$:

$$\begin{aligned}
s_{11,ij} &= m_{1,ij} + c_{0,ij}; \\
s_{21,ij} &= z_{ij} \cdot \prod_{k=1}^{m} \prod_{l=1}^{m} (f(s_{11,kl}))^{y_{ik} y_{lj}}; \\
c_{1,ij} &= s_{31,ij} = f^{-1}(s_{21,ij}) + x_{ij}.
\end{aligned}$$

□

5.1. $\mathbf{S}_{11}$ Independence

Knowing that entries of the initialization matrix are uniformly distributed random variables independent of $\mathbf{M}$, for fixed $s^0_{11,ij} \in \mathbb{Z}_q$ we have:

$$\begin{aligned} \Pr(s_{11,ij} = s^0_{11,ij}) = \Pr(c_{0,ij} = s^0_{11,ij} - m_{1,ij}) = \\ = \frac{1}{q} \underbrace{\sum_{m_0 \in \mathbb{Z}_q} \Pr(m_{1,ij} = m_0)}_{=1} = \frac{1}{q}, \end{aligned} \tag{6}$$

i.e., entries $s_{11,ij}$ are uniformly distributed in $\mathbb{Z}_q$. The summation of the probabilities to all possible values gives us the total probability, which is equal to 1. This fact is noted in the Equation (6). This notation will be used in the further part of the proof.

It is easy to see, that

$$\begin{aligned} \Pr(s_{11,ij} = s^0_{11,ij}, m_{1,ij} = m^0_{1,ij}) = \\ = \Pr(c_{0,ij} = s^0_{11,ij} - m^0_{1,ij}, m_{1,ij} = m^0_{1,ij}) = \\ = \frac{1}{q} \Pr(m_{1,ij} = m^0_{1,ij}) = \\ = \Pr(s_{11,ij} = s^0_{11,ij}) \Pr(m_{1,ij} = m^0_{1,ij}), \end{aligned} \tag{7}$$

i.e., entries $s_{11,ij}$ are independent of entries $m_{1,ij}$. Then we have

$$\begin{aligned} \Pr(\cap^m_{i,j=1}\{s_{11,ij} = s^0_{11,ij}\}) = \\ = \Pr(\cap^m_{i,j=1}\{c_{0,ij} + m_{1,ij} = s^0_{11,ij}\}) = \\ = \sum_{m^0_{ij} \in \mathbb{Z}_q} \Pr(\cap^m_{i,j=1}\{c_{0,ij} = \underbrace{s^0_{11,ij} - m^0_{1,ij}}_{\in \mathbb{Z}_q}\}, \\ \cap^m_{i,j=1}\{m_{1,ij} = m^0_{1,ij}\}) = \left(\frac{1}{q}\right)^{m^2} \cdot \\ \cdot \underbrace{\sum_{m^0_{1,ij} \in \mathbb{Z}_q} Pr(\cap^m_{i,j=1}\{m_{1,ij} = m^0_{1,ij}\})}_{=1} = \left(\frac{1}{q}\right)^{m^2}. \end{aligned} \tag{8}$$

i.e., entries $s_{11,ij}$ are independent of each other.

5.2. $\mathbf{S}_{21}$ Independence

Before proving the uniformity of matrix $\mathbf{S}_{21}$, we need the following corollary, which can be easily verified using the results of Lemma 2 and Lemma 3 in [15].

Corollary 1. *Let random variables $w_1, w_2, \ldots, w_n$ be independent and uniformly distributed in $\mathbb{G}_q$, $v_1, v_2, \ldots, v_n$ be independent and uniformly distributed in $\mathbb{Z}_{q\setminus 0}$, then the product $w_1^{v_1} \cdot w_2^{v_2} \cdot \cdots \cdot w_n^{v_n}$ is uniformly distributed in $\mathbb{G}_q$.*

Because entries of $\mathbf{S}_{11}$, $\mathbf{Z}$ and $\mathbf{X}$ are independent and uniformly distributed in the appropriate structure, Corollary 1 implies that entries of $\mathbf{S}_{21}$ are uniformly distributed in $\mathbb{G}_q$:

$$\Pr(s_{21,ij} = s^0_{21,ij}) = \frac{1}{q} \tag{9}$$

and independent of $\mathbf{M}_1$:

$$\Pr(s_{21,ij} = s^0_{21,ij}, \cap_{i,j=1}^m \{m_{1,ij} = m^0_{ij}\}) =$$
$$= \Pr(z_{ij} \prod_{k=1}^m \prod_{l=1}^m (f(s_{11,kl}))^{y_{ik}y_{lj}} = s^0_{21,ij}, \cap_{i,j=1}^m \{m_{1,ij} = m^0_{1,ij}\}) =$$
$$\sum_{c^0_{0,kl} \in \mathbb{Z}_q} \sum_{y^0_{kl} \in \mathbb{Z}_{q \setminus 0}} \Pr(z_{ij} = \underbrace{s^0_{21,ij} (\prod_{k=1}^m \prod_{l=1}^m (f(c^0_{0,kl} + m^0_{1,kl}))^{y^0_{ik} y^0_{lj}})^{-1}}_{\in \mathbb{G}_q},$$
$$\cap_{i,j=1}^m \{m_{1,ij} = m^0_{1,ij}\}, \cap_{k,l=1}^m \{c_{0,kl} = c^0_{0,kl}\}, \cap_{k,l=1}^m \{y_{kl} = y^0_{kl}\}) =$$
$$= \frac{1}{q} \cdot \Pr(\cap_{i,j=1}^m \{m_{1,ij} = m^0_{1,ij}\}) \cdot \underbrace{\sum_{c^0_{0,kl} \in \mathbb{Z}_q} \Pr(\cap_{k,l=1}^m \{c_{0,kl} = c^0_{0,kl}\})}_{=1} \cdot$$
$$\cdot \underbrace{\sum_{y^0_{kl} \in \mathbb{Z}_{q \setminus 0}} \Pr(\cap_{k,l=1}^m \{y_{kl} = y^0_{kl}\})}_{=1} = \frac{1}{q} \cdot \Pr(\cap_{i,j=1}^m \{m_{1,ij} = m^0_{1,ij}\}) =$$
$$= \Pr(s_{21,ij} = s^0_{21,ij}) \Pr(\cap_{i,j=1}^m \{m_{1,ij} = m^0_{ij}\}). \tag{10}$$

Entries of $\mathbf{S}_{21}$ are independent of each other:

$$\Pr(\cap_{i,j=1}^m \{s_{21,ij} = s^0_{21,ij}\}) =$$
$$= \Pr(\cap_{i,j=1}^m \{z_{ij} \prod_{k=1}^m \prod_{l=1}^m (f(s_{11,kl}))^{y_{ik}y_{lj}} = s^0_{ij}\}) =$$
$$= \sum_{s^0_{11,kl} \in \mathbb{Z}_q} \sum_{y^0_{ij} \in \mathbb{Z}_{q \setminus 0}} \Pr\big(\cap_{i,j=1}^m \{z_{ij} = \underbrace{s_{21,ij} (\prod_{k=1}^m \prod_{l=1}^m (f(s^0_{11,kl}))^{y^0_{ik} y^0_{lj}})^{-1}}_{\in \mathbb{G}_q}\},$$
$$\cap_{k,l=1}^m \{s_{11,kl} = s^0_{11,kl}\}, \cap_{i,j=1}^m \{y_{ij} = y^0_{ij}\}) = \left(\frac{1}{q}\right)^{m^2}, \tag{11}$$

where $\mathbf{S}_{11}$ and $\mathbf{Z}$ are independent:

$$\Pr(s_{11,ij} = s^0_{11,ij}, z_{ij} = z^0_{ij}) = \sum_{m^0_{1,ij} \in \mathbb{Z}_q} \Pr(c_{0,ij} = \underbrace{s^0_{11,ij} - m^0_{1,ij}}_{\in \mathbb{Z}_q},$$
$$z_{ij} = z^0_{ij}, m_{1,ij} = m^0_{1,ij}) = \frac{1}{q} \Pr(z_{ij} = z^0_{ij}) =$$
$$= \Pr(s_{11,ij} = s^0_{11,ij}) \Pr(z_{ij} = z^0_{ij}). \tag{12}$$

