symmetry

MDPI

Article

Perfectly Secure Shannon Cipher Construction Based on the Matrix Power Function

Eligijus Sakalauskas [1,*], Lina Dindienė [1], Aušrys Kilčiauskas [2] and Kęstutis Lukšys [1]

[1] Department of Applied Mathematics, Kaunas University of Technology, 44249 Kaunas, Lithuania; lina.dindiene@ktu.lt (L.D.); kestutis.luksys@ktu.lt (K.L.)
[2] Department of Informatics, Kauno kolegija/University of Applied Science, 50468 Kaunas, Lithuania; ausrys.kilciauskas@go.kauko.lt
* Correspondence: eligijus.sakalauskas@ktu.lt

Received: 1 April 2020; Accepted: 6 May 2020; Published: 23 May 2020

Abstract: A Shannon cipher can be used as a building block for the block cipher construction if it is considered as one data block cipher. It has been proved that a Shannon cipher based on a matrix power function (MPF) is perfectly secure. This property was obtained by the special selection of algebraic structures to define the MPF. In an earlier paper we demonstrated, that certain MPF can be treated as a conjectured one-way function. This property is important since finding the inverse of a one-way function is related to an *NP*-complete problem. The obtained results of perfect security on a theoretical level coincide with the *NP*-completeness notion due to the well known Yao theorem. The proposed cipher does not need multiple rounds for the encryption of one data block and hence can be effectively parallelized since operations with matrices allow this effective parallelization.

Keywords: Shannon cipher; symmetric encryption; perfect security; block cipher

1. Introduction

The modern design of block ciphers is based on the confusion–diffusion paradigm introduced by Claude Shannon ([1]). A direct implementation of the above paradigm is a substitution–permutation network (SPN), which is used for the block cipher construction when it is realized in multiple rounds, each of which uses a different sub-key derived from the original key. This procedure is used for every data block encryption when all data is divided into separate blocks.

One of the examples of the SPN realization for standardized symmetric block cipher creation is the Data Encryption Standard (DES) adoption in 1977 ([2]). The corresponding block cipher was proposed on this basis. In order to increase the security of the DES, which is only 64 bits key length (while real security relies on 56 bits key length), the Tripple DES (TDES) algorithm was adopted by the ANSI committee X9.F.1 in 1998. Since this algorithm was popular and widely used, some special recommendations were accepted for the Triple Data Encryption Algorithm (TDEA) to modify the block cipher in 2017 ([3]).

The other sound realization of the SPN is the design of a block cipher adopted as an Advanced Encryption Standard (AES) ([4]).

We have restricted our consideration to a single data block encryption using the confusion–diffusion paradigm. Then, this encryption can be considered as the Shannon cipher outlined in ([5]). If the Shannon cipher is proved to be secure under certain conditions, then, on that basis, a secure block cipher can be created. Hence, Shannon cipher can be interpreted as a building block for the block cipher construction. The security of the Shannon cipher is considered in the sense of perfect security which is directly related to the notion of pseudo-randomness ([5]).

Perfect security, which is formulated in Lemma 1 in Section 4, is the "gold standard" in cryptography. Many security proofs are based on the computational relaxation of perfect security. The alternative definition of perfect security states that an encryption scheme is perfectly secure if no adversary can succeed with a probability any better than one half. That is, an adversary cannot be able to distinguish the encryption of one plaintext from the encryption of another. It is called adversarial indistinguishability. On the other hand, adversarial indistinguishability is related to pseudo-randomness. If an encryption key is chosen randomly and uniformly from the key space, the ciphertext is pseudo-random and uniformly distributed on any message space.

Yao A., C. [6] revealed a fundamental relation between one-way functions (OWFs) and pseudo-random generators. Yao A., C. theorem states that pseudo-random generators exist if and only if OWFs exist ([6]). Hence the intriguing idea is to construct a computationally effective block cipher using the one-way function (OWF). According to this, if the OWFs do exist, then a ciphertext is pseudo-random. Until the century dilemma P vs. NP is not solved (and it is unclear if it can be ever solved) it is believed that NP-complete problems can be accepted as the conjectured OWFs.

