Received 13 June 2023, accepted 8 July 2023, date of publication 17 July 2023, date of current version 26 July 2023.
Digital Object Identifier 10.1109/ACCESS.2023.3295909

RESEARCH ARTICLE

Periodicity Detection of the Substitution Box in the CBC Mode of Operation: Experiment and Study

ZHANNA ALIMZHANOVA[1], MARIA SKUBLEWSKA-PASZKOWSKA[2], (Member, IEEE), AND DAUREN NAZARBAYEV[1]
[1]Department of Information Systems, Faculty of Information Technology, Al-Farabi Kazakh National University, 050040 Almaty, Kazakhstan
[2]Department of Computer Science, Faculty of Electrical Engineering and Computer Science, Lublin University of Technology, 20-618 Lublin, Poland
Corresponding author: Dauren Nazarbayev (d.a.nazarbayev@gmail.com)

ABSTRACT This paper presents a technique for investigating the cyclic properties of substitution boxes (S-boxes) in the Cipher Block Chaining (CBC) mode of operation. S-boxes provide nonlinear transformations in encryption algorithms to create confusion and enhance cryptographic strength. The CBC mode design is used in block ciphers to hide periodic patterns and create a diffusion effect. The main objective of this study was to detect the periodicity of the bijective S-boxes in CBC mode to evaluate their cryptographic strength. The study of S-boxes using the presented technique allows us to examine them in a different manner and study their diffusion levels, the metrics of which are the periodicities of the S-box element sequences. To apply the diffusion effect of the CBC mode to the S-boxes, the encryption function used in the cryptographic ciphers was changed to a substitution function for the S-boxes used as an inner nonlinear component of the encryption function. The S-box used in the Advanced Encryption Standard (AES) was selected for experiment and study. In this study, the cyclic properties of the S-box were considered from two different aspects: periodicity detection of the S-box with respect to iterations and blocks. According to our study, the maximal periods of the AES S-box and various other S-boxes were found to be very large, indicating that the influence of the CBC mode spread over many iterations and blocks, thus confirming the high level of cryptographic strength of the S-boxes.

INDEX TERMS AES, block cipher, CBC mode of operation, cyclic properties, periodicity, S-box, cryptographic strength.

I. INTRODUCTION

Cryptography, which has its roots in ancient times, is in an essential position to perform in the field of information security. Currently, cryptography has changed. It differs significantly from cryptography, which existed until the twentieth century and is divided into classic and modern cryptography [1], [2], [3]. Modern cryptography tasks, which can be observed in applications such as electronic digital signatures, information authentication, information integrity control, electronic money, and secure network communications, have been extended. Therefore, security measures are being considered at the level of progress with the development of information technology and computing power. Modern cryptography is one of the most relevant sciences, in which advanced knowledge of mathematics and computer science is required. Current cryptography uses two approaches, symmetric and asymmetric [4], [5], [6]. Symmetric cryptography is divided into block and stream ciphers [7].

Block ciphers accept messages and produce fixed-length results called blocks under the action of a secret key. Currently, a block length of 128 bits is considered optimal for balancing the security and computational speed of encryption [8]. Not all data can be encrypted in a single block, because there are very large datasets. In such cases, various techniques, called modes of operation, are used to enhance the effects of encryption algorithms. The operating mode is a symmetric encryption scheme designed to encrypt an

The associate editor coordinating the review of this manuscript and approving it for publication was Ladislau Matekovits.

arbitrary length [9]. In many applications, block ciphers operate in one mode or the other. Various operating modes have been developed for this purpose [10], [11], [12]. However, some of these modes have advantages and disadvantages in their use. For example, in the Electronic Codebook (ECB), blocks perform independently of each other; they are repeated in both plaintext and ciphertext. The advantage is that the blocks are independent, which makes it possible to perform encryption operations in parallel. The disadvantage is that they are repeatable with respect to each identical block, which is a vulnerability to cryptographic attacks. To eliminate repetition, other modes have been developed including Cipher Block Chaining (CBC), Output Feedback (OFB), Cipher Feedback (CFB), and Counter Mode (CTR).

One of the main ways to provide nonlinear transformations in cryptographic ciphers is to use substitution boxes (S-boxes), which are Boolean vector functions with certain cryptographic and cyclic properties on which the cryptographic strength of the entire cipher depends [13], [14]. In most cases, they are represented in substitution tables formulated using various mathematical transformations.

This study investigated the bijective S-box used in the Rijndael encryption algorithm or the Advanced Encryption Standard (AES) [15], [16]. The purpose of our study was to detect the periodicity of the S-box with respect to iterations and blocks in the CBC mode. This provides an indication of the level of diffusion formation, by which we can investigate the cryptographic strength of the S-box as an additional criterion.

The remainder of this paper is organized as follows. Section II presents the related work. Section III describes the experiments and results, and Section IV concludes the study. In Section III, experiments and results are presented using two approaches. The first is the periodicity detection of the S-box in the CBC mode with respect to the iterations and the second is with respect to the blocks.

II. RELATED WORK

The foundation of modern cryptography was laid by the American scientist Shannon [1], [17], who formulated two important conditions for the strength of cryptographic ciphers: confusion and diffusion. The entire point of confusion is to make it difficult to find statistical and analytical connections between the bits of the secret key and the ciphertext. Diffusion refers to the spread of the influence of one bit of plaintext over several bits of ciphertext. S-boxes used in cryptographic ciphers are required to create confusion. For S-boxes to affect the bit confusion, they must satisfy cryptographic criteria or properties. There are different cryptographic criteria, such as balancedness, algebraic degree, nonlinearity, correlation immunity, algebraic immunity, avalanche criteria, and complexity parameters [18], [19], [20], to evaluate the resistance of encryption algorithms to various cryptographic attacks [21], [22], [23].

It is well known that S-boxes do not provide high results for all the above criteria. Therefore, there is great interest in finding optimal S-boxes in combination with the limit values of the criteria. Finding the optimal S-boxes is an actual problem in cryptography. Currently, there is considerable interest in designing new S-boxes. For example, in [24], the authors proposed a method to improve cryptographic properties, including the distance to the strict avalanche criterion (DSAC) of an existing AES S-box by modifying and adding affine transformations. DSAC is 372. For more details on DSAC, see [25]. In the study [25] a function for F_{2^8}, which is a new S-box for AES, was proposed. The function is defined for byte x as:

$$S(x) = \begin{cases} \dfrac{Ax+\alpha}{Ax+\beta}, & \text{if } x \neq A^{-1}\beta \\ 01 & \text{if } x = A^{-1}\beta, \end{cases}$$

where A is an 8×8 invertible matrix of bits and α, β are two different bytes. The proposed S-box exhibits improved cryptographic properties. For example, DSAC is 328, which is better than that of AES S-box, which is 432.

To evaluate cryptographic strength against existing cryptographic attacks, it is also important to investigate the cyclic properties of the cipher's internal components, including the S-box. The weaknesses of the cryptographic cipher are the short periods and presence of fixed and opposite fixed points. In [26], using certain input data, the authors studied the output data of the AES in the ECB, CBC, OFB, and CFB modes and detected characteristic periodic patterns in the output data of the four modes. The authors of [27] investigated the cyclic properties of the internal components of AES. They stated that the periods of the linear and non-linear functions of the AES were short; however, when these functions were combined, the period increased dramatically to approximately 2^{110}. In another study [28], new period results were obtained using a combination of four internal functions of the AES, with a very large period (greater than 10^{205}).