5.3. $\mathbf{S}_{31} = \mathbf{C}_1$ *Independence*

Entries of $\mathbf{C}_1 = \mathbf{S}_{31}$ are uniformly distributed in $\mathbb{Z}_q$:

$$\Pr(s_{31,ij} = s_{30}) = \Pr(f^{-1}(s_{21,ij}) = s_{30} - x_{ij}) = \frac{1}{q} \underbrace{\sum_{x^0_{ij} \in \mathbb{Z}_q} Pr(x_{ij} = x^0_{ij})}_{=1} = \frac{1}{q}, \tag{13}$$

because, similarly as in (10), $\mathbf{S}_{21}$ is independent of $\mathbf{X}$:

$$\Pr(s_{31,ij} = s_{30}) = \Pr(f^{-1}(s_{21,ij}) = s_{30} - x_{ij}) = \\ = \frac{1}{q} \underbrace{\sum_{x_{ij}^0 \in \mathbb{Z}_q} Pr(x_{ij} = x_{ij}^0)}_{=1} = \frac{1}{q}, \tag{14}$$

because, similarly as in (10), $\mathbf{S}_{21}$ is independent of $\mathbf{X}$:

$$\Pr(s_{21,ij} = s_{21,ij}^0, \cap_{i,j=1}^m \{x_{ij} = x_{ij}^0\}) = \\ = \Pr\left(z_{ij} \prod_{k=1}^m \prod_{l=1}^m (f(s_{11,kl}))^{y_{ik} y_{lj}} = s_{21,ij}^0,\right. \\ \left. \cap_{i,j=1}^m \{x_{ij} = x_{ij}^0\}\right) = \sum_{m_{1,ij}^0 \in \mathbb{Z}_q} \sum_{c_{0,kl}^0 \in \mathbb{Z}_q} \sum_{y_{ij}^0 \in \mathbb{Z}_{q \setminus 0}} Pr\Big(z_{ij} = \\ = s_{21,ij}^0 (\prod_{k=1}^m \prod_{l=1}^m (f(c_{0,kl}^0 + m_{1,kl}^0))^{y_{ik}^0 y_{lj}^0})^{-1}, \\ \cap_{i,j=1}^m \{x_{ij} = x_{ij}^0\}, \cap_{i,j=1}^m \{y_{ij} = y_{ij}^0\}, \cap_{i,j=1}^n \{m_{1,ij} = m_{1,ij}^0\}, \\ \cap_{k,l=1}^n \{c_{0,kl} = c_{0,kl}^0\}\Big) = \frac{1}{q} \Pr(\cap_{i,j=1}^m \{x_{ij} = x_{ij}^0\}) = \\ = \Pr(s_{21,ij} = s_{21,ij}^0) \Pr(\cap_{i,j=1}^m \{x_{ij} = x_{ij}^0\}). \tag{15}$$

$\mathbf{C}_1$ is independent of $\mathbf{M}_1$, because:

$$\Pr(s_{31,ij} = s_{31,ij}^0, \cap_{i,j=1}^m \{m_{1,ij} = m_{1,ij}^0\}) = \\ = \Pr(f^{-1}(s_{21,ij}) + x_{ij} = s_{31,ij}^0, \cap_{i,j=1}^n \{m_{1,ij} = m_{1,ij}^0\}) = \\ = \sum_{x_{ij}^0 \in \mathbb{Z}_q} \Pr(s_{21,ij} = f(s_{31,ij}^0 - x_{ij}^0), \cap_{i,j=1}^m \{m_{1,ij} = m_{1,ij}^0\}, \\ \cap_{i,j=1}^n \{x_{ij} = x_{ij}^0\}) = \\ = \frac{1}{q} \Pr(\cap_{i,j=1}^m \{m_{1,ij} = m_{1,ij}^0\}) = \\ \Pr(s_{31,ij} = s_{31,ij}^0) \Pr(\cap_{i,j=1}^m \{m_{1,ij} = m_{1,ij}^0\}). \tag{16}$$

Finally, according to (15), we have that entries $s_{31,ij}$ are independent of each other:

$$\Pr(\cap_{i,j=1}^m \{s_{31,ij} = s_{31,ij}^0\}) = \Pr(\cap_{i,j=1}^m \{f^{-1}(s_{21,ij}) + \\ + x_{ij} = s_{31,ij}^0\}) = \sum_{x_{ij}^0 \in \mathbb{Z}_q} \Pr(\cap_{i,j=1}^m \{f^{-1}(s_{21,ij}) = \\ = \underbrace{s_{31,ij}^0 - x_{ij}^0}_{\in \mathbb{Z}_q}\}, \cap_{i,j=1}^m \{x_{ij} = x_{ij}^0\}) = \prod_{i,j=1}^m \Pr(f^{-1}(s_{21,ij}) = \\ = s_{31,ij}^0 - x_{ij}^0) = \left(\frac{1}{q}\right)^{m^2}. \tag{17}$$

The process of proving the main three independencies for each block is iterative. The proof of the perfect security of the second block relies on the same idea and technique as was shown for the first block. Because the expressions of the formulas are more complex and much longer, we place the proof of the second block in Appendix A.

Let us summarize the results. From the analysis of the first CBC mode block, we obtain that:

B1.1 Entries of $\mathbf{S}_{11}$ are uniformly distributed in $\mathbb{Z}_q$ (6), independent of $\mathbf{M}_1$ (7) and mutually independent (8);

B1.2 Entries of $\mathbf{S}_{21}$ are uniformly distributed in $\mathbb{G}_q$ (9), independent of $\mathbf{M}_1$ (10), $\mathbf{M}_2$ (A3), $\mathbf{X}$ (15) and mutually independent (11);

B1.3 Entries of $\mathbf{S}_{31} = \mathbf{C}_1$ are uniformly distributed in $\mathbb{Z}_q$ (14), independent of $\mathbf{M}_1$ (16), $\mathbf{M}_2$ (A7), $\mathbf{M}_3$ (A19), $\mathbf{X}$ (A13), $\mathbf{Z}$ (A6), $\mathbf{Y}$ (A9) and mutually independent (17).

From the analysis of the second CBC mode block (see Appendix A), we obtain that:

B2.1 Entries of $\mathbf{S}_{12}$ are uniformly distributed in $\mathbb{Z}_q$ (A1), independent of $\mathbf{M}_2$ (A2), $\mathbf{X}$, $\mathbf{Y}$ (A11), $\mathbf{Z}$ (A12) and mutually independent (A4);

B2.2 Entries of $\mathbf{S}_{22}$ are uniformly distributed in $\mathbb{G}_q$ (A5), independent of $\mathbf{M}_2$ (A8), $\mathbf{M}_3$ (A18) $\mathbf{X}$ (A14) and mutually independent (A10);

B2.3 Entries of $\mathbf{S}_{32} = \mathbf{C}_2$ are uniformly distributed in $\mathbb{Z}_q$ (A15), independent of $\mathbf{M}_2$ (A16), $\mathbf{M}_3$ (A20), $\mathbf{X}$, $\mathbf{Y}$ (A23), $\mathbf{Z}$ (A22) and mutually independent (A17).

From the results of **B1.1**–**B1.3**, we obtain that the first block of the CBC mode (3) is perfectly secure. **B2.1**–**B2.3** imply that the second block of the CBC mode (3) is perfectly secure. i.e., Euquation (5) holds for the first two blocks in CBC mode with Algorithm (3).

To prove that each of the n blocks of the CBC mode with our cipher is perfectly secure, we need the method of mathematical induction. According to it, we now generalize the results of **B1.1**–**B1.3** and **B2.1**–**B2.3** and assume that the N-th block of the mode is perfectly secure, i.e., the following assumptions hold:

BN.1 Entries of $\mathbf{S}_{1N}$ are uniformly distributed in $\mathbb{Z}_q$, independent of $\mathbf{M}_N$, $\mathbf{X}$, $\mathbf{Y}$, $\mathbf{Z}$ and mutually independent;

BN.2 Entries of $\mathbf{S}_{2N}$ are uniformly distributed in $\mathbb{G}_q$, independent of $\mathbf{M}_N$, $\mathbf{M}_{N+1}$, $\mathbf{X}$ and mutually independent;

BN.3 Entries of $\mathbf{S}_{3N} = \mathbf{C}_N$ are uniformly distributed in $\mathbb{Z}_q$, independent of $\mathbf{M}_N$, $\mathbf{M}_{N+1}$, $\mathbf{M}_{N+2}$, $\mathbf{X}$, $\mathbf{Y}$, $\mathbf{Z}$ and mutually independent.

Under the assumptions **BN.1**–**BN.3**, in the next section we show that the $(N+1)$-th block of the mode is perfectly secure, i.e., the latter assumptions hold for the $(N+1)$-th block, too.

5.4. $\mathbf{S}_{1,N+1}$ *Independence*

Without loss of generality, to shorten the equalities and keeping in mind that each formula can be written for an entry of the matrix, the next equations are presented in matrix form.

Following the same idea as in matrices $\mathbf{S}_{11}$ (6) and $\mathbf{S}_{12}$ (A1), we obtain that entries of matrix $\mathbf{S}_{1,N+1}$ are uniformly and independently distributed in $\mathbb{Z}_q$:

$$\begin{aligned}
&\Pr(\mathbf{S}_{1,N+1} = \mathbf{S}^0_{1,N+1}) = \Pr(\mathbf{C}_N + \mathbf{M}_{N+1} = \mathbf{S}^0_{1,N+1}) = \\
&= \sum_{\mathbf{M}^0_{N+1} \in \mathbb{Z}_q} \Pr(\mathbf{C}_N = \mathbf{S}^0_{1,N+1} - \mathbf{M}^0_{N+1}, \mathbf{M}_{N+1} = \mathbf{M}^0_{N+1}) = \\
&= \left(\frac{1}{q}\right)^{m^2} \underbrace{\sum_{\mathbf{M}^0_{N+1} \in \mathbb{Z}_q} \Pr(\mathbf{M}_{N+1} = \mathbf{M}^0_{N+1})}_{\text{total probability = 1}} = \left(\frac{1}{q}\right)^{m^2}. \qquad (18)
\end{aligned}$$

