Turkish Journal of Engineering

Turkish Journal of Engineering (TUJE)
Vol. 4, Issue 3, pp. 123-128, July 2020
ISSN 2587-1366, Turkey
DOI: 10.31127/tuje.646926
Research Article

THE CLASSICAL AES-LIKE CRYPTOLOGY VIA THE FIBONACCI POLYNOMIAL MATRIX

Orhan Dişkaya *1, Erdinç Avaroğlu 2 and Hamza Menken 3

1 Mersin University, Graduate School of Natural and Applied Sciences, Ciftlikkoy, Mersin, TURKEY
ORCID ID 0000-0001-5698-7834
orhandiskaya@mersin.edu.tr

2 Mersin University, Computer Engineering Department, Ciftlikkoy, Mersin, TURKEY
ORCID ID 0000-0003-1976-2526
eavaroglu@mersin.edu.tr

3 Mersin University, Department of Mathematics Ciftlikkoy, Mersin, TURKEY
ORCID ID 0000-0003-1194-3162
hmenken@mersin.edu.tr

* Corresponding Author

Received: 14/11/2019 Accepted: 23/12/2019

ABSTRACT
Galois field, has an important position in cryptology. Advanced Encryption Standard (AES) also used in polynomial operations. In this paper, we consider the polynomial operations on the Galois fields, the Fibonacci polynomial sequences. Using a certain irreducible polynomial, we redefine the elements of Fibonacci polynomial sequences to use in our cryptology algorithm. So, we find the classical AES-like cryptology via the Fibonacci polynomial matrix. Successful results were achieved with the method used.

Keywords: *Fibonacci Numbers, Fibonacci Polynomial Numbers, Cassini Identity, Fibonacci Matrix, Galois Field*

1. INTRODUCTION

The Advanced Encryption Standard (AES), also known by its original name Rijndael (Daemen and Rijmen, 2003), is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. The AES block encryption algorithm is used for the algorithmic part of the developed system. AES is the applicable block encryption standard developed by J. Daemen and V. Rijmen in 1997 and adopted as a standard in 2000. AES is an iterative block cipher based on a design principle known as a substitution-permutation network (SPN). AES operates on a 4×4 column-major order matrix of bytes, called the state. Matrix calculations are done in a special finite field. AES supports 128-, 192-, 256- bit keys. The number of cycles of repetition for 128-bit, 192-bit, and 256-bit keys are 10, 12, and 14, respectively. These stages include key addition, byte substitution, ShiftRow, and MixColumn (Avaroğlu, Koyuncu, Özer and Türk, 2015). We too created a new encryption algorithm (known as AES-like) by using the AES algorithm. In AES-like, Galois field arithmetic is used in most layers, especially in matrix operations. We give an introduction to Galois fields as needed for this purpose before we introduced with the algorithm. A background on Galois fields is not needed for a basic understanding of AES-like. So, we will obtain a basic entrance to Galois fields (Paar and Pelzl, 2009; Stewart, 1990). Information on the following classical cryptology benefit in (Klima and Sigmon, 2012).

1.1. Definition : In (Paar and Pelzl, 2009). A field F is a set of elements with the following features:

1. All elements of F form an additive group with the group operation + and the neutral element 0.
2. All elements of F except 0 form a multiplicative group with the group operation × and the neutral element 1.
3. When the two group operations are mixed, the distributive law holds, i.e., for all $a,b,c \in F$:
$$a\left(b+c\right)=ab+ac.$$

In extension fields $GF\left(2^m\right)$ elements are not represented as integers but as polynomials with coefficients in $GF\left(2\right)$. However, we take $m=5$ for the next process. In AES-like the finite field contains 32 elements and is denoted as $GF\left(2^5\right)$. In the field, $GF\left(2^5\right)$, which is used in AES-like, each element $A\in GF\left(2^5\right)$ is thus represented as:

$$A\left(x\right)=a_4x^4+a_3x^3+a_2x^2+a_1x+a_0,$$
$$\left\{a_i\right\}\in GF\left(2\right)=\left\{0,1\right\}$$

Note that there are exactly $32=2^5$ such polynomials. The set of these 32 polynomials is the finite field $GF\left(2^5\right)$. Each elements of this polynomial correspond to one letter of the alphabet.