III. EXPERIMENTS AND RESULTS

Ehrsam et al. created a CBC operation mode in 1976 [29]. In CBC mode, each plaintext block is operated using a Boolean logical XOR operation with a previous ciphertext block.

The general calculation formulas for encryption are derived using the following formulas for ECB:

$$C_i = E_k(P_i), \quad i = \overline{1,n} \tag{1}$$

and for CBC:

$$C_1 = E_k(P_1 \oplus IV), \quad C_i = E_k(P_i \oplus C_{i-1}), \ i = \overline{2,n} \tag{2}$$

where i is the block number, P_i is the plaintext of the i-th block, C_i is the ciphertext of the i-th block, k is the encryption key, E_k is the encryption function, IV is the initialization vector, and n is the total number of blocks.

TABLE 1. **Cycle structure of the AES S-box.**

	Disjoint cycles in the AES S-box	Cycle length
1	(00, 63, FB, 0F, 76, 38, 07, C5, A6, 24, 36, 05, 6B, 7F, D2, B5, D5, 03, 7B, 21, FD, 54, 20, B7, A9, D3, 66, 33, C3, 2E, 31, C7, C6, B4, 8D, 5D, 4C, 29, A5, 06, 6F, A8, C2, 25, 3F, 75, 9D, 5E, 58, 6A, 02, 77, F5, E6, 8E, 19, D4, 48, 52)	59
2	(01, 7C, 10, CA, 74, 92, 4F, 84, 5F, CF, 8A, 7E, F3, 0D, D7, 0E, AB, 62, AA, AC, 91, 81, 0C, FE, BB, EA, 87, 17, F0, 8C, 64, 43, 1A, A2, 3A, 80, CD, BD, 7A, DA, 57, 5B, 39, 12, C9, DD, C1, 78, BC, 65, 4D, E3, 11, 82, 13, 7D, FF, 16, 47, A0, E0, E1, F8, 41, 83, EC, CE, 8B, 3D, 27, CC, 4B, B3, 6D, 3C, EB, E9, 1E, 72, 40, 09)	81
3	(04, F2, 89, A7, 5C, 4A, D6, F6, 42, 2C, 71, A3, 0A, 67, 85, 97, 88, C4, 1C, 9C, DE, 1D, A4, 49, 3B, E2, 98, 46, 5A, BE, AE, E4, 69, F9, 99, EE, 28, 34, 18, AD, 95, 2A, E5, D9, 35, 96, 90, 60, D0, 70, 51, D1, 3E, B2, 37, 9A, B8, 6C, 50, 53, ED, 55, FC, B0, E7, 94, 22, 93, DC, 86, 44, 1B, AF, 79, B6, 4E, 2F, 15, 59, CB, 1F, C0, BA, F4, BF, 08, 30)	87
4	(0B, 2B, F1, A1, 32, 23, 26, F7, 68, 45, 6E, 9F, DB, B9, 56, B1, C8, E8, 9B, 14, FA, 2D, D8, 61, EF, DF, 9E)	27
5	(73, 8F)	2

TABLE 2. **Input data for the calculation of the maximal period of the S-box with respect to the iterations.**

Plaintext	Initialization vector	Length of block	Number of blocks
$P = [i]$, $i = \overline{00, FF}$	$IV = [k]$, $k = \overline{00, FF}$	$l = 1$	$n = 1$

In the proposed technique for investigating the nonlinear layer of S-boxes, we replaced the encryption function E_k used in block ciphers with a substitution function for the S-boxes used as an inner nonlinear component of the encryption function E_k, denoted by S to study the effect of diffusion in the CBC mode on S-boxes. By changing the encryption function to a substitution function, we can write (1) and (2) for ECB as follows:

$$C_i = S(P_i), \quad i = \overline{1, n} \tag{3}$$

and for CBC:

$$C_1 = S(P_1 \oplus IV), \quad C_i = S(P_i \oplus C_{i-1}), \; i = \overline{2, n} \tag{4}$$

Algorithm 1, in which formulas (3) and (4) are applied, is as follows:

Algorithm 1 Algorithm for the Substitution Function in the ECB and CBC Modes of Operation

Input: P – plaintext, IV – initialization vector, l – length of block, n – number of blocks, mode - option of one of the two modes: "ECB" or "CBC", sbox – the option of a specific S-box, for example, an AES S-box).
Output: C – ciphertext, presented as matrix $(n \times l)$

```
Function Substitution (P, IV, l, n, mode, sbox)
if (mode = "ECB") then
    for i ← 1 to n
        for j ← 1 to l
            C[i, j] ← sbox[P[i, j]]
        end for
    end for
else if (mode = "CBC") then
    for i ← 1 to n
        for j ← 1 to l
            if (i = 1) then
                C[i, j] ← sbox [P[i, j] ⊕ IV[j]]
            else
                C[i, j] ← sbox [P[i, j] ⊕ C[i − 1, j]]
            end if
        end for
    end for
end if
return C
```

A. PERIODICITY DETECTION OF THE S-BOX IN CBC MODE WITH RESPECT TO THE ITERATIONS

To demonstrate the proposed technique, we selected the bijective S-box consisting of 256 elements (bytes) used in AES as an example.

Definition 1: The process of repeatedly applying the same function is called iteration.

Definition 2: A cyclic or iterated function is the identity function when iterated a finite number of times:

$$f^n(x) = f(\ldots(f(f(x)))\ldots) = x$$

where f^n is the n-th iterate of function f. For example, every permutation of a finite set is a cyclic function, according to this definition.

Definition 3: Let $S\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a function that defines an S-box. For $x \in \mathbb{F}_{2^n}$, the period of x under S is the smallest positive integer n such that $S^n(x) = x$.

Definition 4: The order of an arbitrary element of permutation of a finite set is equal to the least common multiple (LCM) of the cycle lengths in its cyclic decomposition.

Permutations of a finite set should be considered when investigating the cyclic properties of the bijective S-boxes [30]. For more details on LCM, see [31].

TABLE 3. The periods of each element of the AES S-box in the ECB and CBC modes for input data of (5).