Analogously as in (7) and (A2), we easily verify the independence between $\mathbf{S}_{1,N+1}$ and $\mathbf{M}_{N+1}$:

$$\begin{aligned}
&\Pr(\mathbf{S}_{1,N+1} = \mathbf{S}^0_{1,N+1}, \mathbf{M}_{N+1} = \mathbf{M}^0_{N+1}) = \\
&= \sum_{\mathbf{S}^0_{2,N} \in \mathbb{G}_q} \Pr(\mathbf{X} = \mathbf{S}^0_{1,N+1} - \mathbf{M}^0_{N+1} - \\
&- F^{-1}(\mathbf{S}^0_{2,N}), \mathbf{M}_{N+1} = \mathbf{M}^0_{N+1}, \mathbf{S}_{2,N} = s^0_{2,N}) = \\
&= \left(\frac{1}{q}\right)^{m^2} \Pr(\mathbf{M}_{N+1} = \mathbf{M}^0_{N+1}) \cdot \\
&\cdot \underbrace{\sum_{\mathbf{S}^0_{2,N} \in \mathbb{G}_q} \Pr(\mathbf{S}_{2,N} = \mathbf{S}^0_{2,N})}_{=1} = \left(\frac{1}{q}\right)^{m^2} \Pr(\mathbf{M}_{N+1} = \mathbf{M}^0_{N+1}) = \\
&= \Pr(\mathbf{S}_{1,N+1} = \mathbf{S}^0_{1,N+1}) \Pr(\mathbf{M}_{N+1} = \mathbf{M}^0_{N+1}).
\end{aligned} \tag{19}$$

5.5. $\mathbf{S}_{2,N+1}$ Independence

Similarly to (9) and (A5), $s_{2,N+1;ij}$ are all uniformly distributed in $\mathbb{G}_q$. Hence, by Corollary 1 we have:

$$\Pr(s_{2,N+1;ij} = s^0_{2,N+1;ij}) = \frac{1}{q}. \tag{20}$$

Finally, by Equations (11) and (A10), entries of $\mathbf{S}_{22}$ are mutually independent:

$$\begin{aligned}
&\Pr(\mathbf{S}_{2,N+1} = \mathbf{S}^0_{2,N+1}) = \Pr(\mathbf{Z} \odot^{\mathbf{Y}} F(\mathbf{S}_{1,N+1})^{\mathbf{Y}} = \mathbf{S}^0_{ij}) = \\
&= \sum_{\mathbf{C}^0_N \in \mathbb{Z}_q} \sum_{\mathbf{Y}^0 \in \mathbb{Z}_{q\setminus 0}} \sum_{\mathbf{M}^0_{N+1} \in \mathbb{Z}_q} \Pr\left(\mathbf{Z} = \mathbf{S}^0_{2,N+1} \odot \right. \\
&\left. \odot (^{\mathbf{Y}^0} F(\mathbf{C}^0_N + \mathbf{M}^0_{N+1})^{\mathbf{Y}^0})^{-1}, \mathbf{C}_N = \mathbf{C}^0_N, \mathbf{Y} = \mathbf{Y}^0, \right. \\
&\left. \mathbf{M}_{N+1} = \mathbf{M}^0_{N+1}\right) = \left(\frac{1}{q}\right)^{m^2}.
\end{aligned} \tag{21}$$

As in (10) and in (A8), $\mathbf{S}_{2,N+1}$ and $\mathbf{M}_{N+1}$ are independent:

$$\begin{aligned}
&\Pr(\mathbf{S}_{2,N+1} = \mathbf{S}^0_{2,N+1}, \mathbf{M}_{N+1} = \mathbf{M}^0_{N+1}\}) = \\
&= \sum_{\mathbf{C}^0_N \in \mathbb{Z}_q} \sum_{\mathbf{Y}^0 \in \mathbb{Z}_{q\setminus 0}} \Pr(\mathbf{Z} = \mathbf{S}^0_{2,N+1} \odot (^{\mathbf{Y}^0} F(\mathbf{C}^0_N + \mathbf{M}^0_{N+1})^{\mathbf{Y}^0})^{-1}, \\
&\mathbf{M}_{N+1} = \mathbf{M}^0_{N+1}, \mathbf{C}_N = \mathbf{C}^0_N, \mathbf{Y} = \mathbf{Y}^0) = \\
&= \left(\frac{1}{q}\right)^{m^2} \cdot \Pr(\mathbf{M}_{N+1} = \mathbf{M}^0_{N+1}) \cdot \sum_{\mathbf{C}^0_N \in \mathbb{Z}_q} \Pr(\mathbf{C}_N = \mathbf{C}^0_N) \cdot \\
&\cdot \sum_{\mathbf{Y}^0 \in \mathbb{Z}_{q\setminus 0}} \Pr(\mathbf{Y} = \mathbf{Y}^0) = \\
&= \Pr(\mathbf{S}_{2,N+1} = \mathbf{S}^0_{1,N+1}) \Pr(\mathbf{M}_{N+1} = \mathbf{M}^0_{N+1}\}).
\end{aligned} \tag{22}$$

5.6. $\mathbf{S}_{3,N+1} = \mathbf{C}_{N+1}$ *Independence*

Entries of $\mathbf{C}_{N+1}$ are uniformly and independently distributed in $\mathbb{Z}_q$ (similarly as in Equations (6) and (A15)):

$$\begin{aligned}\Pr(\mathbf{S}_{3,N+1} = \mathbf{S}^0_{3,N+1}) = \Pr(F^{-1}(\mathbf{S}_{2,N+1}) = \mathbf{S}^0_{3,N+1} - \mathbf{X}) = \\ = \sum_{\mathbf{C}^0_N \in \mathbb{Z}_q} \sum_{\mathbf{Y}^0 \in \mathbb{Z}_{q\setminus 0}} \sum_{\mathbf{X}^0 \in \mathbb{Z}_q} \sum_{\mathbf{M}^0_{N+1} \in \mathbb{Z}_q} \Pr(\mathbf{Z} = F(\mathbf{S}^0_{3,N+1} - \mathbf{X}^0) \cdot \\ \cdot ({}^{\mathbf{Y}^0}F(\mathbf{C}^0_{N,kl} + \mathbf{M}^0_{N+1})^{\mathbf{Y}^0})^{-1}, \mathbf{C}_N = \mathbf{C}^0_N, \mathbf{Y} = \mathbf{Y}^0, \mathbf{M}_{N+1} = \mathbf{M}^0_{N+1}, \\ \mathbf{X} = \mathbf{X}^0) = \Pr(z_{ij} = z^0_{ij}) = \left(\frac{1}{q}\right)^{m^2}. \end{aligned} \tag{23}$$

Finally, according to (16) and (A16), $\mathbf{C}_{N+1}$ is also independent of $\mathbf{M}_{N+1}$:

$$\begin{aligned}\Pr(\mathbf{S}_{3,N+1} = \mathbf{S}^0_{3,N+1}, \mathbf{M}_{N+1} = \mathbf{M}^0_{N+1}) = \sum_{\mathbf{X}^0 \in \mathbb{Z}_q} \sum_{\mathbf{C}^0_N \in \mathbb{Z}_q} \sum_{\mathbf{Y}^0 \in \mathbb{Z}_{q\setminus 0}} \Pr(\mathbf{Z} = \\ = F(\mathbf{S}^0_{3,N+1} - \mathbf{X}^0)({}^{\mathbf{Y}^0}F(\mathbf{C}^0_N + \mathbf{M}^0_{N+1})^{\mathbf{Y}^0})^{-1}, \mathbf{C}_N = \mathbf{C}^0_N, \mathbf{Y} = \mathbf{Y}^0, \\ \mathbf{M}_{N+1} = \mathbf{M}^0_{N+1}, \mathbf{X} = \mathbf{X}^0) = \\ = \left(\frac{1}{q}\right)^{m^2} \Pr(\mathbf{M}_{N+1} = \mathbf{M}^0_{N+1}) = \\ = \Pr(\mathbf{S}_{3,N+1} = \mathbf{S}^0_{3,N+1}) \Pr(\mathbf{M}_{N+1} = \mathbf{M}^0_{N+1}). \end{aligned} \tag{24}$$

Now, we can write the conclusions on the $(N+1)$-th block:

B(N+1).1 Entries of $\mathbf{S}_{1,N+1}$ are uniformly distributed in $\mathbb{Z}_q$ (18), independent of $\mathbf{M}_{N+1}$ (19) and mutually independent (18);

B(N+1).2 Entries of $\mathbf{S}_{2,N+1}$ are uniformly distributed in $\mathbb{G}_q$ (20), independent of $\mathbf{M}_{N+1}$ (22) and mutually independent (21);

B(N+1).3 Entries of $\mathbf{S}_{3,N+1} = \mathbf{C}_{N+1}$ are uniformly distributed in $\mathbb{Z}_q$ (23), independent of $\mathbf{M}_{N+1}$ (24) and mutually independent (23).

B(N+1).1–B(N+1).3 imply the perfect security of each of the CBC mode (3) blocks.

Proposition 1 implies one more important property of the proposed CBC cipher. The following corollary states, that each block of (3) is independent of previous blocks, i.e., information of the previous blocks does not affect the probability of the current block.

Corollary 2. *If the block cipher is proposed by algorithm* (3)*, then the following properties hold:*

$$\Pr(\mathbf{C}_i = \mathbf{C}^0_i | \cap_{j=1}^{i-1} \{\mathbf{C}_j = \mathbf{C}^0_j\}) = \Pr(\mathbf{C}_i = \mathbf{C}^0_i), \;\; i = 1, \ldots, N.$$

The proof of Corollary 2 follows directly from the proof of Proposition 1 by applying the same principle of mathematical induction.