The notion of pseudo-randomness plays a fundamental role in cryptography, in general, and in private-key encryption, in particular. Loosely speaking, a pseudo-random string is a string that looks like a uniformly distributed string, as long as the entity that is "looking" runs in a polynomial time. Just as indistinguishability can be viewed as a computational relaxation of perfect secrecy, pseudo-randomness is a computational relaxation of true randomness.

The main reason of a Shannon cipher construction on the base of the MPF is that the MPF can be interpreted as a conjectured OWF. This conjectured OWF based on the MPF was proposed earlier in our papers ([7–11]) for some cryptographic protocol construction.

Some solutions of MPF application in a cryptographic function construction were proposed recently. In [12] the MPF is used for an asymmetric cipher construction, and in [13] for a digital signature algorithm. The MPF represents a class of non-commuting cryptography that is in the particular interest of a certain group of cryptographers. The linear algebra attack for cryptographic functions based on the MPF is presented in [14]. This attack was prevented in our subsequent paper [11].

In general, the MPF can be defined over different algebraic structures. [15] demonstrates that a conjectured OWF based on the MPF defined over a modified medial semigroup is NP-complete. Hence there is some evidence that the MPF could also be used for the block cipher construction.

This paper presents a Shannon cipher based on the matrix power function defined over the certainly-selected algebraic structures. The first result of a block cipher S-box construction using the MPF is published in [16].

The proof that Shannon cipher based on the MPF defined over the certainly-selected algebraic structures is perfectly secure is presented. A cipher with perfect secrecy is unconditionally secure against a ciphertext-only attack.

Thus far, the main trend of the block cipher construction used the number of rounds for one data block encryption to achieve a good confusion and diffusion, thus providing a required level of security. These rounds are performed sequentially and therefore there is no ability to parallelize computations.

The proposed Shannon cipher is realized in one round using matrix operations. The matrix operations in its turn can be effectively parallelized. So if we have two matrices of order n, then their addition, multiplication and powering matrix by matrix can be effectively performed using n (or integer fraction of n) parallel computations between n rows and n columns of operand matrices. In such a case, these computational results are the entries of a new matrix. Afterwards, obtained matrices are combined, forming a final matrix. Hence, the proposed Shannon cipher can be effectively realized in multiprocessor computation devices.

2. Mathematical Background

Conventionally the field of integers with additive and multiplication operations modulo 3 is denoted by $Z_3 = \{0,1,2\}$. Subset of Z_3 without zero element is denoted by $Z_{3\backslash 0} = \{1,2\}$. The third

order subgroup of multiplication group $Z_7^* = \{1, 2, \ldots, 6\}$ with multiplication operation modulo 7 is denoted by $G_3 = \{1,2,4\}$.

Let S be any finite set. The uniformly and randomly chosen element s in S we denote by

$$s \leftarrow \text{rand}(S).$$

Let f be a function

$$f : Z_3 \rightarrow G_3, \tag{1}$$

with the following mapping

$$f(0) = 4, f(1) = 2, f(2) = 1. \tag{2}$$

Evidently this mapping is one-to-one but not an isomorphism with respect to multiplication and addition operations defined in Z_3. Then there exists the inverse one-to-one mapping f^{-1} defined by Equation (2).

Let $Q = \{q_{ij}\}$ be a matrix with entries $q_{ij} \in G_3$. Denote, in general, matrices $X = \{x_{ij}\}$, $x_{ij} \in Z_3$ and $Y = \{y_{ij}\}$, $y_{ij} \in Z_3$. All matrices are square and of order n. Symbolically, the matrix power function (MPF) is defined in the following way:

$$^{X}Q^{Y} = C, \tag{3}$$

where matrix $C = \{c_{ij}\}$ is defined over G_3.

Group G_3 is named as a platform group and field Z_3 as a power field. Then formally matrices Q and C are defined over the group of direct product $G_3^{n \times n}$ and matrices X, Y over $Z_3^{n \times n}$.