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	59	81	59	59	87	59	59	59	87	81	87	27	81	81	81	59
1	81	81	81	81	27	87	81	81	87	59	81	87	87	87	81	87
2	59	59	87	27	59	59	27	81	87	59	87	27	87	27	59	87
3	87	59	27	59	87	87	59	87	59	81	81	87	81	81	87	59
4	81	81	87	81	87	27	87	81	59	87	87	81	59	81	87	81
5	87	87	59	87	59	87	27	81	59	87	87	81	87	59	59	81
6	87	27	81	59	81	81	59	87	27	87	59	59	87	81	27	59
7	87	87	81	2	81	59	59	59	81	87	81	59	81	81	81	59
8	81	81	81	81	81	87	87	81	87	87	81	81	81	59	59	2
9	87	81	81	87	87	87	87	87	87	87	87	27	87	59	27	27
A	81	27	81	87	87	59	59	87	59	59	81	81	81	87	87	87
B	87	27	87	81	59	59	87	59	87	27	87	81	81	81	87	87
C	87	81	59	59	87	59	59	59	27	81	81	87	81	81	81	81
D	87	87	59	59	59	59	87	81	27	87	81	27	87	81	87	27
E	81	81	87	81	87	87	59	87	27	81	81	81	81	87	87	27
F	81	27	87	81	87	59	87	27	81	87	27	59	87	59	81	81

Algorithm 2 Algorithm for Periodicity Detection in the S-Box With Respect to the Iterations

Input: P - plaintext, IV – initialization vector, l –length of block, n –number of blocks, mode - option of one of the two modes: "ECB" or "CBC", sbox – the option of a specific S-box, for example, an AES S-box).
Output: T – the period
Function Period (P, IV, l, n, mode, sbox)
$C \leftarrow$ substitution(P, IV, l, n, mode, sbox)
  { C - ciphertext}
T$\leftarrow$ 1
if (int (P) $\neq$ int (C)) **then**
  {P and C for equality comparison}
  while (int (P) $\neq$ int (C))
    $C \leftarrow$ Substitution(C, IV, l, n, mode, sbox)
    $T \leftarrow T + 1$
  end while
end if
return T

Theorem 1 (Order of Permutations): The order of permutation of a finite set written in the disjoint cycle form is the LCM of the cycle lengths.

Theorem 2 (Products of Disjoint Cycles): Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.

The proofs of Theorems 1 and 2 are provided in [32].

In our study, terms such as order, cycle length, and period are interchangeable.

Let us review the cyclic properties of the AES S-box, its cycle structure includes five disjoint cycles with lengths of 59, 81, 87, 27, and 2 (see Table 1). For the disjoint cycles of the AES S-box and the length of each cycle, refer to [27]. The AES S-box period can be found in [25] and [28]. By calculating the LCM of the cycle lengths of the disjoint cycles, we obtained the order of an arbitrary element of

Algorithm 3 Algorithm to Calculate the Maximal Period of the S-Box With Respect to the Iterations

Input: l –length of the block, n –number of blocks, mode - option of one of the two modes: "ECB" or "CBC", sbox – the option of a specific S-box, for example, an AES S-box).
Output: G – the maximal period of the S-box
$L \leftarrow \underbrace{[0, 0, \ldots, 0]}_{256 \text{ elements}}$
for $k \leftarrow 0$ **to** 255
  $A \leftarrow \underbrace{[0, 0, \ldots, 0]}_{256 \text{ elements}}$
  for $i \leftarrow 0$ **to** 255
    $P \leftarrow \underbrace{[\underbrace{[i, i, \ldots, i]}_{l}, \underbrace{[i, i, \ldots, i]}_{l}, \ldots, \underbrace{[i, i, \ldots, i]}_{l}]}_{n \text{ blocks}}$
    $IV \leftarrow \underbrace{[k, k, \ldots, k]}_{256 \text{ elements}}$
      {IV– the initialization vector}
    $T \leftarrow$ Period (P, IV, l, n, mode, sbox)
      {T- the period}
    $A\,[i] \leftarrow T$ {A - array of the T variable}
  end for
  $L[k] \leftarrow LCM(A)$
    {L - array of LCM of the A variable}
end for
$G \leftarrow$ LCM(L)
return G

the AES S-box as 277182, which was the maximal period. Thus, we can state that the order of an arbitrary S-box element is:

$$S^{277182}(x) = x$$

here, $x = \overline{00, FF}$.

Algorithm 4 Algorithm to Calculate the Maximal Period of the S-Box With Respect to the Blocks

Input: l–length of the block, n–number of blocks, mode - option of one of the two modes: "ECB" or "CBC", sbox – the option of a specific S-box, for example, an AES S-box).
Output: G maximal period of the S-box

$L \leftarrow \underbrace{[0, 0, \ldots, 0]}_{256 \text{ elements}}$
for $i \leftarrow 0$ **to** 255
  $A \leftarrow \underbrace{[0, 0, \ldots, 0]}_{256 \text{ elements}}$
  for $k \leftarrow 0$ **to** 255
    $P \leftarrow \underbrace{[\underbrace{[i, i, \ldots, i]}_{l}, \underbrace{[i, i, \ldots, i]}_{l}, \ldots, \underbrace{[i, i, \ldots, i]}_{l}]}_{n \text{ blocks}}$
    $IV \leftarrow \underbrace{[k, k, \ldots, k]}_{256 \text{ elements}}$
    {IV – the initialization vector}
    $C \leftarrow$ substitution (P, IV, l, n, mode, sbox) {C – the ciphertext}
    for $T \leftarrow 1$ **to** n {T – the period}
      if ($C[0] = C[T]$) **then**
        $A[k] \leftarrow T$ {A - array of the T variable}
        break
      end if
    end for
  end for
  $L[i] \leftarrow$ LCM(A)
end for {L - maximal periods for each element of the S-box }
$G \leftarrow$ LCM(L)
return G

From this, we can conclude that any plaintext within one block transformed through the AES S-box after 277182 iterations returns to the plaintext again:

$$P \rightarrow S(P) \rightarrow C_1 \rightarrow S(C_1) \rightarrow \ldots C_i \rightarrow \ldots C_{277182} = P$$

where P is the plaintext, S is the substitution function, C_i is the ciphertext at the i-th iteration.

To detect periodicity and calculate the order of an arbitrary element of the S-box, that is, the maximal period of the S-box with respect to iterations, we present Algorithms 2 and 3, respectively.

To determine the periodicity of the S-box with respect to the iterations, we set some input data: all plaintexts and initialization vectors consist of only one block each, all blocks contain only one element each in hexadecimal notation, and the range of change of elements is from 0 to 255 (see Table 2).

By implementing Algorithms 2 and 3, we obtained the maximal periods for each element of the AES S-box in ECB mode with respect to the iterations (see Table 3).

In case of ECB mode, by calculating the LCM of the periods in Table 3, in Algorithm 3 denoted by the variable L, we found that the maximal period with respect to the iterations, the denoted by variable G, was 277182 iterations.

The next part of the study examined the AES S-box in the CBC mode. By implementing Algorithms 2 and 3 for the input data (5), the periods for each element in CBC mode were equal to the maximal periods for each element in ECB mode (see Table 3).

$$P = [i], \quad i = \overline{00, FF}, IV = [00] \tag{5}$$

In the case of input data (6), we already obtained other periods (see Table 4).

$$P = [i], \quad i = \overline{00, FF}, IV = [01] \tag{6}$$

The period values in Table 4 are already different because all the elements operate using a Boolean logical XOR operation with initialization vector $IV = [01]$.

Therefore, by changing the initialization vector $IV = [k]$, $k = \overline{00, FF}$, we obtained the maximal periods for each element in the CBC mode (see Table 5). In Algorithm 3, we denoted by variable L. By calculating the LCM of the values for each element, we obtained the maximal period of the AES S-Box in CBC mode with respect to the iterations (see Table 6), denoted by variable G. The maximal period was approximately 9.68×10^{89} iterations.

B. PERIODICITY DETECTION OF THE S-BOX IN CBC MODE WITH RESPECT TO THE BLOCKS

Our study shows that by applying the substitution function, we can determine the periods in CBC mode with respect to the blocks. We applied the CBC mode construction used in block ciphers to investigate the cyclic properties of AES S-box.