1.2. Definition : (Addition and subtraction in $GF\left(2^5\right)$). In (Paar and Pelzl, 2009). Let $A\left(x\right),B\left(x\right)\in GF\left(2^5\right)$. The sum and the subtraction of the two elements are then computed according to:

$$A\left(x\right)\pm B\left(x\right)=\left(a_4\pm b_4\right)x^4+\left(a_3\pm b_3\right)x^3$$
$$+\left(a_2\pm b_2\right)x^2+\left(a_1\pm b_1\right)x+\left(a_0\pm b_0\right),$$
$$\left(a_i\pm b_i\right)\bmod 2 \ \text{ for } \ i\in\left\{0,1,2,3,4\right\}$$

1.3. Example: For $A\left(x\right)=x^4+x^2+x$ and $A\left(x\right)=x^4+x^3+x^2+1$, the sum $A\left(x\right)+B\left(x\right)$ of two elements from $GF\left(2^5\right)$ is computed:

$$A(x)+B(x)=x^3+x+1.$$

1.4. Definition: (Multiplication in $GF\left(2^5\right)$). In (Paar and Pelzl, 2009). Let $A\left(x\right),B\left(x\right)\in GF\left(2^5\right)$ and let

$$P\left(x\right)=p_0+p_1x+p_2x^2+p_3x^3+p_4x^4+p_5x^5,$$
$$p_i\in GF\left(2^5\right)$$

be an irreducible polynomial. Multiplication of the two elements $A\left(x\right),B\left(x\right)$ is performed as

$$A\left(x\right).B\left(x\right)\bmod P\left(x\right).$$

The irreducible polynomials of $GF(2^5)$ are as follows,
x^5+x^2+1,
x^5+x^3+1,
$x^5+x^3+x^2+x+1$,
$x^5+x^4+x^3+x+1$,
$x^5+x^4+x^3+x^2+1$,
$x^5+x^4+x^2+x+1$.
For AES, the irreducible polynomial
$P(x)=x^8+x^4+x^3+x+1$
is used. It is part of the AES specification. For AES-like, we consider the irreducible polynomials as following,
$P(x)=x^5+x^2+1$.

1.5. Example: For $A(x)=x^4+x^2+1$ and $B(x)=x^3+x$ in the field $GF(2^5)$, the multiplication $A(x).B(x)$ according to the irreducible polynomial $P(x)=x^5+x^2+1$ is
$A(x).B(x)=x^7+x=x^2(x^2+1)+x=x^4+x^2+x.$
Especially, we are concerned with software implementations of the Galois fields. Hence, we know
$A(x)=x^4+x^2+1=(10101)_2=21_{10}$
$B(x)=x^3+x=(01010)_2=10_{10}$.
The field elements, are normally stored as bit vectors in the computers. If we look at the multiplication from the previous example, the following very atypical operation is being performed on the bit level:
$A(x).B(x)=(x^4+x^2+1)(x^3+x)=x^4+x^2+x$
$$(10101)(01010)=(10110)$$

This computation is not identical to integer arithmetic. The result would have been $(01101)_2=13_{10}$, which is clearly not the same as the Galois field multiplication product. Inversion in $GF(2^5)$ is the core operation to decrypt of the matrix polynomial.

1.6. Definition: In (Paar and Pelzl, 2009). For a given field $GF(2^5)$ and the corresponding irreducible reduction polynomial $P(x)$, the inverse A^{-1} of a nonzero element $A \in GF(2^5)$ is defined as:

$$A^{-1}(x)A(x) = 1 mod P(x).$$

1.7. Definition: In (Koshy, 2018; 2019). The Fibonacci sequence $\{F_n\}_{n\geq 0}$ is

$$F_0 = 0,\ F_1 = 1 \text{ and } F_{n+2} = F_{n+1} + F_n.$$

Here, F_n is the nth Fibonacci number. The first few members of this sequence is given as follow;

n	0	1	2	3	4	5	6	7	8	...
F_n	0	1	1	2	3	5	8	13	21	...

Table 1. A few the Fibonacci numbers

1.8. Definition: In (Koshy, 2018; 2019). The Fibonacci Polynomial sequence $\{f_n(x)\}_{n\geq 0}$ is

$$f_0(x) = 0,\ f_1(x) = 1 \text{ and } f_{n+2}(x) = xf_{n+1}(x) + f_n(x).$$

The first few members of this sequence is given as follow;

Table 2. A few the Fibonacci polynomial numbers

n	0	1	2	3	4	5	...
$f_n(x)$	0	1	x	x^2+1	x^3+2x	x^4+3x^2+1	...