Formally, the MPF is defined by the following relation

$$\prod_{t=1}^{m} \prod_{s=1}^{m} q_{st}^{x_{is} \cdot y_{tj}} = c_{ij}, \quad i, j = 1, 2..., m. \tag{4}$$

Then the MPF provides the following mapping

$$MPF : Z_3^{n \times n} \times G_3^{n \times n} \times Z_3^{n \times n} \rightarrow G_3^{n \times n}, \tag{5}$$

where $C = \{c_{ij}\}$ and $c_{ij} \in G_3$.

Let $C_1 = \{c_{1,ij}\}$ be a matrix defined over Z_3. Then mapping f defined in Equations (1) and (2) can be separately applied to all entries of matrix C_1, obtaining a mapping

$$F : Z_3^{n \times n} \rightarrow G_3^{n \times n}.$$

For all $C_1 \in Z_3^{n \times n}$ we have

$$F(C_1) = C_2,$$

where $C_2 \in G_3^{n \times n}$.

Mapping F just replaces all entries of matrix $C_1 = \{c_{1,ij}\}$ to the entries of matrix $C_2 = \{c_{2,ij}\}$, where, according to Equations (1) and (2), $f(c_{1,ij}) = c_{2,ij}$.

To construct symmetric cipher based on the MPF introduced by Equations (3)–(5) we need an additional matrix, namely matrix $M = \{m_{ij}\}$, $m_{ij} \in Z_3$ defining a message to be encrypted.

The symmetric encryption-decryption key K in our construction is represented by two invertible matrices K=(X, Y). To satisfy security conditions, the matrix Y must be invertible and its entries are randomly generated from the subset $Z_{3\backslash 0}$, i.e., $y_{ij} \in \{1, 2\}$. X is randomly generated from the subset Z_3, $x_{ij} \in \{0, 1, 2\}$.

3. Shannon Cipher Construction Based on the Matrix Power Function (MPF)

Conventionally, the Shannon cipher is any deterministic cipher. It is defined over the key space **K**, the message space **M** and the ciphertext space **C**.

Definition 1. *The Shannon cipher SC is defined by the following triplet* $SC = (Gen, Enc, Dec)$*, where*

- *Gen is a function of secret key K generation at random and uniformly distributed in* **K**.
- *Enc is the encryption function which takes as an input a key K in* **K** *and a message M in* **M** *and produces as output a ciphertext C in* **C**.

$$C = Enc(K, M).$$

- *Dec is a decryption function that takes as input a key K in* **K** *and a ciphertext C in* **C** *and produces a message M in* **M**.

$$M = Dec(K, C).$$

*The Shannon cipher is defined over (***K**,**M**,**C***) and with this notation we can write:*

$$Enc : \mathbf{K} \times \mathbf{M} \to \mathbf{C},$$
$$Dec : \mathbf{K} \times \mathbf{C} \to \mathbf{M}.$$

In general, it is assumed that M is a random variable distributed over the message space **M**, however, it is not assumed that M is uniformly distributed over **M**. The key K is uniformly distributed in **K** and is independent of M, while ciphertext $C = Enc(K, M)$ is a random variable distributed over the ciphertext space **C**.

The Shannon cipher is constructed for plaintext and ciphertext blocks defined by $n \times n$ matrices $M = \{m_{ij}\}$ and $C = \{c_{ij}\}$, respectively, over the field $Z_3 = \{0, 1, 2\}$, where $m_{ij} \in Z_3$ and $c_{ij} \in Z_3$. Hence the message space **M** consists of $n \times n$ matrices M and ciphertext space **C** of $n \times n$ matrices C and both spaces are denoted by $Z_3^{n \times n}$.

The key space **K** consists of two matrices X and Y composing a vector valued symmetric key $K = (X, Y)$, where $X = \{x_{ij}\}$, $x_{ij} \in Z_3$ and $Y = \{y_{ij}\}$, $y_{ij} \in Z_{3\setminus 0}$. Then the key space **K** is a direct product of the spaces $Z_3^{n \times n} \times Z_{3\setminus 0}^{n \times n}$. The additional requirement is that the matrix Y is an invertible matrix.