Consider the example of finding the maximal period of the AES S-box in CBC mode with respect to the blocks for the input data presented in Table 7.

In the input data, all plaintexts consist of 257 blocks each, initialization vectors consist of only one block each, all blocks contain a single element in hexadecimal notation, and the range of elements changes from 0 to 255. The selection of 257 blocks was sufficient because the periods for each S-box element individually in CBC mode ranged from 1 to 256 with respect to the blocks.

Algorithm 4 presents an algorithm to calculate the maximal period of the S-box with respect to the blocks. By implementing Algorithm 4 on the input data of (7), we obtained the results for the AES S-box.

$$P = \underbrace{[00], \ldots, [00]}_{257 \text{ blocks}}, \quad IV = [00] \tag{7}$$

These results are the values of the ciphertexts in the ECB and CBC modes, showing periodicity with respect to the blocks

TABLE 4. The periods of each element of the AES S-box in the CBC mode for input data of (6).

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	166	166	166	166	166	166	4	166	166	14	7	166	14	166	18	166
1	166	43	166	166	166	166	166	166	166	43	166	7	4	166	166	43
2	166	18	166	166	43	166	166	166	43	43	166	7	166	166	166	166
3	14	166	166	166	43	166	166	166	166	166	43	14	166	43	166	43
4	166	14	166	166	43	7	166	166	14	43	166	18	166	43	18	166
5	43	166	43	166	2	166	166	166	166	166	166	166	166	166	166	166
6	43	166	166	166	43	166	166	166	14	7	166	166	166	43	43	166
7	43	166	43	166	166	166	18	166	166	18	18	166	166	166	166	166
8	14	18	166	166	18	166	166	43	43	166	43	166	166	43	166	43
9	18	43	166	166	166	166	43	18	166	166	166	166	166	166	166	166
A	166	166	7	43	4	43	166	43	43	166	166	166	166	43	18	166
B	166	166	43	166	14	43	166	18	166	166	166	166	18	166	166	18
C	166	166	166	166	166	4	1	14	166	166	43	166	166	18	43	166
D	166	43	166	43	166	14	18	14	166	166	166	166	166	166	166	166
E	166	1	43	166	166	7	166	166	166	166	166	43	166	43	166	43
F	166	166	166	166	166	18	14	166	166	14	166	166	2	166	166	166

TABLE 5. The approximate values of the maximal periods for each element of the AES S-box in the CBC mode for the input data of Table 2.

	0	1	2	3	4	5	6	7
0	3.36×10^{79}	6.06×10^{72}	3.45×10^{74}	7.13×10^{85}	3.56×10^{80}	5.29×10^{83}	7.07×10^{87}	2.87×10^{83}
1	3.01×10^{80}	2.42×10^{81}	2.1×10^{81}	2.63×10^{81}	9.05×10^{87}	4.87×10^{87}	3.5×10^{81}	7.63×10^{87}
2	5.69×10^{80}	1.36×10^{81}	3.84×10^{79}	3.77×10^{81}	7.13×10^{81}	3.77×10^{79}	4.43×10^{83}	2.27×10^{81}
3	4.44×10^{85}	5.49×10^{85}	8.36×10^{76}	6.38×10^{84}	2.22×10^{83}	4.74×10^{85}	3.69×10^{78}	1.23×10^{77}
4	5.35×10^{79}	2.54×10^{83}	5.27×10^{81}	9.68×10^{89}	3.99×10^{85}	2.87×10^{83}	1.03×10^{83}	1.94×10^{89}
5	9.68×10^{89}	5.07×10^{87}	5.06×10^{85}	1.81×10^{79}	2.31×10^{83}	6.5×10^{79}	1.21×10^{79}	4.86×10^{85}
6	8.12×10^{85}	1.76×10^{81}	6.9×10^{85}	2.64×10^{83}	8.48×10^{78}	4.43×10^{82}	3.41×10^{83}	7.63×10^{87}
7	6.14×10^{84}	8.45×10^{85}	8.36×10^{76}	4.16×10^{87}	1.71×10^{81}	1.51×10^{85}	1.44×10^{80}	2.16×10^{81}
8	1.79×10^{73}	9.49×10^{80}	1.39×10^{87}	1.13×10^{81}	2.18×10^{83}	4.61×10^{84}	1.11×10^{81}	3.61×10^{85}
9	9.64×10^{84}	8.05×10^{84}	1.33×10^{81}	3.73×10^{74}	2.6×10^{83}	1.5×10^{83}	1.67×10^{78}	7×10^{85}
A	4.71×10^{82}	1.13×10^{77}	1.36×10^{81}	7.18×10^{78}	2.58×10^{82}	3.9×10^{79}	9.83×10^{80}	1.08×10^{87}
B	5.86×10^{78}	1.53×10^{87}	4.79×10^{82}	8.47×10^{73}	5.91×10^{74}	1.13×10^{84}	9.68×10^{89}	5.74×10^{82}
C	4.98×10^{83}	6.35×10^{83}	3.39×10^{80}	8.53×10^{86}	1.13×10^{79}	6.66×10^{82}	1.25×10^{86}	5.6×10^{87}
D	1.14×10^{81}	1.5×10^{79}	6.44×10^{80}	3.65×10^{85}	7.63×10^{87}	8.22×10^{80}	6.54×10^{83}	3.94×10^{83}
E	4.62×10^{83}	6.76×10^{85}	3.8×10^{81}	2.57×10^{81}	1.01×10^{86}	4.57×10^{83}	1.44×10^{86}	2.89×10^{83}
F	6.21×10^{80}	4.59×10^{87}	1.76×10^{83}	2.26×10^{83}	1.59×10^{88}	2.37×10^{79}	2.09×10^{85}	2.32×10^{85}

	8	9	A	B	C	D	E	F
0	2.22×10^{83}	8.82×10^{84}	3.47×10^{76}	2.04×10^{78}	3×10^{79}	9.68×10^{89}	1.49×10^{75}	9.73×10^{86}
1	1.87×10^{81}	1.19×10^{78}	2.35×10^{81}	6.1×10^{76}	2.02×10^{81}	8.88×10^{84}	7.92×10^{80}	2.61×10^{78}
2	1.52×10^{79}	4.08×10^{83}	6.29×10^{85}	1.11×10^{85}	1.58×10^{81}	3×10^{75}	4×10^{83}	1.59×10^{81}
3	2.11×10^{83}	8.24×10^{82}	3.87×10^{79}	7.92×10^{73}	7.63×10^{87}	1.09×10^{77}	1.13×10^{83}	6.39×10^{80}
4	1.27×10^{83}	3.52×10^{82}	1.43×10^{79}	9.18×10^{85}	2.9×10^{81}	1.53×10^{83}	2.65×10^{85}	7.19×10^{79}
5	5.67×10^{84}	8.32×10^{80}	7.63×10^{87}	6.46×10^{76}	4.62×10^{83}	9.02×10^{83}	2.58×10^{79}	6.97×10^{87}
6	1.07×10^{84}	6.17×10^{87}	1.66×10^{81}	2.56×10^{80}	4.95×10^{80}	9.27×10^{81}	5.65×10^{78}	9.69×10^{85}
7	1.44×10^{81}	3.49×10^{83}	4.86×10^{85}	5.81×10^{85}	9.68×10^{89}	7.09×10^{85}	7.4×10^{84}	8.82×10^{85}
8	5.53×10^{80}	2.02×10^{85}	2.35×10^{78}	7.63×10^{87}	2.81×10^{79}	4.81×10^{84}	5.31×10^{78}	2.18×10^{83}
9	4.01×10^{78}	2.42×10^{83}	7.98×10^{84}	8.82×10^{84}	9.68×10^{89}	1.01×10^{81}	3.6×10^{81}	6.41×10^{87}
A	3.65×10^{85}	5.04×10^{83}	4.03×10^{85}	6.58×10^{80}	3.53×10^{83}	4.43×10^{82}	4.18×10^{83}	3×10^{83}
B	8.53×10^{86}	2.68×10^{81}	6.97×10^{87}	2.62×10^{81}	1.41×10^{76}	3.49×10^{83}	2.54×10^{83}	7.05×10^{83}
C	4.42×10^{81}	6.97×10^{87}	9.68×10^{89}	1.91×10^{83}	4.61×10^{84}	3×10^{80}	6.34×10^{82}	2.65×10^{81}
D	2.64×10^{79}	2.5×10^{85}	9.68×10^{89}	3.63×10^{83}	2.54×10^{83}	9.68×10^{89}	1.56×10^{83}	1.56×10^{81}
E	1.53×10^{87}	1.18×10^{78}	7.63×10^{87}	4.78×10^{83}	4.9×10^{81}	3.25×10^{79}	7.96×10^{83}	1.1×10^{85}
F	2.35×10^{83}	7.3×10^{84}	9.07×10^{78}	3.65×10^{85}	3.17×10^{77}	4.44×10^{85}	1.02×10^{78}	4.16×10^{72}