According to irreducible polynomial $P(x)$ the Fibonacci polynomials $f_n(x)$ are as follows;

Table 3. A few the irreducible polynomial numbers

n	$f_n(x)$	Z_2
0	0	mod 2
1	1	mod 2
2	x	mod 2
3	$x^2 + 1$	mod 2
4	x^3	mod 2
5	$x^4 + x^2 + 1$	mod 2
6	$x^2 + x + 1$	mod 2
7	$x^4 + x^3 + x + 1$	mod 2
8	$x^4 + x^2$	mod 2
9	$x^4 + x^2 + x$	mod 2
...	...	...

The following identity is non-zero, which tells us that Fibonacci polynomial matrix can be reversed,

1.9. Theorem (Cassini Identity): In (Koshy, 2018; 2019). Let $f_n(x)$ denote the nth Fibonacci polynomial sequence. Then,

$$f_{n+1}(x)\, f_{n-1}(x) - f_n^2(x) = (-1)^n, \quad n \geq 1.$$

1.10. Theorem (Fibonacci Polynomial Matrix): In [3, 4]. Let,

$$Q(x) = \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix}$$

It then follows by inductive method that,

$$Q^n(x) = \begin{pmatrix} f_{n+1}(x) & f_n(x) \\ f_n(x) & f_{n-1}(x) \end{pmatrix}$$

where $n \geq 1$. $Q^n(x)$ is called the Fibonacci polynomial matrix.

1.11. Theorem (Inverse of a 2x2 Matrix): Let $Q^n(x)$ be a Fibonacci Polynomial Matrix. Let $Q^n(x)$ be the Fibonacci polynomial matrix. Then, the determinant of $Q^n(x)$ is

$$|Q^n(x)| = f_{n+1}(x)\, f_{n-1}(x) - f_n^2(x) = 1.$$

and inverse of $Q^n(x)$ is given by

$$Q^n(x)^{-1} = \begin{pmatrix} f_{n-1}(x) & f_n(x) \\ f_n(x) & f_{n+1}(x) \end{pmatrix}.$$

Polynomials of the Galois field are equivalent of each alphabet is as following,

Table 4.The polynomials are equivalent of each alphabet

No	Bit	Polynom	Alphabet
0	00000	0	A
1	00001	1	B
2	00010	x	C
3	00011	$x + 1$	Ç
4	00100	x^2	D
5	00101	$x^2 + 1$	E
6	00110	$x^2 + x$	F
7	00111	$x^2 + x + 1$	G
8	01000	x^3	Ğ
9	01001	$x^3 + 1$	H
10	01010	$x^3 + x$	I
11	01011	$x^3 + x + 1$	İ
12	01100	$x^3 + x^2$	J
13	01101	$x^3 + x^2 + 1$	K
14	01110	$x^3 + x^2 + x$	L
15	01111	$x^3 + x^2 + x + 1$	M
16	10000	x^4	N
17	10001	$x^4 + 1$	O
18	10010	$x^4 + x$	Ö
19	10011	$x^4 + x + 1$	P
20	10100	$x^4 + x^2$	R
21	10101	$x^4 + x^2 + 1$	S
22	10110	$x^4 + x^2 + x$	Ş

23	10111	$x^4 + x^2 + x + 1$	T
24	11000	$x^4 + x^3$	U
25	11001	$x^4 + x^3 + 1$	Ü
26	11010	$x^4 + x^3 + x$	V
27	11011	$x^4 + x^3 + x + 1$	W
28	11100	$x^4 + x^3 + x^2$	X
29	11101	$x^4 + x^3 + x^2 + 1$	Y
30	11110	$x^4 + x^3 + x^2 + x$	Z
31	11111	$x^4 + x^3 + x^2 + x + 1$	Q

2. MAIN RESULTS

In the present work, we consider a message text in ns lengths (called the n-letter). Then, this messaging creates a cryptology algorithm using certain mathematical rules (Fibonacci polynomial matrix). We obtain a decryption algorithm by applying inversely of the stated mathematical rules. Similar investigations on the following algorithm were given in (Uçar, Taş, and Özgür, 2017).