The encryption operation for one data block M consists of the following three steps:

$$\begin{aligned} C_1 &= X + M; \\ C_2 &= F(X) \odot^Y F(C_1)^Y; \\ C = C_3 &= F^{-1}(C_2) + X., \end{aligned} \tag{6}$$

where $+$ is a conventional matrix addition and $\odot$ is the Hadamard product of matrices, i.e., matrix entries are multiplied directly as it is done with a conventional matrix addition operation.

Symbolically, these steps can be expressed using three encryption functions Enc1, Enc2 and Enc3 in the following form

$$\begin{aligned} C_1 &= Enc1(X, M), \\ C_2 &= Enc2(X, Y, C_1), \\ C_3 &= Enc3(X, C_2). \end{aligned}$$

Equations (6) can be rewritten in one single equation

$$C = C_3 = F^{-1}(F(X) \odot^Y F(X + M)^Y) + X.$$

The obtained cipher C is a matrix of order n defined over Z_3 as a message matrix M.

For the decryption we need to introduce an inverse matrix in Hadamard sense in $G_3^{n\times n}$. Let a matrix T be in $G_3^{n\times n}$. Then the inverse matrix T^A, in Hadamard sense, of a matrix T is such that

$$T^A \odot T = T \odot T^A = \mathbb{1},$$

where $\mathbb{1}$ is a matrix consisting of all elements equal to $\mathbb{1} \in G_3$.

The decryption procedure is performed in a reverse order. Since matrix Y has its inverse in $Z_{3\setminus 0}^{n\times n}$, while algebraic structures, namely, group G_3 and field Z_3, are symmetric, then

$$M = (F^{-1}(^{Y^{-1}}\left[(F(X))^A \odot F(C-X)\right]^{Y^{-1}}) - X,$$

where $F(X)^A$ is an inverse matrix of matrix $F(X)$ in Hadamard sense and $\odot$ is the Hadamard product of matrices.

By fixing a uniformly and randomly generated key K, two arguments of encryption function $Enc(,)$ can be interpreted as the following one-to-one permutation function $\Pi_K(M) : Z_3^{n\times n} \to Z_3^{n\times n}$, where

$$\begin{aligned} \Pi_K(M) &= Enc(K, M) = C, \\ \Pi_{K^{-1}}(M) &= Dec(K, C) = M. \end{aligned}$$

Looking forward, we intend that the constructed Shannon cipher could be suitable to creating a block cipher with one round per block M operation. The defined block length is $|M| = |Z_3^{n\times n}| = 3n^2$, composed of digits in Z_3. The main property required for this application is that Π_K should behave like a random permutation. However, since a random permutation realization having a practically acceptable block length is impractical, the notion of pseudo-random permutation is introduced. Intuitively, we can call Π_K pseudorandom if for a randomly and uniformly chosen key K it is indistinguishable from a function chosen uniformly at random from the set of all functions having the same domain and range. For this reason, Shannon introduced the confusion–diffusion paradigm ([1]).

A direct implementation of the confusion–diffusion paradigm is a substitution–permutation network ([17,18]). There are two confusion phases, namely C_1 and C_3 in Equation (6). The encryption key for these operations is matrix X. The diffusion phase is realized for computing C_2 in intermediately encrypted data block $F(C_1)$ in $G_3^{n\times n}$.

In the next section we demonstrate that Π_K is a perfectly secure pseudo-random permutation.

4. Security Analysis

Let M_0 be a fixed value in a message space **M** and $C_0 = Enc(K, M_0)$ is in **C**. Referencing to [5] the following Lemma can be formulated.

Lemma 1. *An encryption scheme* (Gen, Enc, Dec) *over a message space* **M** *is perfectly secret if and only if for every probability distribution over* **M**, *every message* $M \in$ **M**, *and every ciphertext* $C \in$ **C**

$$Pr(C = C_0 | M = M_0) = Pr(C = C_0), \tag{7}$$

which means that conditional probability is equal to unconditional probability and hence a ciphertext is independent from the message.

Before proving the main theorem of perfect security we need to prove the following lemmas.