6. Resistance of the CBC Mode to the Chosen Plaintext Attack

In this section, we show that due to the perfect secrecy property of the original block cipher, the proposed CBC mode can withstand the chosen plaintext attack. To achieve this goal, we consider the initial block cipher as a random permutation in the matrix space and afterwards show that any effective adversary does not have a significant advantage of winning the defined attack game, which formalizes the CPA security of the CBC mode of our cipher. This provides an additional level of resistance against algebraic cryptanalysis based on the OWF.

The basic idea behind the proof is to perform an in-depth analysis of the CBC mode by inspecting the encryption of the whole massive plaintext while also considering the encryption of a single block. The purpose of this analysis is to show that both approaches

do not let any efficient adversary discover any useful information he can use to harm the secrecy of the encrypted data.

Each of the presented approaches can be described by an attack game played between an adversary $\mathcal{A}$ (an algorithm seeking security issues) and a challenger—a machine replying to queries sent by $\mathcal{A}$. This technique of proof is highly inspired by the one described in [10]. We think that it clearly demonstrates the essence of the security proof and also find it easy to follow. Note also that throughout this paper all the adversaries are denoted by uppercase calligraphic letters.

Let us examine our block cipher ε as a random permutation. Relying on the fact that the message space and the ciphertext space are the same size (in fact, it is the same space), we denote by $C = Rand(M)$ a random one-to-one mapping, which maps a matrix $M \in Mat_m(\mathbb{Z}_q)$ to a matrix $C \in Mat_m(\mathbb{Z}_q)$. Consider the following Attack Game aimed at the pseudo-randomness of the encryption algorithm (1), i.e., this game determines if an adversary $\mathcal{A}$ can distinguish between a random permutation and an actual encryption function [10]:

Attack Game 1. *For the block cipher* $\varepsilon = \left\{ Enc(\vec{\mathbf{K}}, \mathbf{M}), Dec(\vec{\mathbf{K}}, \mathbf{C}) \right\}$ *given by algorithm* (1) *we define two experiments. Then for a value* $b \in \{0, 1\}$ *we have an Experiment b:*

- *The challenger selects a function* E_b *as follows:*

$$E_b = \begin{cases} Enc(K, M), \text{ if } b = 0; \\ Rand(M), \text{ otherwise.} \end{cases}$$

- *The adversary* $\mathcal{A}$ *submits a sequence of queries i.e., plaintexts in their matrix form* $\mathbf{M}_i$*, where* $i = 1, 2, \ldots$*;*
- *For the i-th query the challenger computes* $\mathbf{C}_i = E_b(\mathbf{M}_i)$ *and sends all the* $\mathbf{C}_i$*'s to an adversary.*
- $\mathcal{A}$ *outputs* $\hat{b} \in \{0, 1\}$

Denote by W_b *the random event that in Experiment b* $\mathcal{A}$ *outputs 1. Then* $\mathcal{A}$*'s advantage is defined as*

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

Proposition 2. *For all efficient adversaries* $\mathcal{A}$ *their advantage* $BCadv[\mathcal{A}, \varepsilon]$ *in Attack Game 1 is negligible.*

Proof. Let us assume that the adversary $\mathcal{A}$ sends m^2 queries, i.e., matrices $\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_{m^2}$, to its challenger. Since the adversary can choose these queries adaptively, we assume that these matrices are linearly independent. However, due to this assumption matrices $\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_{m^2}$ form a basis of the set $Mat_m(\mathbb{Z}_q)$, which is the domain and codomain of both functions $Enc(\vec{\mathbf{K}}, \mathbf{M})$, and $Rand(\mathbf{M})$. Hence the adversary can construct any matrix $\mathbf{M} \in Mat_m(\mathbb{Z}_q)$ since this set is spanned by the linear combinations of the basis matrices. In other words, we have:

$$\mathbf{M} = \sum_{j=1}^{m^2} \alpha_j \mathbf{M}_j. \tag{25}$$

According to the rules of the Attack Game 1 the challenger replies with the response matrices $\mathbf{C}_i = E_b(\mathbf{M}_i)$, where $i = 1, 2, \ldots, m^2$. Since both functions $Enc(\vec{\mathbf{K}}, \mathbf{M})$ and $Rand(\mathbf{M})$ are one-to-one (by their definitions), all response values are distinct, and since the set $Mat_m(\mathbb{Z}_q)$ is the codomain of both these functions, all the responses can be expressed as follows:

$$\mathbf{C}_i = \sum_{j=1}^{m^2} \beta_{ij} \mathbf{M}_j, \tag{26}$$

where $i = 1, 2, \ldots, m^2$. Furthermore, if more queries are made, then all of them together with all of the obtained responses can be expressed in a similar way.

Let us now consider Experiment 0. Relying on the perfect secrecy property of the block cipher ε, we can see that each ciphertext is equally likely, i.e.,

$$\Pr(Enc(\vec{\mathbf{K}}, \mathbf{M}_i) = \mathbf{C}_i^0) = \left(\frac{1}{q}\right)^{m^2},$$

where $\mathbf{C}_i^0$ is some fixed matrix. Furthermore, for any query matrix $\mathbf{M}$ the coefficients α_j in (25) are statistically independent from the coefficients β_{ij} in (26). Note, also, that for any response value $\mathbf{C}_i$ the coefficients β_{ij} are statistically independent from coefficients β_{kj}, where $k < i$ due to Corollary 2.

However, this behaviour of the encryption function is indistinguishable from a random permutation. In other words, an adversary can win the considered Attack Game if he can somehow tell apart the secret key $\vec{\mathbf{K}} = \{\mathbf{X}, \mathbf{Y}, \mathbf{Z}\}$ from the set of all possible keys $\mathbb{K}$. Otherwise, both functions $Enc(\vec{\mathbf{K}}, \mathbf{M})$, and R and $(\mathbf{M})$ look the same to the adversary. Hence, he can do no better than to randomly pick the secret key $\vec{\mathbf{K}}$ from the set $\mathbb{K}$. For this reason, the advantage the adversary has in the considered Attack Game can be estimated as follows:

$$BCadv[\mathcal{A}, \varepsilon] \leq \frac{1}{|\mathbb{K}|}, \tag{27}$$

where $|\mathbb{K}|$ is the size of the set $\mathbb{K}$. To calculate this value we recall the constrains on the key matrices $\mathbf{X}, \mathbf{Y}, \mathbf{Z}$:

- Matrix $\mathbf{X}$ does not contain any zero entries and, hence, it comes from the set of $(q\text{ - }1)^{m^2}$ possible matrices;
- Matrix $\mathbf{Y}$ has to be invertible and, hence, there are a total of $\prod_{i=1}^{m}(q^m - q^{i-1})$ possible choices;
- Matrix $\mathbf{Z}$ does not have any additional constrains and hence all q^{m^2} possibilities are allowed.

It can now be seen that the expression (27) can be rewritten in the following way:

$$BCadv[\mathcal{A}, \varepsilon] \leq \frac{1}{(q^2 - q)^{m^2} \prod_{i=1}^{m}(q^m - q^{i-1})}.$$

Evidently, this advantage is negligible. □

Note that Attack Game 1 is used to consider the original block cipher. The following Attack Game can be formulated for a newly defined CBC mode. This game, together with the previously presented Attack Game 1, is essential in the proof of the resistance of the CBC mode of our cipher to the chosen plaintext attack.

Attack Game 2. *For the probabilistic cipher* $\varepsilon' = \left\{Enc(\vec{\mathbf{K}}, \mu), Dec(K, c)\right\}$ *given by Algorithm* (3)*, we define two experiments. Then for a value* $b \in \{0, 1\}$*, we have Experiment b:*

- *The challenger selects a random key* $\vec{\mathbf{K}} = \{\mathbf{X}, \mathbf{Y}, \mathbf{Z}\}$*;*
- *The adversary* $\mathcal{A}$ *submits a sequence of queries i.e., plaintext pairs* (μ_{i0}, μ_{i1}) *of equal lengths, where* $i = 1, 2, \ldots, Q$*;*
- *For the i-th query the challenger computes* $C_i = Enc(\vec{\mathbf{K}}, \mu_{ib})$*, where* $b \in \{0, 1\}$ *is the experiment indicator, and sends all the* C_i*'s to an adversary.*
- $\mathcal{A}$ *outputs* $\hat{b} \in \{0, 1\}$

Denote by W_b *the random event that in Experiment b* $\mathcal{A}$ *outputs 1. Then* $\mathcal{A}$*'s advantage is defined as*

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

Note that any probabilistic cipher is considered to be CPA secure if $\mathcal{A}$'s advantage in Attack Game 2 is negligible. We formalize this fact for our cipher in the following proposition:

Proposition 3. *Consider probabilistic cipher* $\varepsilon' = \left\{ Enc(\vec{\mathbf{K}}, \mu), Dec(\vec{\mathbf{K}}, c) \right\}$ *given by Algorithm (3). For all efficient adversaries* $\mathcal{A}$*, their advantage in Attack Game 2 is expressed as follows:*

$$CPAadv[\mathcal{A}, \varepsilon'] = \frac{2Q^2l^2}{N}, \tag{28}$$

where Q *is the number of queries in Attack Game 2 and* l *is the total amount of blocks needed to encrypt a plaintext* μ_{ib}*.*

Proof. Let us define the following adversaries:

- $\mathcal{A}$ is an adversary which plays the Attack Game 2;
- $\mathcal{B}$ is an adversary interacting with $\mathcal{A}$ who plays Attack Game 1 with his own challenger.