TABLE 6. The maximal period of the AES S-box in CBC mode for the input data of Table 2.

	The exact value of maximal period
G	968436580918576345099219978398802560813380476522978784146683128513295225386177352832416000

(see Table 8). Fig.1 shows the visualization periodicity of the ciphertexts with respect to the blocks for input data (7) in decimal notation.

TABLE 7. Input data for the calculation of the maximal period of the S-box with respect to the blocks.

Plaintext	Initialization vector	Length of block	Number of blocks
$P = \underbrace{[i], \ldots, [i]}_{n\ blocks},$ $i = \overline{00, FF}$	$IV = [k]$ $k = \overline{00, FF}$	$l = 1$	$n = 257$

Table 9 presents the periods with input data for the case in which

$$P = \underbrace{[i], [i], \ldots, [i], \ldots, [i]}_{257\ \text{blocks}}, \quad IV = [00], \quad i = \overline{00, F\,F} \tag{8}$$

TABLE 8. Values of ciphertexts in the ECB and CBC modes for input data are shown in (7).

		Data values (hexadecimal notation)	Period
Data block sequence	Plaintext	$\underbrace{[00], [00], \ldots [00] \ldots, [00]}_{257\ blocks}$	1
	Ciphertext in the ECB mode	$\underbrace{[63], [63], \ldots [63] \ldots, [63]}_{257\ blocks}$	1
	Ciphertext in the CBC mode	[63], [FB], [0F], [76], [38], [07], [C5], [A6], [24], [36], [05], [6B], [7F], [D2], [B5], [D5], [03], [7B], [21], [FD], [54], [20], [B7], [A9], [D3], [66], [33], [C3], [2E], [31], [C7], [C6], [B4], [8D], [5D], [4C], [29], [A5], [06], [6F], [A8], [C2], [25], [3F], [75], [9D], [5E], [58], [6A], [02], [77], [F5], [E6], [8E], [19], [D4], [48], [52], [00], [63], [FB], [0F], [76], [38], [07], [C5], [A6], [24], [36], [05], [6B], [7F], [D2], [B5], [D5], [03], [7B], [21], [FD], [54], [20], [B7], [A9], [D3], [66], [33], [C3], [2E], [31], [C7], [C6], [B4], [8D], [5D], [4C], [29], [A5], [06], [6F], [A8], [C2], [25], [3F], [75], [9D], [5E], [58], [6A], [02], [77], [F5], [E6], [8E], [19], [D4], [48], [52], [00], [63], [FB], [0F], [76], [38], [07], [C5], [A6], [24], [36], [05], [6B], [7F], [D2], [B5], [D5], [03], [7B], [21], [FD], [54], [20], [B7], [A9], [D3], [66], [33], [C3], [2E], [31], [C7], [C6], [B4], [8D], [5D], [4C], [29], [A5], [06], [6F], [A8], [C2], [25], [3F], [75], [9D], [5E], [58], [6A], [02], [77], [F5], [E6], [8E], [19], [D4], [48], [52], [00], [63], [FB], [0F], [76], [38], [07], [C5], [A6], [24], [36], [05], [6B], [7F], [D2], [B5], [D5], [03], [7B], [21], [FD], [54], [20], [B7], [A9], [D3], [66], [33], [C3], [2E], [31], [C7], [C6], [B4], [8D], [5D], [4C], [29], [A5], [06], [6F], [A8], [C2], [25], [3F], [75], [9D], [5E], [58], [6A], [02], [77], [F5], [E6], [8E], [19], [D4], [48], [52], [00], [63], [FB], [0F], [76], [38], [07], [C5], [A6], [24], [36], [05], [6B], [7F], [D2], [B5], [D5], [03], [7B], [21], [FD], [54]	59

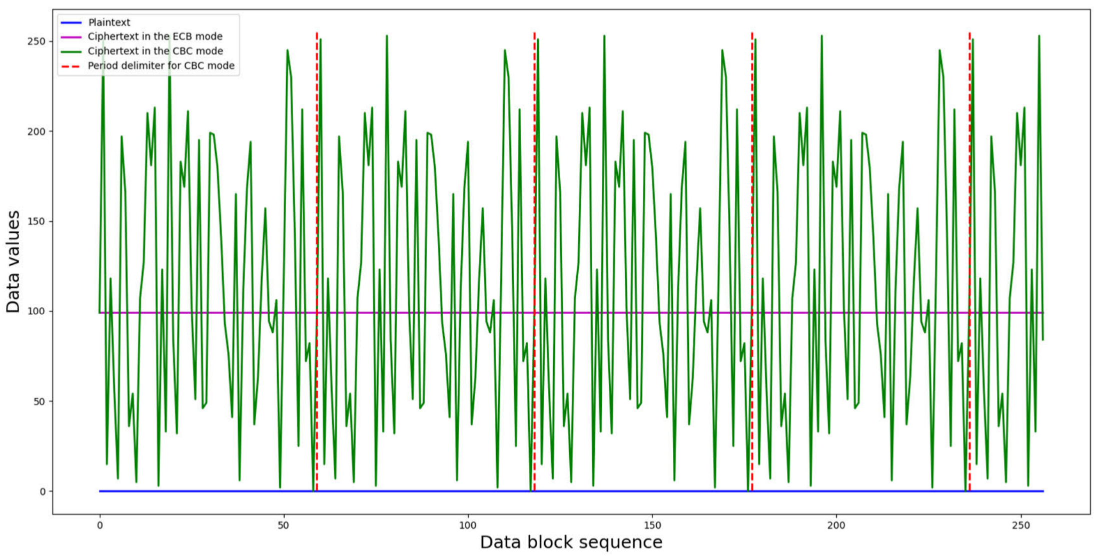

FIGURE 1. Visualization of the periodicity in the ciphertexts in ECB and CBC modes with respect to the blocks.