Lemma 2. *If random variables* z_1, z_2 *are independent and uniformly distributed in* $Z_{3\setminus 0}$, *and* w *is uniformly distributed in* G_3 *independent of* z_1 *and* z_2, *then distribution of* $z_1 \cdot z_2$ *is uniform in* $Z_{3\setminus 0}$, *and random variable* $w^{z_1 \cdot z_2}$ *has uniform distribution in* G_3.

Proof. Since z_1 is z_2 are independent, we can easily write the following probabilities:

$$Pr(z_1 \cdot z_2 = j) \quad = \quad \sum_{j_1 \cdot j_2 = j} Pr(z_1 = j_1, z_2 = j_2) = 2\left(\frac{1}{2}\right)^2 = \frac{1}{2}, \;\; j = \{1,2\},$$

where summation under $j_1 \cdot j_2 = j$ gives two possible combinations of $j_1, j_2 \in Z_{3\backslash 0}$ (see contingency Table 1).

Table 1. Table of $z_1 \cdot z_2$.

z_1	z_2	$z_1 \cdot z_2$
1	1	1
1	2	2
2	1	2
2	2	1

According to the above, $z_1 \cdot z_2$ is uniformly distributed in $Z_{3\backslash 0}$.

Denote $u = z_1 \cdot z_2$. Under the assumption of an independence we get the following probabilities (that is also seen in Table 2):

$$Pr(w^u = j) \quad = \quad \sum_{j_1^{j_2} = j} Pr(w = j_1, u = j_2) = 2\left(\frac{1}{6}\right) = \frac{1}{3}, \;\; j = \{1,2,4\},$$

where summation under $j_1^{j_2} = j$ gives two pairs of j_1, j_2 ($j_1 \in G_3, j_2 \in Z_{3\backslash 0}$) to be equal to each j.

Table 2. Table of power function.

w	u	w^u
1	1	1
1	2	1
2	1	2
2	2	4
4	1	4
4	2	2

These probabilities imply that distribution of w^u is uniform in G_3 and the lemma is proved. □

Lemma 3. *If random variables $v_1, v_2, \ldots v_n$ are independent and uniformly distributed in G_3, then the distribution of $v_1 v_2 \ldots v_n$ is uniform in G_3.*

Proof. In case $n = 2$, this lemma is simply proven by contingency Table 3.

Table 3. Table of $v_1 \cdot v_2$.

v_1	v_2	$v_1 \cdot v_2$
1	1	1
1	2	2
1	4	4
2	1	2
2	2	4
2	4	1
4	1	4
4	2	1
4	4	2

Or, in short,

$$Pr(v_1 \cdot v_2 = j) \quad = \quad \sum_{j_1 \cdot j_2 = j} Pr(v_1 = j_1, v_2 = j_2) = 3\left(\frac{1}{9}\right) = \frac{1}{3}, j \in G_3,$$

where summation under $j_1 \cdot j_2 = j$ gives three possible combinations of $j_1, j_2 \in G_3$.

We assume that the lemma holds for $n = N$:

$$Pr(v_1 v_2 \dots v_N = j) = \frac{1}{3}, \ \ j \in G_3. \tag{8}$$

It is sufficient to show that lemma is valid for $n = N + 1$, which follows directly from the assumption of independent random variables and Equation (8):

$$Pr(v_1 v_2 \dots v_N v_{N+1} = j) \quad = \quad \sum_{j_1 \cdot j_2 = j} Pr(v_1 v_2 \dots v_N = j_1) Pr(v_{N+1} = j_2) = \sum_{j_1 \cdot j_2 = j} \frac{1}{3} \cdot \frac{1}{3} = \frac{1}{3}.$$

Hence the lemma is proven. □

The Theorem of Perfect Security

Referencing to Lemma 1–3, we prove the following theorem.