Our aim is to show that a collaboration of these adversaries does not have any significant advantage in winning the defined Attack Game 2.

Obviously, the amount of blocks is poly-bounded and can be calculated as follows:

$$l = \lceil \frac{|\mu|}{m^2 t} \rceil,$$

where $\lceil \rceil$ is the ceiling function. Additionally, note that the denominator of the fraction in (28) equals $\lceil \log_2 |\mathbb{M}| \rceil$ and hence the size of message space of the CBC mode $\mathbb{M}$ and is super-poly. Hence, our strategy for this proof is similar to the one described in Theorem 5.4 of [10].

Note that prior to encrypting the first block of the plaintext μ_{ib}, a challenger randomly selects an initialization vector C_0 and hence the intermediate block S_{i1} consists of random uniformly distributed entries. Hence, by the construction of our scheme, the advantage $CPAadv^*[\mathcal{A}, \varepsilon']$ of adversary $\mathcal{A}$ to win a bit-guessing version of the Attack Game 2 is given by:

$$CPAadv^*[\mathcal{A}, \varepsilon'] = |\Pr(W_0) - \frac{1}{2}|.$$

Moreover, multiple queries involving the same message μ result in distinct ciphertext due to perfect secrecy property of the block cipher and the randomness of the initialization vector. In other words, because picking the same initialization vector is practically an impossible event, the ciphertexts are distinct due to$Enc(\vec{\mathbf{K}}, \mathbf{M}_j)$ being a one-to-one mapping for any block $\mathbf{M}_j$. In fact, as was previously proven, the value of $Enc(\vec{\mathbf{K}}, \mathbf{M}_j)$ is indistinguishable from a random permutation and hence $BCadv[\mathcal{B}, \varepsilon]$ is negligible. Evidently, this includes the first block as well.

All that remains is to define Games 2 and 3 as in Theorem 5.4 of [10] and evaluate the appropriate results. To shorten our paper we omit these steps. □

However, because both the total amount of blocks l and the total amount of queries Q are poly-bounded whereas the size of the message space is super-poly, the advantage $CPAadv[\mathcal{A}, \varepsilon']$ is negligible and hence the CBC mode of the original Shannon cipher is CPA secure.

As an example, we explore the $CPAadv^*[\mathcal{A}, \varepsilon']$ of the CBC mode ε' defined by (3) when the value of $q = 2039$ and $m = 8$. Then, we have:

$$CPAadv[\mathcal{A}, \varepsilon'] = \frac{2Q^2l^2}{(l+1)2039^{64}} + \frac{2}{(2039^2 - 2039)^{64} \prod_{i=1}^{8} (2039^8 - 2039^{i-1})} \approx$$
$$\approx \frac{2Q^2l^2}{(l+1)2039^{64}} + 2^{-2110}.$$

Note that the $BCadv[\mathcal{B}, \varepsilon] \approx 2^{-2110}$ is negligible even compared to the first fraction in the above expression and, hence, does not have much of an impact on the $CPAadv[\mathcal{A}, \varepsilon']$. Ignoring $BCadv[\mathcal{B}, \varepsilon]$ we obtain the following result:

$$\frac{Q^2 l^2}{(l+1)} < \frac{2039^{64}}{2} CPAadv[\mathcal{A}, \varepsilon'].$$

Then, assuming $CPAadv[\mathcal{A}, \varepsilon'] = 2^{-112}$ and that an adversary can submit 2^{112} queries, each query could contain approximately 2^{366} blocks. In other words, the size of the message is practically unlimited.

In general, ignoring the $BCadv[\mathcal{B}, \varepsilon]$ and approximating the expression $\frac{l^2}{l+1} \approx l$ in order to have $CPAadv[\mathcal{A}, \varepsilon'] < 2^{-112}$ we obtain a following result:

$$Q^2 l < 2^{-113} q^{m^2}. \tag{29}$$

Exploring values of q presented in [12] and limiting the message to 2^{32} blocks we present the minimal values of the matrix size and the maximal number of queries allowed to achieve the desired adversary advantage in Table 1:

Table 1. Minimal matrix size and maximal number of queries to achieve $CPAadv[\mathcal{A}, \varepsilon'] < 2^{-112}$ for distinct values of q.

q	m	Q
3	10	107
11	7	4891
53	6	$\approx 2^{30.6}$
2039	4	44,736
16,776,899	3	$\approx 2^{35.5}$

The presented values in Table 1 should be interpreted as follows: for a given value of q (say, 3) any smaller value of m gives an adversary an advantage $CPAadv[\mathcal{A}, \varepsilon'] > 2^{-112}$ even if $Q = 1$. For given values of q and m (say, 3 and 10) the presented value of Q is the maximum number of queries the adversary can send before his advantage surpasses the value 2^{-112}. In other words, when the adversary sends $Q + 1$-st query (108-th, if $q = 3$ and $m = 10$) he obtainss $CPAadv[\mathcal{A}, \varepsilon'] > 2^{-112}$. All the results presented in Table 1 were calculated using inequality (29), where $l = 2^{32}$.

Note that in our investigation we used Sophie Germain primes q relatively close but smaller than powers of 2. We can see that the maximal amount of queries can be reasonably small. This issue can be easily fixed by slightly increasing the matrix size. As we previously saw, setting $q = 2039$ and $m = 8$ practically makes all efforts of any efficient CPA adversary irrelevant. Moreover, we can also settle for a tolerable CPA advantage, say 2^{-80}, which greatly increases the number of queries required to surpass the chosen value.

7. Conclusions

In this paper, we proposed a new block cipher based on the previously defined Shannon cipher which operates in CBC mode. The construction of our block cipher relies on the link between perfect secrecy and pseudo-random number generators described by Yao in [9]. Moreover, we modified our initial proposal in such a way that the perfect secrecy property remains intact. This fact together with Theorem 5.4 in [10] allowed us to prove that our block cipher is secure against CPA.

In our previous publications, we have shown that MPF is a worthy candidate OWF and hence is suitable for applications in cryptography. Using the described transformation of the initial plaintext in its matrix form, we obtain a block that can be encrypted by executing a single round algorithm (1). Currently, this is a rather unusual idea in symmetric cryptography. However, we think that the proven perfect secrecy property of the original

Shannon cipher and CPA security of the newly defined block cipher can aid our proposal to find its place among other secure symmetric ciphers.

It is also worth noting that due to construction, presented in Section 4, no additional rounds are needed to perform data encryption. For this reason, the execution of the encryption process can be parallelized, i.e., we can use extra processors to perform calculations simultaneously for a single block. The latter property is related to the fact that matrix operations can be effectively parallelized up to m^2 parallel computations where m is an order of matrices defining our function. We think that this fact can be used to our advantage resulting in a significant boost in performance. However, in this paper, we only considered the resistance of the proposed CBC mode to chosen-plaintext attack (CPA) and leave its performance analysis for our future publication.

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

Funding: This research received no external funding.

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

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

Appendix A

Here, we present the detailed and comprehensive proof of the second block security of Proposition 1.

In the second block of (3), entries of matrices are of the following form:

$$\begin{aligned} s_{12,ij} &= m_{2,ij} + c_{1,ij};\\ s_{22,ij} &= z_{ij} \cdot \prod_{k=1}^{m}\prod_{l=1}^{m}(f(s_{12,kl}))^{y_{ik}y_{lj}};\\ c_{2,ij} &= s_{32,ij} = f^{-1}(s_{22,ij}) + x_{ij}. \end{aligned}$$

Appendix A.1. $\mathbf{S}_{12}$ *Independence*

Following the proof of the first block (6), $s_{12,ij}$ are uniformly distributed in $\mathbb{Z}_q$:

$$\begin{aligned} &\Pr(s_{12,ij} = s^0_{12,ij}) = \Pr(c_{1,ij} + m_{2,ij} = s^0_{ij}) =\\ &= \sum_{m^0_{2,ij}\in\mathbb{Z}_q} \Pr(c_{1,ij} = s^0_{12,ij} - m^0_{2,ij}, m_{2,ij} = m^0_{2,ij}) =\\ &= \sum_{m^0_{2,ij}\in\mathbb{Z}_q}\sum_{s^0_{21,ij}\in\mathbb{G}_q} \Pr(x_{ij} = \underbrace{s^0_{12,ij} - m^0_{2,ij} - f^{-1}(s^0_{21,ij})}_{\in\,\mathbb{Z}_q},\\ &\qquad m_{2,ij} = m^0_{2,ij}, s_{21,ij} = s^0_{21,ij}) =\\ &= \frac{1}{q}\underbrace{\sum_{m^0_{2,ij}\in\mathbb{Z}_q}\sum_{s^0_{21,ij}\in\mathbb{G}_q} \Pr(m_{2,ij} = m^0_{2,ij}, s_{21,ij} = s^0_{21,ij})}_{=\,1} = \frac{1}{q}. \end{aligned} \tag{A1}$$