For example, the period for each element, $T = 256$ appears for $P = \underbrace{[76], [76], \ldots, [76], \ldots, [76]}_{257\text{ blocks}}, IV = [00]$ or $P = \underbrace{[EA], [EA], \ldots, [EA], \ldots, [EA]}_{257\text{ blocks}}, IV = [00]$ and, for $P = \underbrace{[52], [52], \ldots, [52], \ldots, [52]}_{257\text{ blocks}}, IV = [00]$ the period $T = 1$, because for the S-box parameter equal to 52, returns the value 00 (see Table 1). Therefore, with plaintext $P = \underbrace{[52], [52], \ldots, [52], \ldots, [52]}_{257\text{ blocks}}$, the values of the ciphertext $C = \underbrace{[00], [00], \ldots, [00], \ldots, [00]}_{257\text{ blocks}}$ are equal to the value of the initialization vector, as shown in (8).

Based on the input data in Table 7, the maximal periods for each element in the CBC mode are listed in Table 10, denoted by variable L in Algorithm 4. By calculating the LCM for each element in Table 10, we obtained that the maximal period of the AES S-box in the CBC mode with respect to the blocks, indicated by the variable G, was approximately 9.68×10^{89} blocks, which yielded the same result with respect to the iterations. The exact value of the maximal period is shown in Table 6.

TABLE 9. The periods for each element of the AES S-box in the CBC mode for input data of (8).

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	59	166	202	194	43	204	107	227	86	18	182	31	101	172	43	138
1	141	239	148	96	103	229	252	50	225	233	66	98	138	68	72	76
2	90	226	245	228	56	114	18	70	222	186	242	31	201	75	125	212
3	105	215	84	81	118	116	222	34	19	220	136	96	35	184	176	196
4	7	87	249	37	141	157	61	209	135	249	21	135	33	236	74	192
5	63	22	1	166	90	40	198	164	245	196	34	100	99	123	88	146
6	225	89	228	81	106	243	245	226	55	217	23	17	240	232	49	106
7	25	191	236	61	115	196	256	93	104	38	70	180	14	37	57	223
8	103	75	73	218	97	83	40	107	94	211	160	229	6	195	145	56
9	238	166	31	205	45	46	205	52	107	118	243	60	72	179	222	72
A	230	119	235	130	74	12	73	167	246	166	242	118	147	138	171	27
B	47	144	93	93	36	249	141	93	124	51	174	118	228	223	113	88
C	29	62	178	249	103	45	245	230	200	218	142	144	226	36	236	108
D	36	135	242	36	215	238	141	143	175	199	55	230	167	87	4	31
E	5	157	71	182	128	83	90	209	182	16	256	50	122	130	119	198
F	33	69	86	96	113	97	173	46	186	170	168	171	57	144	80	96

TABLE 10. The maximal periods for each element of the AES S-box in the CBC mode for input data of Table 7.

	0	1	2	3	4	5	6	7
0	277182	899388	29896	162378	3823560	3060	129042	17706
1	434280	6692	11100	1958880	142850700	11450	252	197350650
2	73260	8136	980	4788	2168040	51572118	2970	4744110
3	21840	9030	364980	3662820	16166	1298388	2220	12948390
4	1026480	548100	498	2783880	363780	51810	119209860	17556
5	174384	499290	418572	115038	2340	15661800	9702	96432
6	12600	113543352	17556	94122	327540	972	1470	6780
7	276900	35526	1416	26478270	3892980	9996	256	730422
8	856548	28200	6857620	10464	721098	53784	25800	211860
9	3570	14774	460497870	40590	50400	18216	419430	2099500
A	14490	94248	5170	44891730	39738	45540	97528	208416
B	18612	102960	75888	581064	36720	498	25662	174468
C	11600	2637108	44856	498	54384	781560	2940	2070
D	45756	1207440	3146	2082636	234780	4760	2822820	8008
E	340470	314314	15762	9282	551040	2223072	182880	46398
F	2300100	89562	45540612	131040	61924	3168990	4146810	492660

	8	9	A	B	C	D	E	F
0	12402060	17640	850668	338954	284214	82044	976960	22770
1	10350	71764	32882850	91728	53130	6324	106488	30020
2	5550	10602	1452	55057860	14070	23400	27546750	1832740
3	5686320	11220	7460280	7392	45360	13064	388080	97020
4	143640	498	267960	5130	21626220	4956	18337200	9408
5	4410	766360	893520	163800	2189880	854112	596904	116946
6	35232120	37758	71760	784992	240	13224	83790	11212362
7	251160	631408	5810	23940	10744272	597402	19950	191334
8	23632728	278520	31680	9618	621456	16380	803880	13743576
9	1105524	51205392	2430	1489020	347256	10740	1554	38808
A	492	148238	726	6555608	99960	6486	151164	313740
B	516460	310590	78300	291460	684	171710	15594	108504
C	46200	4796	47712	7920	12656	27720	2124	64260
D	4200	179100	134640	4830	130260	2277660	4620	8773248
E	9828	16061360	256	13650	3919860	101010	328440	7920
F	55614	97580	26040	131670	1321488	48240	828240	6240

Table 11 presents the maximal periods of the various S-boxes used in encryption algorithms, such as Skipjack [33], SMS4 [34], Kuznyechik [35], Camellia [36], CLEFIA [37], and SEED [38], as well as those constructed using different methods and techniques proposed by the authors [24], [25], [39], [40], [41], [42], [43], [44], [45], [46], [47], [48], and [49]. To determine the maximal periods for these S-boxes with respect to the blocks, we used the input data listed in Table 7. The best results, namely the approximate values of the maximal periods of the S-boxes in the CBC mode with respect to the blocks exceeding $10^{100} > 2^{332}$ were shown Skipjack (2.6×10^{101}), Camellia S_1 (1.2×10^{100}) and proposed by Hussain et al. (2.9×10^{104}) [45].

TABLE 11. The approximate values of the maximal periods of the various S-boxes in the CBC mode for input data of Table 7.

S-boxes	Maximal periods	S-boxes	Maximal periods
Skipjack [33]	2.6×10^{101}	Nitaj et al. [25]	2.64×10^{90}
SMS4 [34]	9.92×10^{93}	Wang et al. [39]	6.47×10^{90}
Kuznyechik [35]	3.14×10^{97}	Zhu et al. [40]	2.7×10^{99}
Camellia S_1 [36]	1.2×10^{100}	Zahid et al. [41]	6.4×10^{99}
Camellia S_2 [36]	6.98×10^{97}	Lu et al. [42]	3.17×10^{90}
Camellia S_3 [36]	6.95×10^{97}	Jiang and Ding [43]	6.14×10^{92}
Camellia S_4 [36]	6.98×10^{97}	Gao et al. [44]	7.66×10^{94}
CLEFIA S_0 [37]	3.17×10^{96}	Hussain et al. [45]	2.9×10^{104}
CLEFIA S_1 [37]	1.45×10^{91}	Zhang et al. [46]	8.4×10^{94}
SEED S_0 [38]	1.18×10^{90}	Chew and Ismail [47]	4.95×10^{95}
SEED S_1 [38]	1.41×10^{95}	Khan et al. [48]	6.71×10^{94}
Cui et al. [24]	6.21×10^{77}	Ahmad et al. [49]	5.9×10^{99}

IV. CONCLUSION

In this paper, we investigate the diffusion effect of the CBC mode on the bijective AES S-box by detecting its periodicity in two ways. The periods of the S-box element sequences in the CBC were calculated with respect to iterations using Algorithms 2 and 3 (Tables 3, 4, and 5), and with respect to blocks using Algorithm 4 (Tables 9 and 10). In our study, the maximal periods of the AES S-box with respect to iterations and blocks showed the same result, which was approximately 9.68×10^{89} (Table 6).