Theorem 1. *If a key K is chosen randomly and uniformly from* **K**, *the probability distribution of M over* **M** *is arbitrary, the distributions of K and M over* **K** *and* **M** *are independent and given the encryption algorithm Enc, the distribution of C over* **C** *is fully determined by the distributions over* **K** *and* **M**, *then the Shannon cipher in Equation* (6) *based on MPF is perfectly secure.*

Proof. Each element of matrix C_1 in Equation (6) of order n takes the following form:

$$c_{1,ij} = x_{ij} + m_{ij}, \ \ i, j \in \{1, \dots, n\}.$$

If x_{ij} are chosen at random and are uniformly distributed, and m_{ij} are random arbitrary distributed values in Z_3, then for all $c_{10} \in Z_3$

$$Pr(c_{1,ij} = c_{10}) \quad = \quad Pr(x_{ij} = c_{10} - m_{ij}) = \frac{1}{3} \sum_{m_0 \in Z_3} Pr(m_{ij} = m_0) = \frac{1}{3}. \tag{9}$$

Probability in Equation (9) can be seen directly from the table of values (see Table 4).

Table 4. Table of $c_{1,ij}$.

c_{10}	m_0	$-m_0$	x_{ij}
0	0	0	0
0	1	2	2
0	2	1	1
1	0	0	1
1	1	2	0
1	2	1	2
2	0	0	2
2	1	2	1
2	2	1	0

Conditional probabilities:

$$Pr(c_{1,ij} = c_{10} | m_{ij} = m_0) \quad = \quad P(x_{ij} = c_{10} - m_0) = \frac{1}{3}, \tag{10}$$

because x_{ij} and m_{ij} are independent, and $c_{10} - m_0 \in Z_3$.

Equalities (9) and (10) prove, that

$$Pr(C_1 = C_{10}) = Pr(C_1 = C_{10} | M = M_0) = \frac{1}{3}. \tag{11}$$

Let us turn to matrix C_2 of Equation (6). Denote the elements of matrix C_2 of order n by:

$$\begin{aligned} c_{2,ij} &= f(x_{ij})(f(c_{11}))^{y_{11}y_{11}}(f(c_{21}))^{y_{12}y_{11}} \dots (f(c_{nn}))^{y_{nn}y_{nn}} \\ &= f(x_{ij})(f(c_{11}))^{y_1}(f(c_{21}))^{y_2}(f(c_{12}))^{y_3} \dots (f(c_{nn}))^{y_{n \cdot n}}, \ \ i,j \in \{1,\dots,n\}, \end{aligned}$$

where y_{ij} are chosen randomly and are uniformly distributed over $Z_{3\backslash 0}$ and $f(c_{ij}) \in G_3$. According to Lemma 2, multiplication $y_{ij} \cdot y_{kl}$ is uniformly distributed (in $Z_{3\backslash 0}$) random value and all $(f(c_{ij}))^{y_k}$ are uniformly distributed in G_3. For simplicity, denote $y_{ij} \cdot y_{kl} = y_s, s \in \{1,\dots,n \cdot n\}$.

Since $c_{2,ij}$ is the product of $(n \cdot n + 1)$ independent random variable from G_3, Lemma 3 yields that for all $c_{20} \in G_3$ and $i,j = 1,\dots,n$:

$$Pr(c_{2,ij} = c_{20}) = \frac{1}{3}. \tag{12}$$

Conditional probabilities of elements of matrix C_2 are the following:

$$\begin{aligned} &Pr(c_{2,ij} = c_{20} | c_{11} = c_{11,0}, \dots, c_{nn} = c_{nn,0}) \\ &= \quad Pr(c_{2,ij} = c_{20} | f(c_{11}) = z_{11,0}, \dots, f(c_{nn}) = z_{nn,0}) = \frac{Pr(c_{2,ij}=c_{20}, z_{11}=z_{11,0}, \dots, z_{nn}=z_{nn,0})}{Pr(z_{11}=z_{11,0}, \dots, z_{nn}=z_{nn,0})}, \end{aligned} \tag{13}$$

here $z_* = f(c_*)$. Using the independence of matrices X, Y and C_1:

$$\begin{aligned} &Pr(c_{2,ij} = c_{20}, z_{11} = z_{11,0}, \dots, z_{nn} = z_{nn,0}) \\ &= \quad \mathrm{P}(f(x_{ij}) \cdot z_{11}^{y_1} \cdot \dots \cdot z_{nn}^{y_{n \cdot n}} = c_{20}, z_{11} = z_{10}, \dots, z_{nn} = z_{nn,0}) \\ &= \quad \mathrm{P}(f(x_{ij}) = c_{20}(z_{10}^{y_1} \cdot \dots \cdot z_{nn,0}^{y_{n \cdot n}})^{-1}, z_{11} = z_{11,0}, \dots, z_{nn} = z_{nn,0}) \\ &= \quad \textstyle\sum_{k_1,\dots,k_{n \cdot n} \in Z_{3\backslash 0}} \mathrm{P}\big(f(x_{ij}) = c_{20}(z_{10}^{k_1} \cdot \dots \cdot z_{nn,0}^{k_{n \cdot n}})^{-1}, \bigcap_{i=1}^{n \cdot n} y_i = k_i, \bigcap_{i,j=1}^{n} z_{ij} = z_{ij,0}\big) \\ &= \quad \tfrac{1}{3}\mathrm{P}(z_{11} = z_{10}, \dots, z_{nn} = z_{nn,0}). \end{aligned} \tag{14}$$

According to Lemma 3, expression $(z_{11}^{y_1} \cdot \dots \cdot z_{nn}^{y_{n \cdot n}})$ takes values in G_3.

The inverse variables are also in G_3 (see Table 5).

Table 5. Table of inverse variables.

z^y	$(z^y)^{-1}$
1	1
2	4
4	2

Equalities (12)–(14) prove, that

$$Pr(C_2 = C_{20}) = Pr(C_2 = C_{20} | C_1 = C_{10}) = \frac{1}{3}, \tag{15}$$

that is, elements of matrix C_2 are independent of the elements of matrix C_1. Since matrix M is in the expression of C_1, matrix C_2 is independent of M too.

The third equation in Equation (6) for each element of the matrix of order n can be rewritten in the following form

$$c_{3,ij} = f^{-1}(c_{2,ij}) + x_{ij}, \;\; i,j \in \{1,\ldots,n\}.$$

Similarly as in Equations (9) and (10) we obtain that

$$Pr(C_3 = C_{30}|C_2 = C_{20}) = Pr(C_3 = C_{30}) = \frac{1}{3}. \tag{16}$$

Thus, the elements of matrix C_3 are independent of the elements of matrix C_2. By this, C_3 does not depend on the value of M.

By taking equalities (11), (15) and (16) all together it is proved that Equation (7) holds. Hence we have proved that the proposed Shannon cipher is perfectly secure. □

5. Conclusions and Discussions

One realization of the Sahnnon cipher is proposed. It is based on the MPF defined over specially selected algebraic structures, namely the finite field of integers Z_3 and the subgroup G_3 of group Z_7 of residue classes modulo 7. Due to this special selection, it is proved that the proposed Shannon cipher is perfectly secure.

Such a cipher can be interpreted as one data block cipher consisting of $n \times n$ digits in Z_3. The data in this block is encoded by numbers $\{0,1,2\}$, i.e., by two bits. The obtained result can be extended to the block cipher construction if the entire data is split into the different blocks of length of $n \times n$ digits. Then we directly obtain the Electronic Code Book (ECB) mode of encryption and on this base, the other known secure modes of encryption, e.g., Cipher Block Chaining (CBC), can be constructed.

This research proves that the proposed confusion–diffusion transformation provides perfect security in a single round of operation. The distinguishing property of the proposed cipher is that it does not require a number of round operations for one data block encryption.

The single round operation for a single data block encryption is based on matrix operations. That is a result of the other distinguishing property, namely, that one block encryption can be carried out by effectively parallelizing encryption computations. Since round operations in traditional ciphers must be performed sequentially, the parallelization of round operations cannot be realized in such a case.

The matrix operations can be effectively parallelized. Let us assume we have two operand matrices of order n. Then their addition, Hadamard product and powering matrix by matrix can be effectively performed using n (or integer fraction of n) parallel computations between n rows and n columns of operand matrices. The entries of the resulting matrix are computed in parallel using operations between two n-dimensional vectors. For matrix addition or Hadamard product, two vectors are added or multiplied representing two columns (or rows) of corresponding operand matrices. For matrix powering by matrix, one base vector is powered by the other power vector elementwise, and power operation results are multiplied together. The analogy of this operation can be found in an inner product of two vectors, when addition is replaced with multiplication and multiplication with exponentiation operations, respectively. This parallelization allows us to replace the operations between matrices of order n to n operations between n-dimensional vectors.