Using the same idea as in (7) and (A1), we obtain that $\mathbf{S}_{21}$ and $\mathbf{M}_2$ are independent:

$$\begin{aligned}
&\Pr(s_{12,ij} = s^0_{12,ij}, \cap_{i,j=1}^{m}\{m_{2,ij} = m^0_{2,ij}\}) = \\
&= \sum_{s^0_{21,ij}\in\mathbb{G}_q} \Pr(x_{ij} = s^0_{12,ij} - m^0_{2,ij} - f^{-1}(s^0_{21,ij}), \\
&\cap_{i,j=1}^{m}\{m_{2,ij} = m^0_{2,ij}\}, s_{21,ij} = s^0_{21,ij}) = \\
&= \Pr(s_{12,ij} = s_{10}) \Pr(\cap_{i,j=1}^{m}\{m_{2,ij} = m^0_{2,ij}\}).
\end{aligned} \tag{A2}$$

In the last step of (A2), we refer to the independence of the entries $m_{2,ij}$ and $s_{21,ij}$, which can be proved in this way (analogously to (10)):

$$\begin{aligned}
&\Pr(s_{21,ij} = s^0_{21,ij}, \cap_{i,j=1}^{m}\{m_{2,ij} = m^0_{ij}\}) = \sum_{c^0_{0,kl}\in\mathbb{Z}_q} \sum_{y^0_{kl}\in\mathbb{Z}_{q\setminus 0}} \sum_{m^0_{1,ij}\in\mathbb{Z}_q} \Pr(z_{ij} = \\
&= \underbrace{s^0_{21,ij}(\prod_{k=1}^{m}\prod_{l=1}^{m}(f(c^0_{0,kl} + m^0_{1,kl}))^{y^0_{ik}y^0_{lj}})^{-1}}_{\in\mathbb{Z}_q}, \cap_{i,j=1}^{m}\{m_{1,ij} = m^0_{1,ij}\}, \\
&\cap_{k,l=1}^{m}\{c_{0,kl} = c^0_{0,kl}\}, \cap_{k,l=1}^{m}\{y_{kl} = y^0_{kl}\}, \cap_{i,j=1}^{m}\{m_{2,ij} = m^0_{2,ij}\}) = \\
&= \frac{1}{q}\cdot \Pr(\cap_{i,j=1}^{m}\{m_{2,ij} = m^0_{2,ij}\}) = \Pr(s_{21,ij} = s^0_{21,ij}) \Pr(\cap_{i,j=1}^{m}\{m_{2,ij} = m^0_{ij}\}).
\end{aligned} \tag{A3}$$

The third independence of $\mathbf{S}_{12}$ is that entries of it are mutually independent. In the same way as in (8) and (A1), it follows that:

$$\begin{aligned}
&\Pr(\cap_{i,j=1}^{m}\{s_{12,ij} = s^0_{12,ij}\}) = \Pr(\cap_{i,j=1}^{m}\{c_{1,ij} + m_{2,ij} = s^0_{12,ij}\}) = \\
&= \sum_{s^0_{21,ij}\in\mathbb{G}_q} \sum_{m^0_{2,ij}\in\mathbb{Z}_q} \Pr(\cap_{i,j=1}^{m}\{x_{ij} = s^0_{12,ij} - m^0_{2,ij} - f^{-1}(s^0_{21,ij})\}, \\
&\cap_{i,j=1}^{m}\{m_{2,ij} = m^0_{2,ij}\}, \cap_{i,j=1}^{m}\{s_{21,ij} = s^0_{21,ij}\}) = \\
&= \left(\frac{1}{q}\right)^{m^2} \cdot \sum_{s^0_{21,ij}\in\mathbb{G}_q} \sum_{m^0_{2,ij}\in\mathbb{Z}_q} \Pr(\cap_{i,j=1}^{m}\{m_{2,ij} = m^0_{2,ij}\}, \\
&\cap_{i,j=1}^{m}\{s_{21,ij} = s^0_{21,ij}\}) = \left(\frac{1}{q}\right)^{m^2},
\end{aligned} \tag{A4}$$

because the double sum at the end of (A4) is equal to 1.

Appendix A.2. $\mathbf{S}_{22}$ *Independence*

According to Corollary 1, entries of matrix $\mathbf{S}_{22}$ are uniformly distributed in $\mathbb{G}_q$:

$$\Pr(s_{22,ij} = s^0_{22,ij}) = \frac{1}{q}. \tag{A5}$$

To show that $\mathbf{S}_{22}$ is independent of $\mathbf{M}_2$, first we prove that $\mathbf{C}_1 = \mathbf{S}_{31}$ is independent of $\mathbf{Z}$:

$$\begin{aligned}
&\Pr(s_{31,ij} = s^0_{31,ij}, \cap_{i,j=1}^{m}\{z_{ij} = z^0_{ij}\}) = \sum_{s^0_{21,ij}\in\mathbb{G}_q} \Pr(x_{ij} = \underbrace{s^0_{31,ij} - f^{-1}(s^0_{21,ij})}_{\in\mathbb{Z}_q}, \\
&\cap_{i,j=1}^{m}\{z_{ij} = z^0_{ij}\}, s_{21,ij} = s^0_{21,ij}) = \\
&= \frac{1}{q}\Pr(\cap_{i,j=1}^{m}\{z_{ij} = z^0_{ij}\}) = \Pr(s_{31,ij} = s^0_{31,ij}) \Pr(\cap_{i,j=1}^{m}\{z_{ij} = z^0_{ij}\}).
\end{aligned} \tag{A6}$$

Additionally, we need the independence of the entries $c_{1,ij} = s_{31,ij}$ and $m_{2,ij}$. Similarly as in (16):

$$\begin{aligned}
&\Pr(c_{1,ij} = c^0_{1,ij}, \cap_{i,j=1}^{m}\{m_{2,ij} = m^0_{2,ij}\}) = \\
&= \sum_{s^0_{21,ij} \in \mathbb{G}_q} \Pr(x_{ij} = c^0_{1,ij} - f^{-1}(s^0_{21,ij}), s_{21,ij} = s^0_{21,ij}, \\
&\qquad \cap_{i,j=1}^{m}\{m_{2,ij} = m^0_{2,ij}\}) = \\
&= \frac{1}{q} \cdot \sum_{s^0_{21,ij} \in \mathbb{G}_q} \Pr(s_{21,ij} = s^0_{21,ij}) \Pr(\cap_{i,j=1}^{m}\{m_{2,ij} = m_0\}) \\
&\qquad = \Pr(c_{1,ij} = c^0_{1,ij}) \Pr(\cap_{i,j=1}^{m}\{m_{2,ij} = m^0_{2,ij}\}).
\end{aligned} \tag{A7}$$

Hence, analogously as in (10), (A6) and (A7) imply that matrices $\mathbf{S}_{22}$ and $\mathbf{M}_2$ are independent:

$$\begin{aligned}
&\Pr(s_{22,ij} = s^0_{22,ij}, \cap_{i,j=1}^{m}\{m_{2,ij} = m^0_{2,ij}\}) = \\
&= \sum_{c^0_{1,kl} \in \mathbb{Z}_q} \sum_{y^0_{kl} \in \mathbb{Z}_{q \setminus 0}} \Pr(z_{ij} = s^0_{22,ij} (\prod_{k=1}^{m}\prod_{l=1}^{m} (f(c^0_{1,kl} + m^0_{2,kl}))^{y^0_{ik} y^0_{lj}})^{-1}, \\
&\cap_{i,j=1}^{m}\{m_{2,ij} = m^0_{2,ij}\}, \cap_{k,l=1}^{m}\{c_{1,kl} = c^0_{1,kl}\}, \cap_{k,l=1}^{m}\{y_{kl} = y^0_{kl}\}) = \\
&= \frac{1}{q} \cdot \Pr(\cap_{i,j=1}^{m}\{m_{2,ij} = m^0_{2,ij}\}) = \Pr(s_{22,ij} = s^0_{22,ij}) \cdot \\
&\qquad \cdot \Pr(\cap_{i,j=1}^{m}\{m_{2,ij} = m^0_{2,ij}\}),
\end{aligned} \tag{A8}$$

with the fact that $\mathbf{C}_1$ and $\mathbf{Y}$ are independent:

$$\begin{aligned}
&\Pr(c_{1,ij} = c^0_{1,ij}, \cap_{i,j=1}^{m}\{y_{ij} = y^0_{ij}\}) = \sum_{c^0_{0,ij} \in \mathbb{Z}_q} \sum_{m^0_{1,ij} \in \mathbb{Z}_q} \sum_{z^0_{ij} \in \mathbb{Z}_q} \Pr(x_{ij} = c^0_{1,ij} - \\
&- f^{-1}(z^0_{ij} \prod_{k=1}^{m}\prod_{l=1}^{m} (f(c^0_{0,kl} + m^0_{1,kl}))^{y^0_{ik} y^0_{lj}}), \cap_{i,j=1}^{m}\{m_{1,ij} = m^0_{1,ij}\}, \cap_{i,j=1}^{m}\{c_{0,ij} = c^0_{0,ij}\}, \\
&\qquad z_{ij} = z^0_{ij}, \cap_{i,j=1}^{m}\{y_{ij} = y^0_{ij}\}) = \frac{1}{q} \cdot \Pr(\cap_{i,j=1}^{m}\{y_{ij} = y^0_{ij}\}).
\end{aligned} \tag{A9}$$