2.1. The Fibonacci Blocking Algorithm: The Coding Algorithm

Step 1. Consider a text of length n and assume that each letter represents one length.

Step 2. Divide the text into 2s blocks and transform it into 2×1 matrices. 2×1 matrices are multiplied by the *n-th* Fibonacci polynomial matrix in 2×2 . If there is an ascending letter in the text that is converted into 2s block, its letters are multiplied $f_n(x)$.

Step 3. Divide the latest created text into 3s blocks and transform it into 3×1 matrices. 3×1 matrices are multiplied by the key matrix in 3×3 :

$$\text{Key matrix} = \begin{pmatrix} B & B & C \\ Ç & E & \breve{G} \\ K & E & Y \end{pmatrix} = \begin{pmatrix} 1 & 1 & 2 \\ 3 & 5 & 8 \\ 13 & 5 & 30 \end{pmatrix}$$

If there is an ascending 2 letter in the text that is converted into 3s block, it letters is multiplied by 2.key matrix in 2×2 :

$$\text{2.Key Matrix} = \begin{pmatrix} E & A \\ O & D \end{pmatrix} = \begin{pmatrix} 5 & 0 \\ 17 & 4 \end{pmatrix}$$

If there is an ascending letter in the text that is converted into 3-block, its letters are multiplied by polynomial *”F”*.

Step 4. New text created in step 3 is addition by Fibonacci polynomial numbers $\sum_{i=1}^{n} f_i(x)$ respectively by starting from the left.

$$\sum_{i=1}^{n} f_i(x) = f_1(x) + f_2(x) + f_3(x) + \ldots + f_n(x).$$

The Decoding Algorithm

Step 1. Consider encrypted a text of length n and assume that each letter represents one length.

Step 2. Encrypted text is addition by Fibonacci polynomial numbers $\sum_{i=1}^{n} f_i(x)$ respectively by starting from the left:

$$\sum_{i=1}^{n} f_i(x) = f_1(x) + f_2(x) + f_3(x) + \ldots + f_n(x).$$

Step 3. Divide the encrypted text into 3s blocks and transform it into 3×1 matrices. 3×1 matrices are multiplied by the inverse of the key matrix in 3×3 :

$$\text{Inverse Key matrix} = \begin{pmatrix} F & Ç & Z \\ S & \breve{G} & N \\ V & T & G \end{pmatrix} = \begin{pmatrix} 6 & 3 & 30 \\ 22 & 8 & 16 \\ 26 & 23 & 7 \end{pmatrix}$$

If there is an ascending 2 letter in the encrypted text that is converted into 3s block, its letters are multiplied by the inverse of the 2.Key Matrix.

$$\text{Inverse 2.Key Matrix} = \begin{pmatrix} T & A \\ \breve{G} & H \end{pmatrix} = \begin{pmatrix} 23 & 0 \\ 8 & 9 \end{pmatrix}.$$

If there is an ascending letter in the encrypted text that is converted into 3s block, its letters are multiplied by *”L”* polynomial.

Step 4. Divide the encrypted text into 2s blocks and transform it into 2×1 matrices. 2×1 matrices are multiplied by the nth inverse of the Fibonacci polynomial matrix. If there is an ascending letter in the encrypted text that is converted into 2s block, it letters is multiplied the inverse of $f_n(x)$.

2.2. Example of the Fibonacci Blocking Algorithm:

Consider the following message text in 5s lengths (called the 5-letter):
”HELLO”

The Application of The Coding Algorithm

Step 1. HELLO is 5-letter that means $n=5$.

Step 2.

$$Q^5(x) = \begin{pmatrix} f_6(x) & f_5(x) \\ f_5(x) & f_4(x) \end{pmatrix} = \begin{pmatrix} x^2+x+1 & x^4+x^2+1 \\ x^4+x^2+1 & x^3 \end{pmatrix}$$