For comparative analysis in our study, we determined the maximal periods for other S-boxes in the CBC mode with respect to the blocks (Table 11). It should be noted that in the case of cryptographically and cyclically good S-boxes, the maximal periods showed very large intervals (more than $10^{77} > 2^{255}$), indicating that the influence of the CBC mode spread over a considerable number of iterations and blocks, confirming the high level of cryptographic strength of the S-boxes.

REFERENCES

[1] C. E. Shannon, "A mathematical theory of cryptography," Bell Labs, New York, NY, USA, Tech. Rep. MM 45-110-02, 1945. [Online]. Available: https://evervault.com/papers/shannon.pdf

[2] J. von Zur Gathen, "Classical cryptology," in *CryptoSchool*, 1st ed. Berlin, Germany: Springer-Verlag, 2015, pp. 61–106.

[3] C. Easttom, *Modern Cryptography: Applied Mathematics for Encryption and Information Security*. 1st ed. New York, NY, USA: McGraw-Hill, 2016.

[4] J. Buchmann, "Encryption," in *Introduction to Cryptography*, 2nd ed. New York, NY, USA: Springer, 2001, pp. 69–101.

[5] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976, doi: 10.1109/TIT.1976.1055638.

[6] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978, doi: 10.1145/359340.359342.

[7] C. Paar, J. Pelzl, and B. Preneel, "Stream ciphers," in *Understanding Cryptography*, 1st ed. Berlin, Germany: Springer, 2010, pp. 29–54.

[8] J. P. Aumasson, "Block ciphers," in *Serious Cryptography: A Practical Introduction to Modern Encryption*. San Francisco, CA, USA: No Starch Press, 2017, pp. 53–76.

[9] M. Gagné, P. Lafourcade, Y. Lakhnech, and R. Safavi-Naini, "Automated security proof for symmetric encryption modes," in *Proc. Adv. Comp. Sci. ASIAN*, in Lecture Notes in Computer Science, vol. 537. Heidelberg, Germany: Springer, pp. 39–53, doi: 10.1007/978-3-642-10622-4_4.

[10] F. Niels, B. Schneier, and T. Kohno, "Block cipher modes," in *Cryptography Engineering*. New York, NY, USA: Wiley, 2010, pp. 63–76.

[11] P. Rogaway. (2011). Evaluation of Some Blockcipher Modes of Operation. Cryptography Research and Evaluation Committees (CRYPTREC) for the Government of Japan 630. [Online]. Available: https://web.cs.ucdavis.edu/~rogaway/papers/modes.pdf

[12] M. Dworkin, "Recommendation for block cipher modes of operation: Methods and techniques," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NIST-SP-800-38A, Dec. 2001. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-38a/final

[13] C. K. Wu and D. Feng, "Boolean function representation of S-boxes and Boolean permutations," in *Boolean Functions and Their Applications in Cryptography*. Berlin, Germany: Springer, 2016, pp. 217–241, doi: 10.1007/978-3-662-48865-2_7.

[14] K. Nyberg, "Perfect nonlinear S-boxes," in *Proc. Workshop Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 1991, pp. 378–386, doi: 10.1007/3-540-46416-6_32.

[15] J. Daemen and V. Rijmen, *The Design of Rijndael*, 2nd ed. Berlin, Germany: Springer, 2020.

[16] M. Dworkin, *Advanced Encryption Standard (AES)*, Gaithersburg, MD, USA: National Institute of Standards and Technology, 2023. [Online]. Available: https://www.nist.gov/publications/advanced-encryption-standard-aes-0

[17] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949, doi: 10.1002/j.1538-7305.1949.tb00928.x.

[18] A. F. Webster and S. E. Tavares, "On the design of S-boxes," in *Proc. Adv. in Cryptol. (CRYPTO)*, in Lecture Notes in Computer Science, vol. 218. Berlin, Germany: Springer, Dec. 2000, pp. 523–534, doi: 10.1007/3-540-39799-X_41.

[19] C. Carlet, "Boolean functions, vectorial functions and cryptography," in *Boolean Functions for Cryptography and Coding Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2021, pp. 76–150, doi: 10.1017/9781108606806.

[20] T. W. Cusick and P. A. Stănică, "Avalanche and propagation criteria," in *Cryptographic Boolean Functions and Applications*, 2nd ed. San Diego, CA, USA: Academic, 2017, pp. 31–54.

[21] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," in *Proc. Adv. Cryptol. (CRYPTO)*, in Lecture Notes in Computer Science, vol. 537. Berlin, Germany: Springer, May 2001, pp. 2–21, doi: 10.1007/3-540-38424-3_1.

[22] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Proc. Adv. Cryptol. (EUROCRYPT)*, in Lecture Notes in Computer Science, vol. 765. Berlin, Germany: Springer, Jul. 2001, pp. 386–397, doi: 10.1007/3-540-48285-7_33.

[23] C. Swenson, *Modern Cryptanalysis: Techniques for Advanced Code Breaking*. Hoboken, NJ, USA: Wiley, 2008. [Online]. Available: https://swenson.io/2022_01_25_modern_cryptanalysis_v11_available_for_free.html

[24] J. Cui, L. Huang, H. Zhong, C. Chang, and W. Yang, "An improved AES S-box and its performance analysis," *Int. J. Innov. Comput., Inf. Control*, vol. 7, no. 5, pp. 2291–2302, 2011. [Online]. Available: https://www.researchgate.net/publication/267554952_An_improved_AES_S-box_and_its_performance_analysis

[25] A. Nitaj, W. Susilo, and J. Tonien, "A new improved AES S-box with enhanced properties," in *Proc. ACISP Inf. Sec. Priv.*, Perth, WA, Australia, Dec. 2020, pp. 125–141. [Online]. Available: https://eprint.iacr.org/2020/1597.pdf, doi: 10.1007/978-3-030-55304-3_7.

[26] Z. Alimzhanova, D. Nazarbayev, A. Ayashova, and A. Kaliyeva, "Analysis of ciphertext behaviour using the example of the AES block cipher in ECB, CBC, OFB and CFB modes of operation, using multiple encryption," in *Proc. Intell. Inf. Database Syst. (ACIIDS)*, in Lecture Notes in Computer Science, vol. 13758. Cham, Switzerland: Springer Nature, Dec. 2022, pp. 621–629, doi: 10.1007/978-3-031-21967-2_50.

[27] B. Song and J. Seberry, "Further observations on the structure of the AES algorithm," in *Proc. 10th Int. Workshop (FSE)*, in Lecture Notes in Computer Science, vol. 2887. Berlin, Germany: Springer, 2003, pp. 223–234, doi: 10.1007/978-3-540-39887-5_17.