The last step of matrix $\mathbf{S}_{22}$ is to show the independence between its entries, in the same way as in (11):

$$\begin{aligned}
&\Pr(\cap_{i,j=1}^{m}\{s_{22,ij} = s^0_{ij}\}) = \Pr(\cap_{i,j=1}^{m}\{z_{ij} \prod_{k=1}^{m}\prod_{l=1}^{m} (f(s_{12,kl}))^{y_{ik} y_{lj}} = s^0_{ij}\}) = \\
&= \sum_{s^0_{11,kl} \in \mathbb{Z}_q} \sum_{y^0_{ij} \in \mathbb{Z}_{q \setminus 0}} \Pr\left(\cap_{i,j=1}^{m}\{z_{ij} = s^0_{ij} \left(\prod_{k=1}^{m}\prod_{l=1}^{m} (f(s^0_{12,kl}))^{y^0_{ik} y^0_{lj}}\right)^{-1}\}, \right. \\
&\qquad \left. \cap_{k,l=1}^{m}\{s_{12,kl} = s^0_{12,kl}\}, \cap_{i,j=1}^{m}\{y_{ij} = y^0_{ij}\}\right) = \left(\frac{1}{q}\right)^{m^2}.
\end{aligned} \tag{A10}$$

In the last equality of (A10) we needed two additional independencies: Equations (A11) and (A12). The first is that matrices $\mathbf{S}_{12}$ and $\mathbf{Y}$ are independent:

$$\begin{aligned}\Pr(s_{12,ij}=s^0_{12,ij},\cap_{i,j=1}^m\{y_{ij}=y^0_{ij}\}) &= \sum_{m^0_{2,ij}\in\mathbb{Z}_q}\Pr(c_{1,ij}=s^0_{12,ij}-m^0_{2,ij},m_{2,ij}=m^0_{2,ij},\\ &\cap_{i,j=1}^m\{y_{ij}=y^0_{ij}\})=\\ &=\frac{1}{q}\Pr(\cap_{i,j=1}^m\{y_{ij}=y^0_{ij}\})\cdot\sum_{m^0_{2,ij}\in\mathbb{Z}_q}\Pr(m_{2,ij}=m^0_{2,ij})=\\ &=\frac{1}{q}\Pr(\cap_{i,j=1}^m\{y_{ij}=y^0_{ij}\})=\Pr(s_{12,ij}=s^0_{12,ij})\Pr(\cap_{i,j=1}^m\{y_{ij}=y^0_{ij}\}).\end{aligned}\tag{A11}$$

The second is that matrices $\mathbf{S}_{12}$ and $\mathbf{Z}$ are independent too:

$$\begin{aligned}\Pr(s_{12,ij}=s^0_{12,ij},\cap_{i,j=1}^m\{z_{ij}=z^0_{ij}\}) &= \sum_{m^0_{2,ij}\in\mathbb{Z}_q}\Pr(c_{1,ij}=s^0_{12,ij}-m^0_{2,ij},m_{2,ij}=m^0_{2,ij},\\ &\cap_{i,j=1}^m\{z_{ij}=z^0_{ij}\})=\\ &=\frac{1}{q}\Pr(\cap_{i,j=1}^m\{z_{ij}=z^0_{ij}\})\cdot\sum_{m^0_{2,ij}\in\mathbb{Z}_q}\Pr(m_{2,ij}=m^0_{2,ij})=\\ &\frac{1}{q}\Pr(\cap_{i,j=1}^m\{y_{ij}=y^0_{ij}\})=\Pr(s_{12,ij}=s^0_{12,ij})\Pr(\cap_{i,j=1}^m\{y_{ij}=y^0_{ij}\}).\end{aligned}\tag{A12}$$

Appendix A.3. $\mathbf{S}_{32}=\mathbf{C}_2$ *Independence*

In order to prove that entries $s_{32,ij}=c_{2,ij}$ are all uniformly distributed in $\mathbb{Z}_q$, first, we need the independence between $\mathbf{C}_1$ and $\mathbf{X}$:

$$\begin{aligned}\Pr(c_{1,ij}=c^0_{1,ij},\cap_{i,j=1}^m\{x_{ij}=x^0_{ij}\})&=\Pr(f^{-1}(s_{21,ij})=c^0_{1,ij}-x^0_{ij},\cap_{i,j=1}^m\{x_{ij}=x^0_{ij}\})=\\ &=\frac{1}{q}Pr(\cap_{i,j=1}^m\{x_{ij}=x^0_{ij}\})=\Pr(c_{1,ij}=c^0_{1,ij})\Pr(\cap_{i,j=1}^m\{x_{ij}=x^0_{ij}\}),\end{aligned}\tag{A13}$$

which implies the independence of $\mathbf{S}_{22}$ and $\mathbf{X}$:

$$\begin{aligned}&\Pr(s_{22,ij}=s^0_{22,ij},\cap_{i,j=1}^m\{x_{ij}=x^0_{ij}\})=\\ &=\sum_{m^0_{2,ij}\in\mathbb{Z}_q}\sum_{c^0_{1,kl}\in\mathbb{Z}_q}\sum_{y^0_{ij}\in\mathbb{Z}_{q\setminus 0}}\Pr\Big(z_{ij}=s^0_{22,ij}\cdot\\ &\cdot\Big(\prod_{k=1}^m\prod_{l=1}^m(f(c^0_{1,kl}+m^0_{2,kl}))^{y^0_{ik}y^0_{lj}}\Big)^{-1},\cap_{i,j=1}^m\{x_{ij}=x^0_{ij}\},\\ &\cap_{i,j=1}^m\{y_{ij}=y^0_{ij}\},\cap_{i,j=1}^n\{m_{2,ij}=m^0_{2,ij}\},\cap_{k,l=1}^n\{c_{1,kl}=c^0_{1,kl}\}\Big)=\\ &=\\ &=\frac{1}{q}\Pr(\cap_{i,j=1}^m\{x_{ij}=x^0_{ij}\})=\Pr(s_{22,ij}=s^0_{22,ij})\Pr(\cap_{i,j=1}^m\{x_{ij}=x^0_{ij}\}).\end{aligned}\tag{A14}$$

This, together with (A13), yields

$$\begin{aligned}\Pr(s_{32,ij}=s^0_{32,ij})&=\Pr(f^{-1}(s_{22,ij})=s^0_{31,ij}-x_{ij})=\\ &=\frac{1}{q}\sum_{x^0_{ij}\in\mathbb{Z}_q}Pr(x_{ij}=x^0_{ij})=\frac{1}{q}.\end{aligned}\tag{A15}$$

The main security condition for the second block, the independence between $\mathbf{S}_{32} = \mathbf{C}_2$ and $\mathbf{M}_2$, is satisfied (following the idea of (16)):

$$\begin{aligned}
&\Pr(s_{32,ij} = s^0_{32,ij}, \cap_{i,j=1}^{m}\{m_{2,ij} = m^0_{2,ij}\}) = \\
&= \Pr(f^{-1}(s_{22,ij}) + x_{ij} = s_{30}, \cap_{i,j=1}^{n}\{m_{2,ij} = m^0_{2,ij}\}) = \\
&= \sum_{x^0_{ij} \in \mathbb{Z}_q} \Pr(s_{22,ij} = f(s^0_{32,ij} - x^0_{ij}), \cap_{i,j=1}^{m}\{m_{2,ij} = m^0_{2,ij}\}, \\
&\qquad x_{ij} = x^0_{ij}) = \\
&= \frac{1}{q}\Pr(\cap_{i,j=1}^{m}\{m_{2,ij} = m^0_{2,ij}\}) = \Pr(s_{32,ij} = s^0_{32,ij}) \cdot \\
&\qquad \cdot \Pr(\cap_{i,j=1}^{m}\{m_{2,ij} = m^0_{2,ij}\}).
\end{aligned} \tag{A16}$$

Finally, entries of $\mathbf{S}_{32} = \mathbf{C}_2$ are independent:

$$\begin{aligned}
&\Pr(\cap_{i,j=1}^{m}\{s_{32,ij} = s^0_{32,ij}\}) = \Pr(\cap_{i,j=1}^{m}\{f^{-1}(s_{22,ij}) + x_{ij} = s^0_{32,ij}\}) = \\
&= \sum_{x^0_{ij} \in \mathbb{Z}_q} \Pr(\cap_{i,j=1}^{m}\{f^{-1}(s_{22,ij}) = s^0_{32,ij} - x^0_{ij}\}, \cap_{i,j=1}^{m}\{x_{ij} = x^0_{ij}\}) = \\
&\qquad = \prod_{i,j=1}^{m} \Pr(f^{-1}(s_{22,ij}) = s^0_{32,ij} - x^0_{ij}) = \left(\frac{1}{q}\right)^{m^2}.
\end{aligned} \tag{A17}$$