It is known that

$$9 = (01001) = x^3 + 1 = H$$

$$5 = (00101) = x^2 + 1 = E$$

$$14 = (01110) = x^3 + x^2 + x = L$$

$$17 = (10001) = x^4 + 1 = O$$

So, It is

$$\begin{pmatrix} f_6(x) & f_5(x) \\ f_5(x) & f_4(x) \end{pmatrix}\begin{pmatrix} H \\ E \end{pmatrix} = \begin{pmatrix} x^2+x+1 & x^4+x^2+1 \\ x^4+x^2+1 & x^3 \end{pmatrix}\begin{pmatrix} x^3+1 \\ x^2+1 \end{pmatrix}$$

$$= \begin{pmatrix} x^4+1 \\ 1 \end{pmatrix} = \begin{pmatrix} O \\ B \end{pmatrix},$$

$$\begin{pmatrix} f_6(x) & f_5(x) \\ f_5(x) & f_4(x) \end{pmatrix}\begin{pmatrix} L \\ L \end{pmatrix} = \begin{pmatrix} x^2+x+1 & x^4+x^2+1 \\ x^4+x^2+1 & x^3 \end{pmatrix}\begin{pmatrix} x^3+x^2+x \\ x^3+x^2+x \end{pmatrix}$$

$$= \begin{pmatrix} x^2+x+1 \\ x^4+x^2+x+1 \end{pmatrix} = \begin{pmatrix} G \\ T \end{pmatrix}$$

And

$$(f_5(x))(x^4+1) = (x^4+x^2+1)(x^4+1) = x = C.$$

It results HELLO→OBGTC.

Step 3. Turn into blocks of 3s and multiply with the key matrix,

$$\begin{pmatrix} B & B & C \\ Ç & E & Ğ \\ K & E & Y \end{pmatrix}\begin{pmatrix} O \\ B \\ G \end{pmatrix} = \begin{pmatrix} 1 & 1 & x \\ x+1 & x^2+1 & x^3 \\ x^3+x^2+1 & x^2+1 & x^4+x^3+x^2+1 \end{pmatrix}\begin{pmatrix} x^4+1 \\ 1 \\ x^2+x+1 \end{pmatrix}$$

$$= \begin{pmatrix} x^4+x^3+x^2+x \\ x^3+x^2+x \\ x^4+x^3+x^2+x+1 \end{pmatrix} = \begin{pmatrix} Z \\ L \\ Q \end{pmatrix}$$

If there is an ascending 2 letter in the text that is converted into 3s block, it letters is multiplied by 2.key matrix in 2×2 .

$$\begin{pmatrix} E & A \\ O & D \end{pmatrix}\begin{pmatrix} T \\ C \end{pmatrix} = \begin{pmatrix} x^2+1 & 0 \\ x^4+1 & x^2 \end{pmatrix}\begin{pmatrix} x^4+x^3+x^2+x+1 \\ x \end{pmatrix}$$

$$= \begin{pmatrix} 1 \\ x^3+x^2+1 \end{pmatrix} = \begin{pmatrix} B \\ K \end{pmatrix}.$$

It results OBGTC→ZLQBK

Step 4.
$Z + f_1(x) = x^4 + x^3 + x^2 + x + 1 = Q$
$L + f_2(x) = x^3 + x^2 + x + x = x^3 + x^2 = J$
$Q + f_3(x) = x^4 + x^3 + x^2 + x + 1 + x^2 + 1$
$= x^4 + x^3 + x = V$
$Z + f_4(x) = 1 + x^3 = x^3 + 1 = H$
$K + f_5(x) = x^3 + x^2 + x + 1 + x^4 + x^2 + 1$
$= x^4 + x^3 = U$
It results ZLQBK → QJVHU.

The Application of The Decoding Algorithm:

Step 1.
$Q + f_1(x) = x^4 + x^3 + x^2 + x + 1 + 1$
$= x^4 + x^3 + x^2 + x = Z$
$J + f_2(x) = x^3 + x^2 + x = L$
$V + f_3(x) = x^4 + x^3 + x + x^2 + 1$
$= x^4 + x^3 + x^2 + x + 1 = Q$
$H + f_4(x) = x^3 + 1 + x^3 = 1 = B$
$U + f_5(x) = x^4 + x^3 + x^4 + x^2 + 1 = x^3 + x^2 + 1 = K$
It results QJVHU → ZLQBK .