[28] T. Van Le, R. Sparr, R. Wernsdorf, and Y. Desmedt, "Complementation-like and cyclic properties of AES round functions," in *Proc. Interfaces Conf. AES*, in Lecture Notes in Computer Science, vol. 3373. Berlin, Germany: Springer, 2005, pp. 128–141, doi: 10.1007/11506447_11.

[29] W. F. Ehrsam, C. H. Meyer, J. L. Smith, and W. L. Tuchman, "Message verification and transmission error detection by block chaining," U.S. Patent 4 074 066, Feb. 14, 1978.

[30] M. Anderson and T. Feil, "Permutations," in *A First Course in Abstract Algebra. Rings, Groups, and Fields*, 3rd ed. New York, NY, USA: Chapman Hall/CRC, 2014, pp. 197–206.

[31] N. Robbins, "Divisibility," in *Beginning Number Theory*, 2nd ed. Sudbury, MA, USA: Jones Bartlett, 2006, pp. 27–52.

[32] J. Gallian, "Permutation groups," in *Contemporary Abstract Algebra*, 7th ed. Belmont, CA, USA: Brooks-Cole/Cengage Learning, 2010, pp. 95–120.

[33] National Institute of Standards and Technology. (May 1998). *Skipjack and KEA Algorithm Specifications*. [Online]. Available: https://csrc.nist.gov/presentations/1998/skipjack-and-kea-algorithm-specifications

[34] W. Diffie and G. Ledin, "SMS4 encryption algorithm for wireless networks," IACR Cryptol. ePrint Arch., Aug. 2008, pp. 1–5. [Online]. Available: https://eprint.iacr.org/2008/329.pdf

[35] V. Dolmatov, "GOST R 34.12-2015: Block cipher 'Kuznyechik,'" *Transformation*, vol. 50, p. 10, Mar. 2016. [Online]. Available: https://www.rfc-editor.org/rfc/rfc7801

[36] K. Aoki et al., "Specification of Camellia—A 128-bit block cipher," Version 2.0, Nippon Telegraph, Telephone Corp., Mitsubishi Electr. Corp., Japan, 2000. [Online]. Available: https://www.cryptrec.go.jp/en/cryptrec_03_spec_cypherlist_files/PDF/06_01espec.pdf

[37] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata, "The 128-bit blockcipher CLEFIA," in *Proc. Int. Workshop Fast Softw. Encryption*, in Lecture Notes in Computer Science, vol. 4593. Berlin, Germany: Springer, 2007, pp. 181–195, doi: 10.1007/978-3-540-74619-5_12.

[38] J. Park, S. Lee, J. Kim, and J. Lee, "The SEED encryption algorithm," Netw. Work. Group., ISOC, Reston, VA, USA, Tech. Rep. RFC 4009, 2005, [Online]. Available: https://citeseerx.ist.psu.edu/doc/10.1.1.374.3466

[39] Y. Wang, P. Lei, and K.-W. Wong, "A method for constructing bijective S-box with high nonlinearity based on chaos and optimization," *Int. J. Bifurcation Chaos*, vol. 25, no. 10, Sep. 2015, Art. no. 1550127, doi: 10.1142/S0218127415501278.

[40] D. Zhu, X. Tong, M. Zhang, and Z. Wang, "A new S-box generation method and advanced design based on combined chaotic system," *Symmetry*, vol. 12, no. 12, p. 2087, Dec. 2020, doi: 10.3390/sym12122087.

[41] A. H. Zahid, E. Al-Solami, and M. Ahmad, "A novel modular approach based substitution-box design for image encryption," *IEEE Access*, vol. 8, pp. 150326–150340, 2020, doi: 10.1109/ACCESS.2020.3016401.

[42] Q. Lu, C. Zhu, and G. Wang, "A novel S-box design algorithm based on a new compound chaotic system," *Entropy*, vol. 21, no. 10, p. 1004, Oct. 2019, doi: 10.3390/e21101004.

[43] Z. Jiang and Q. Ding, "Construction of an S-box based on chaotic and bent functions," *Symmetry*, vol. 13, no. 4, p. 671, Apr. 2021, doi: 10.3390/sym13040671.

[44] W. Gao, B. Idrees, S. Zafar, and T. Rashid, "Construction of nonlinear component of block cipher by action of modular group PSL(2, Z) on projective line PL(GF(28))," *IEEE Access*, vol. 8, pp. 136736–136749, 2020, doi: 10.1109/ACCESS.2020.3010615.

[45] I. Hussain, A. Anees, T. Al-Maadeed, and M. Mustafa, "Construction of S-box based on chaotic map and algebraic structures," *Symmetry*, vol. 11, no. 3, p. 351, Mar. 2019, doi: 10.3390/sym11030351.

[46] Y.-Q. Zhang, J.-L. Hao, and X.-Y. Wang, "An efficient image encryption scheme based on S-boxes and fractional-order differential logistic map," *IEEE Access*, vol. 8, pp. 54175–54188, 2020, doi: 10.1109/ACCESS.2020.2979827.

[47] L. C. Nizam Chew and E. S. Ismail, "S-box construction based on linear fractional transformation and permutation function," *Symmetry*, vol. 12, no. 5, p. 826, May 2020, doi: 10.3390/sym12050826.

[48] M. F. Khan, A. Ahmed, and K. Saleem, "A novel cryptographic substitution box design using Gaussian distribution," *IEEE Access*, vol. 7, pp. 15999–16007, 2019, doi: 10.1109/ACCESS.2019.2893176.

[49] M. Ahmad, E. Al-Solami, A. M. Alghamdi, and M. A. Yousaf, "Bijective S-boxes method using improved chaotic map-based heuristic search and algebraic group structures," *IEEE Access*, vol. 8, pp. 110397–110411, 2020, doi: 10.1109/ACCESS.2020.3001868.

ZHANNA ALIMZHANOVA received the Graduate degree from the Faculty of Mathematics, Al-Farabi Kazakh National University, Almaty, Kazakhstan, in 1994, and the degree in physical and mathematical sciences, in 2000. She is currently an Associate Professor with the Department of Information Systems, Al-Farabi Kazakh National University, and a Professor with the Yesbulatov Almaty Academy of the Ministry of Internal Affairs, Kazakhstan. Her current research interests include the mathematical modeling of technical processes, information systems, and information security systems.

MARIA SKUBLEWSKA-PASZKOWSKA (Member, IEEE) received the Graduate degree in computer science from the Lublin University of Technology, Lublin, Poland, and the Ph.D. degree from the Silesian University of Technology, Gliwice, in 2009. She is currently an Assistant Professor with the Department of Computer Science, Lublin University of Technology. Her teaching work concerns programming languages, databases, designing, and implementation of information systems. Her current research interests include motion capture, motion analysis, artificial intelligence, data classification, computer vision, and the usability of graphical interfaces.

DAUREN NAZARBAYEV received the Specialist Diploma in applied mathematics (engineering-mathematician qualification) and the M.S. degree in mathematical and computer modeling from Satbayev Kazakh National Technical University (Satbayev University), in 2005 and 2012, respectively. He is currently pursuing the Ph.D. degree in information security systems with Al-Farabi Kazakh National University. His current research interests include symmetric cryptography and the study of methods and techniques for evaluating the cryptographic strength of encryption algorithms.