For example, let us have a data block size represented by matrix of order $n = 16$. Such a data block has $16 \times 16 = 256$ elements encoded by the numbers $\{0,1,2\}$. Then, parallel computations can be performed using $16, 8, 4$ or even 2 microprocessors. Hence, the proposed Shannon cipher can be effectively realized in multiprocessor computation devices.

Author Contributions: Conceptualization, E.S. and K.L.; Methodology, E.S.; Investigation L.D.; Formal analysis, L.D. and A.K.; Validation, A.K.; Supervision K.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no fund.

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

References

1. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
2. Data Encryption Standard (DES). *Federal Information Processing Standards Publication 197*; United States National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA,1977.
3. Special Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher. *National Institute of Standards and Technology (NIST) Publication*; Revision 2; Department of Commerce, National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA, 2017; pp. 800–867.
4. Advanced Encryption Standard (AES). *Federal Information Processing Standards Publication 197*; United States National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA, 2001; Volume 197.
5. Boneh, D.; Shoup, V. A Graduate Course in Applied Cryptography. Available online: https://toc.cryptobook.us/ (accessed on 31 March 2020).
6. Yao, A.C. Theory and applications of trapdoor functions. In Proceedings of the 23rd Annual Symposium on Foundations of Computer Science, (sfcs 1982), Chicago, IL, USA, 3–5 November 1982; Volume 80–91.
7. Sakalauskas, E.; Listopadskis, N.; Tvarijonas, P. Key Agreement Protocol (KAP) Based on Matrix Power Function. *Information Science And Computing, Book 4 Advanced Studies in Software and Knowledge Engineering*; Institute of Information Theories and Applications FOI ITHEA: Sofia, Bulgaria, 2008; Volume 4, pp. 92–96.
8. Sakalauskas, E. The Multivariate Quadratic Power Problem Over Zn is NP-Complete. *Inf. Technol. Control* **2012**, *41*, 33–39. [CrossRef]
9. Sakalauskas, E.; Mihalkovich, A.; Venčkauskas, A. Improved asymmetric cipher based on matrix power function with provable security. *Symmetry* **2017**, *9*, 9. [CrossRef]
10. Sakalauskas, E. Enhanced matrix power function for cryptographic primitive construction. *Symmetry* **2018**, *10*, 43. [CrossRef]
11. Sakalauskas, E.; Mihalkovich, A. Improved Asymmetric Cipher Based on Matrix Power Function Resistant to Linear Algebra Attack. *Informatica* **2017**, *28*, 517–524. [CrossRef]
12. Noor, S. Cryptographic Schemes Based on Enhanced Matrix Power Function. Ph.D. Thesis, Capital University, Bexley, OH, USA, 2019.
13. Iqbal, S. Digital Signature Based on Matrix Power Function. Ph.D. Thesis, Capital University, Bexley, OH, USA, 2019.
14. Liu, J.; Zhang, H.; Jia, J. A Linear Algebra Attack on the Non-commuting Cryptography Class Based on Matrix Power Function. *International Conference on Information Security and Cryptology. Inscrypt 2016: Information Security and Cryptology*; Springer: Cham, Swizerland, 2017; Volume 10143, pp. 343–354.
15. Sakalauskas, E.; Mihalkovich, A. MPF Problem over Modified Medial Semigroup Is NP-Complete. *Symmetry* **2018**, *10*, 571. [CrossRef]
16. Sakalauskas, E.; Lukšys, K. The matrix power function and its application to block cipher S-box construction. *Int. J. Innov. Comput. Inf. Control;* **2012**, *8*, 2655–2663.
17. Feistel, H. Cryptography and computer privacy. *Sci. Am.* **1973**, *228*, 15–23. [CrossRef]
18. Heys, H.M. The Design of Substitution-Permutation Network Ciphers Resistant to Cryptanalysis. Ph.D. Thesis, Queen's University, Kingston, ON, Canada, 1994.