Additionally, to generalize the analysis of the n-th block, we can show that $\mathbf{C}_2$ is independent of $\mathbf{M}_3$. To prove this, first, we need the independence between $\mathbf{S}_{22}$ and $\mathbf{M}_3$ (similarly as in (A8)):

$$\begin{aligned}
&\Pr(s_{22,ij} = s^0_{22,ij}, \cap_{i,j=1}^{m}\{m_{3,ij} = m^0_{3,ij}\}) = \sum_{c^0_{1,kl} \in \mathbb{Z}_q} \sum_{y^0_{kl} \in \mathbb{Z}_{q \setminus 0}} \Pr(z_{ij} = s^0_{22,ij} \cdot \\
&\cdot (\prod_{k=1}^{m}\prod_{l=1}^{m}(f(c^0_{1,kl} + m^0_{2,kl}))^{y^0_{ik}y^0_{lj}})^{-1}, \cap_{i,j=1}^{m}\{m_{3,ij} = m^0_{3,ij}\}, \\
&\cap_{k,l=1}^{m}\{c_{1,kl} = c^0_{1,kl}\}, \cap_{k,l=1}^{m}\{y_{kl} = y^0_{kl}\}) = \frac{1}{q} \cdot \Pr(\cap_{i,j=1}^{m}\{m_{3,ij} = m^0_{3,ij}\}) = \\
&= \Pr(s_{22,ij} = s^0_{22,ij}) \Pr(\cap_{i,j=1}^{m}\{m_{3,ij} = m^0_{3,ij}\}),
\end{aligned} \tag{A18}$$

where we used the fact that $\mathbf{C}_1$ and $\mathbf{M}_3$ are independent too, because:

$$\begin{aligned}
&\Pr(c_{1,ij} = c^0_{1,ij}, \cap_{i,j=1}^{m}\{m_{3,ij} = m^0_{3,ij}\}) = \\
&= \sum_{s^0_{21,ij} \in \mathbb{Z}_q} \Pr(x_{ij} = c^0_{1,ij} - f^{-1}(s^0_{21,ij}), s_{21,ij} = s^0_{21,ij}, \\
&\cap_{i,j=1}^{m}\{m_{3,ij} = m^0_{3,ij}\}) = \frac{1}{q}\Pr(\cap_{i,j=1}^{m}\{m_{3,ij} = m^0_{3,ij}\}) = \\
&= \Pr(c_{1,ij} = c^0_{1,ij}) \Pr(\cap_{i,j=1}^{m}\{m_{3,ij} = m^0_{3,ij}\}).
\end{aligned} \tag{A19}$$

Using the same idea as in (A16), (A18) and (A19) imply the independence between $\mathbf{C}_2$ and $\mathbf{M}_3$:

$$\begin{aligned}
&\Pr(c_{2,ij} = c^0_{2,ij}, \cap_{i,j=1}^{m}\{m_{3,ij} = m^0_{3,ij}\}) = \\
&= \Pr(f^{-1}(s_{22,ij}) + x_{ij} = s_{30}, \cap_{i,j=1}^{n}\{m_{3,ij} = m^0_{3,ij}\}) = \\
&= \sum_{x^0_{ij}\in\mathbb{Z}_q} \Pr(s_{22,ij} = f(s^0_{32,ij} - x^0_{ij}), \cap_{i,j=1}^{m}\{m_{3,ij} = m^0_{3,ij}\}, \\
&x_{ij} = x^0_{ij}) = \frac{1}{q}\Pr(\cap_{i,j=1}^{m}\{m_{3,ij} = m^0_{3,ij}\}) = \\
&\Pr(c_{2,ij} = c^0_{2,ij})\Pr(\cap_{i,j=1}^{m}\{m_{3,ij} = m^0_{3,ij}\}).
\end{aligned} \tag{A20}$$

To generalize the iterative process of the CBC mode, with each block satisfying the condition of security, we need the independence between $\mathbf{C}_2$ and $\mathbf{Z}$:

$$\begin{aligned}
&\Pr(c_{2,ij} = c^0_{2,ij}, \cap_{i,j=1}^{m}\{z_{ij} = z^0_{ij}\}) = \\
&= \sum_{x^0_{ij}\in\mathbb{Z}_q} \Pr(f^{-1}(s_{22,ij}) = c^0_{2,ij} - x^0_{ij}, \cap_{i,j=1}^{m}\{z_{ij} = z^0_{ij}\}, \\
&x_{ij} = x^0_{ij}) = \sum_{x^0_{ij}\in\mathbb{Z}_q} \Pr(\prod_{k=1}^{m}\prod_{l=1}^{m}(f(s_{12,kl}))^{y_{ik}y_{lj}} = \\
&= (z^0_{ij})^{-1} f(c^0_{2,ij} - x^0_{ij}), x_{ij} = x^0_{ij}, \cap_{i,j=1}^{m}\{z_{ij} = z^0_{ij}\}) = \\
&= \\
&= \frac{1}{q}\underbrace{\sum_{x^0_{ij}\in\mathbb{Z}_q} \Pr(x_{ij} = x^0_{ij}, \cap_{i,j=1}^{m}\{z_{ij} = z^0_{ij}\})}_{\text{total probability of } \cap_{i,j=1}^{m}\{z_{ij} = z^0_{ij}\}} = \\
&= \Pr(c_{2,ij} = c^0_{2,ij})\Pr(\cap_{i,j=1}^{m}\{z_{ij} = z^0_{ij}\}),
\end{aligned} \tag{A21}$$

$$= \Pr(c_{2,ij} = c^0_{2,ij})\Pr(\cap_{i,j=1}^{m}\{z_{ij} = z^0_{ij}\}), \tag{A22}$$

where we used that $\mathbf{S}_{12}$ and $\mathbf{X}$ are independent, which is easy to prove if we keep the same idea as in (A11).

$\mathbf{C}_2$ and $\mathbf{Y}$ are also independently distributed:

$$\begin{aligned}
&\Pr(c_{2,ij} = c^0_{2,ij}, \cap_{i,j=1}^{m}\{y_{ij} = y^0_{ij}\}) = \\
&= \sum_{s^0_{22,ij}\in\mathbb{Z}_q} \Pr(x_{ij} = c^0_{2,ij} - f^{-1}(s^0_{22,ij}), \cap_{i,j=1}^{m}\{y_{ij} = y^0_{ij}\}, \\
&s_{22,ij} = s^0_{22,ij}) = \Pr(c_{2,ij} = c^0_{2,ij})\Pr(\cap_{i,j=1}^{m}\{y_{ij} = y^0_{ij}\}).
\end{aligned} \tag{A23}$$

Independence of matrices $\mathbf{C}_2$ and $\mathbf{X}$ can be easily proved according to (A22), because $\mathbf{S}_{22}$ is independent of $\mathbf{X}$.

References

1. Katz, J.; Lindell, Y. *Introduction to Modern Cryptography*; CRC Press: London, UK, 2020.
2. Feistel, H. Cryptography and Computer Privacy. *Sci. Am.* **1973**, *228*, 15–23. [CrossRef]
3. Dworkin, M.J.; Barker, E.B.; Nechvatal, J.R.; Foti, J.; Bassham, L.E.; Roback, E.; Dray, J.F., Jr. Advanced Encryption Standard (AES). In *Federal Inf. Process. Stds.*; (NIST FIPS); National Institute of Standards and Technology: Gaithersburg, MD, USA, 2001.
4. GOST R 34.12-2015: Block Cipher "Kuznyechik". Available online: https://www.hjp.at/(de)/doc/rfc/rfc7801.html (accessed on 17 March 2022).
5. Biryukov, A.; Dunkelman, O.; Keller, N.; Khovratovich, D.; Shamir, A. Key Recovery Attacks of Practical Complexity on AES-256 Variants with up to 10 Rounds. In *Advances in Cryptology, Proceedings of the EUROCRYPT 2010, Nice, France, 30 May—3 June 2010*; Gilbert, H., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2010; Volume 6110, pp. 299–319. ISBN 978-3-642-13189-9.

6. Diffie, W.; Hellman, M.E. Special Feature Exhaustive Cryptanalysis of the NBS Data Encryption Standard. *Computer* **1977**, *10*, 74–84. [CrossRef]
7. AlTawy, R.; Youssef, A.M. A Meet in the Middle Attack on Reduced Round Kuznyechik. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2015**, *98*, 2194–2198. [CrossRef]
8. Courtois, N.T.; Pieprzyk, J. Cryptanalysis of Block Ciphers with Overdefined Systems of Equations. In *Advances in Cryptology, Processdings of the ASIACRYPT 2002, Queenstown, New Zealand, 1–5 December 2002*; Zheng, Y., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2002; Volume 2501, pp. 267–287. ISBN 978-3-540-00171-3.
9. Yao, A.C. Theory and Application of Trapdoor Functions. In Proceedings of the 23rd Annual Symposium on Foundations of Computer Science (sfcs 1982), Chicago, IL, USA, 3–5 November 1982; IEEE Computer Society: Washington, DC, USA, 1982; pp. 80–91.
10. Boneh, D.; Shoup, V. A Graduate Course in Applied Cryptography. Version 0.5. 2020. Available online: http://toc.cryptobook.us/book.pdf (accessed on 17 March 2022).
11. Shannon, C.E. Communication Theory of Secrecy Systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
12. Levinskas, M.; Michalkovič, A. Avalanche Effect and Bit Independence Criterion of Perfectly Secure Shannon Cipher Based on Matrix Power. *Math. Model. Eng.* **2021**, *7*, 50–53.
13. Mihalkovich, A.; Sakalauskas, E.; Luksys, K. Key Exchange Protocol Defined over a Non-Commuting Group Based on an NP-Complete Decisional Problem. *Symmetry* **2020**, *12*, 1389. [CrossRef]
14. Sakalauskas, E.; Luksys, K. Matrix Power S-Box Construction. *Cryptology ePrint Archive*. 2007. Available online: https://eprint.iacr.org/2007/214.pdf (accessed on 17 March 2022).
15. Sakalauskas, E.; Dindienė, L.; Kilčiauskas, A.; Lukšys, K. Perfectly Secure Shannon Cipher Construction Based on the Matrix Power Function. *Symmetry* **2020**, *12*, 860. [CrossRef]