Step 2. Divide encrypted text into 3s blocks and transform it into 3×1 matrices. 3×1 matrices are multiplied by inverse of the key matrix in 3×3 :

$$\begin{pmatrix} F & Ç & Z \\ S & Ğ & N \\ V & T & G \end{pmatrix}\begin{pmatrix} Z \\ L \\ Q \end{pmatrix} = \begin{pmatrix} O \\ B \\ G \end{pmatrix}$$

If there is an ascending 2 letter in the encrypted text that is converted into 3s block, its letters are multiplied by the inverse of the 2.key matrix:

$$\begin{pmatrix} T & A \\ Ğ & H \end{pmatrix}\begin{pmatrix} B \\ K \end{pmatrix} = \begin{pmatrix} T \\ C \end{pmatrix}$$

It results ZLQBK → OBGTC.

Step 3. Divide the encrypted text into 2s blocks and transform it into 2×1 matrices. 2×1 matrices are multiplied by the *n*th inverse of the Fibonacci polynomial matrix in 2 . If there is an ascending letter in the encrypted text that is converted into 2s block, its letters are multiplied the inverse of $f_n(x)$.

$$Q^5(x)^{-1} = \begin{pmatrix} x^3 & x^4+x^2+1 \\ x^4+x^2+1 & x^2+x+1 \end{pmatrix}$$

and

$$\begin{pmatrix} x^4+1 \\ 1 \end{pmatrix} = \begin{pmatrix} O \\ B \end{pmatrix}, \quad \begin{pmatrix} x^2+x+1 \\ x^4+x^2+x+1 \end{pmatrix} = \begin{pmatrix} G \\ T \end{pmatrix}$$

It is know that,

$$\begin{pmatrix} x^3 & x^4+x^2+1 \\ x^4+x^2+1 & x^2+x+1 \end{pmatrix}\begin{pmatrix} x^4+1 \\ 1 \end{pmatrix} = \begin{pmatrix} x^3+1 \\ x^2+1 \end{pmatrix} = \begin{pmatrix} H \\ E \end{pmatrix},$$

$$\begin{pmatrix} x^3 & x^4+x^2+1 \\ x^4+x^2+1 & x^2+x+1 \end{pmatrix}\begin{pmatrix} x^2+x+1 \\ x^4+x^2+x+1 \end{pmatrix} = \begin{pmatrix} x^3+x^2+x \\ x^3+x^2+x \end{pmatrix} = \begin{pmatrix} L \\ L \end{pmatrix}$$

and let's $f^{-1}(x) = x^4 + x^3 + x$.
So, It is
$f^{-1}(x).C = (x^4 + x^3 + x)(x) = x^4 + 1 = O.$
It results OBGTC→HELLO.

3. CONCLUSION

Rijndael found the AES (Advanced Encryption Standard) with the help of polynomials in Galois fields. We too created a new encryption algorithm with the help of Fibonacci polynomials and polynomials in Galois _elds and this algorithm is called Classical AES-like Cryptology via Fibonacci Polynomial Matrix. First, we present the mathematical basis necessary for understanding the specifications followed by the design rationale and the description itself. Subsequently, the implementation aspects of the cipher and its inverse are treated.

ACKNOWLEDGEMENTS

This work was presented at the Second *Cilicia International Symposium on Engineering and Technology (CISET 2019).*

REFERENCES

Uçar, S , Taş, N., and Özgür, N. (2019). "A New Application to Coding Theory via Fibonacci and Lucas Numbers". *MSAEN 7: 62-70.*

Paar, C., and Pelzl, J. (2009). "Understanding cryptography: a textbook for students and practitioners." *Springer Science, Business Media*.

Koshy, T. (2018). "Fibonacci and Lucas Numbers with Applications." Volume 1, *John Wiley & Sons, New Jersey.*

Koshy, T. (2019). "Fibonacci and Lucas Numbers with Applications." Volume 2, *John Wiley & Sons, New Jersey.*

Stewart, I. (1990). "Galois theory." *Chapman and Hall/CRC.*

Klima, R. E., and Sigmon, N. P. (2012). "Cryptology: classical and modern with maplets." *Chapman and Hall/CRC.*

Daemen,, J., and Rijmen, V. (2003). "AES Proposal: Rijndael". *National Institute of Standards and Technology. p. 1. Archived from the original on 5 March 2013*. Retrieved 21 February 2013.

Avaroğlu, E., Koyuncu, I., Özer, A. B., and Türk, M. (2015). "Hybrid pseudo-random number generator for cryptographic systems." *Nonlinear Dynamics, 82*(1-2), 239-248.